IT-Sicherheit und Recht

Rechtliche und technisch-organisatorische Aspekte für Unternehmen

Herausgegeben von

Dr. Tim Reinhard
Rechtsanwalt

Lorenz Pohl
Rechtsanwalt

und

Dr. Hans-Christoph Capellaro
Dipl.-Math.

mit Beiträgen von

Ulrich Bäumer, LL.M.
Rechtsanwalt, Attorney-at-Law, New York

Joachim Breithaupt
Rechtsanwalt und Steuerberater

Dr. Hans-Christoph Capellaro
Dipl.-Math.

Konstantin Ewald
Rechtsanwalt

Dr. Andreas Imping
Rechtsanwalt und Fachanwalt für Arbeitsrecht

Lorenz Pohl
Rechtsanwalt

Dr. Tim Reinhard
Rechtsanwalt

Dr. Martin Sundermann
Rechtsanwalt

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über dnb.ddb.de abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978 3 503 10037 8

ISBN 978 3 503 10037 8

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Bibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO Norm 9706.

Gesetzt aus der Stempel Garamond, 9/11 Punkt

Satz: multitext, Berlin
Druck: Hubert & Co., Göttingen

Vorwort

Trojanische Pferde waren vor über 3000 Jahren aus Holz gefertigt. Das Prinzip gibt es noch heute, die Technik – insbesondere die Informationstechnologie – hat sich seit dieser Zeit jedoch stark verändert.

Nahezu jedes Unternehmen setzt heute Informationstechnologie ein. Bei fehlenden oder unzureichenden IT-Sicherheitsmaßnahmen riskieren Unternehmen IT-Sicherheitsvorfälle, welche etwa zu Produktionsverzögerungen oder Produktionsstillstand führen können. Geheimhaltungsbedürftige Entwicklungs- oder Kundendaten können ausgespäht werden. Die Unternehmen riskieren neben Reputationsverlusten Schadensersatzforderungen und Konventionalstrafen. Im worst case kann ein IT-Sicherheitsvorfall die Insolvenz eines Unternehmens bedeuten. Umgekehrt ist nicht alles, was aus dem Blickwinkel der IT-Sicherheit wünschenswert und technisch möglich wäre, rechtlich auch erlaubt.

Das vorliegende Buch stellt die wesentlichen rechtlichen Anforderungen dar, welche private Unternehmen nach deutschem Recht beim Thema IT-Sicherheit zu beachten haben. Es geht außerdem in technisch-organisatorischer Hinsicht auf die Erstellung eines unternehmensbezogenen IT-Sicherheitskonzeptes ein. Das Buch richtet sich zum einen an Vorstände, Geschäftsführer, Unternehmensinhaber, IT-Sicherheitsbeauftragte, betriebliche Datenschutzbeauftragte, Leiter von IT-Abteilungen und sonstige IT-Verantwortliche, zum anderen auch an Justiziare, Mitarbeiter von Rechtsabteilungen und allgemein an Juristen, die sich dem Thema IT-Sicherheit in rechtlicher Hinsicht nähern wollen.

Zu danken haben wir allen Mitautoren sowie Herrn Joachim Diehm vom Erich Schmidt Verlag für ihre Mitwirkung an der Entstehung des Buches. Zu Dank verpflichtet sind wir außerdem Frau Nanni Spitzer, Herrn Marcus Wuntke und Frau Katja Jülich für die engagierte Mitarbeit. Für Anregungen und Kritik seitens der Leser sind wir stets offen und bitten Sie, uns diese über den Verlag zukommen zu lassen.

München, im Dezember 2006

Tim Reinhard Lorenz Pohl Hans-Christoph Capellaro

Inhaltsübersicht

Seite

Teil I: Rechtliche Aspekte der IT-Sicherheit 35

1. Kapitel: Grundlagen 37
§ 1 Legaldefinition IT-Sicherheit 37
§ 2 Technische Regelwerke zur IT-Sicherheit und deren Bedeutung 37
§ 3 Signaturrecht 47

2. Kapitel: Datenschutzrecht 55
§ 1 Grundsätze des Datenschutzrechts 55
§ 2 Acht goldene Regeln zur Sicherheit personenbezogener Daten 59
§ 3 Auftragsdatenverarbeitung 81
§ 4 Der Datenschutzbeauftragte 86
§ 5 Sanktionen bei Verstoß gegen Datenschutzrecht 89
§ 6 Datenschutzaudit 91

3. Kapitel: Gesellschaftsrecht 94
§ 1 Einführung 94
§ 2 Organisation der IT Sicherheit im Unternehmen 94
§ 3 IT-Sicherheit im Konzern 130

4. Kapitel: Strafrecht 136
§ 1 Straftaten von Mitarbeitern im Zusammenhang mit der Unternehmens-IT 136
§ 2 Straftaten der Unternehmensleitung 155

5. Kapitel: Vertragliche und deliktische Haftung 159
§ 1 Einleitung 159
§ 2 Haftung für Herstellung, Planung und Vertrieb von Soft- bzw. Hardware 165
§ 3 Haftung von IT-Verwendern 175
§ 4 Zusammenfassung 193

6. Kapitel: Handels- und Steuerrecht 198
§ 1 Handels- und steuerrechtliche Vorgaben an das IT-System 198
§ 2 Digitaler Datenzugriff und Prüfbarkeit digitaler Unterlagen durch die Finanzverwaltung 219

7. Kapitel: Urheberrecht – DRM 226
§ 1 Einführung 226
§ 2 Rechtliche Gesichtspunkte 231

8. Kapitel: Wettbewerbsrecht 249
§ 1 Unzumutbare Belästigungen § 7 UWG 249
§ 2 Betriebsspionage § 17 Abs. 2 UWG 250

Seite
§ 3 Verwertung von Vorlagen § 18 UWG 250
§ 4 „Vorteil durch Rechtsbruch" § 4 Nr. 11 UWG 251

9. Kapitel: Gewerberecht 253
§ 1 Sinn und Zweck der Gewerbeuntersagung nach § 35 Gewerbeordnung (GewO) 253
§ 2 Voraussetzungen der Gewerbeuntersagung 255
§ 3 Adressat der Untersagungsverfügung 259
§ 4 Zuständige Behörde 259
§ 5 Bindung an strafrechtliche Entscheidungen 260
§ 6 Folgen der Untersagungsverfügung 260

10. Kapitel: Vergaberecht 262
§ 1 Einführung in das Vergaberecht 262
§ 2 IT-Sicherheit in der Leistungsbeschreibung öffentlicher Auftraggeber 266
§ 3 IT-Sicherheit bei Wertung der Angebote durch öffentliche Auftraggeber 268

11. Kapitel: Arbeitsrecht 272
§ 1 Überblick 272
§ 2 Pflichten des Arbeitnehmers 273
§ 3 Sanktionierung von Pflichtverletzungen 296
§ 4 Haftung des Arbeitnehmers 301
§ 5 Elektronische Personalakte 308

12. Kapitel: IT-Sicherheit und Basel II 318
§ 1 Basel II und Eigenkapitalvorschriften für Kreditinstitute 318
§ 2 Rating-Systeme und ihre Auswirkungen auf die Unternehmens-IT . . 319
§ 3 Basel II und IT-Anforderungen bei Banken 322

13. Kapitel: Branchenspezifische Aspekte 323
§ 1 Banken 323
§ 2 Krankenhäuser 338

14. Kapitel: Fazit 348

Teil II: Technische und organisatorische Aspekte der IT-Sicherheit 349

1. Kapitel: Die Berücksichtigung der Informationssicherheit im Unternehmen 351
§ 1 Grundbegriffe 351
§ 2 Schaffung der organisatorischen Voraussetzungen 354
§ 3 Das Informationssicherheits-Managementsystem 358
§ 4 Die Bedeutung der Zertifizierung 359

2. Kapitel: Erstellung, Implementierung und Anpassung eines IT-Sicherheitskonzepts im Unternehmen 361
§ 1 Identifikation der Sicherheitsanforderungen 361

Seite
§ 2 Definition der IT-Sicherheitsleitlinie 363
§ 3 Risikoanalyse 365
§ 4 Maßnahmenplanung. 365
§ 5 Definition von Maßnahmen 391
§ 6 Implementierung von Maßnahmen 396
§ 7 Überwachung von IT-Sicherheitsmaßnahmen 401
§ 8 Kontinuierliche Verbesserung der IT-Sicherheitsmaßnahmen 402

Inhaltsverzeichnis

	Seite	Randnummer
Vorwort	5	
Inhaltsübersicht	7	
Abkürzungsverzeichnis	29	

Teil I:
Rechtliche Aspekte der IT-Sicherheit

1. Kapitel: Grundlagen

§ 1	**Legaldefinition IT-Sicherheit**		37	1
§ 2	**Technische Regelwerke zur IT-Sicherheit und deren Bedeutung**		37	2–22
	I.	IT-Grundschutz-Kataloge (vormals: IT-Grundschutzhandbuch)	37	4– 6
	II.	BS 7799-1/ISO 17799 und BS 7799-2/ISO 27001	39	7–10
	III.	CoBIT	42	11–12
	IV.	ITIL	43	13–15
	V.	Common Criteria	44	16–17
	VI.	ITSEC	45	18
	VII.	TCSEC	46	19
	VIII.	ISO-TR 13335	46	20
	IX.	ISO 9000	46	21
	X.	FIPS 140-1/2	47	22
§ 3	**Signaturrecht**		47	23–44
	I.	Einleitung: Zur Bedeutung elektronischer Signaturen	47	23–27
		1. Schriftform von Erklärungen	47	24–25
		2. Hürden für die Akzeptanz der elektronischen Signatur	48	26–27
	II.	Rechtlicher Rahmen des elektronischen Signaturverfahrens	49	28–44
		1. Technische Grundlagen des elektronischen Signaturverfahrens	49	29
		2. Signaturtypen	50	30–36
		2.1 Nichtqualifizierte Signaturen	50	31–33
		2.1.1 Einfache Signaturen	50	32
		2.1.2 Fortgeschrittene Signaturen	50	33
		2.2 Qualifizierte Signaturen	51	34–36
		2.2.1 Definition der qualifizierten Signatur	51	35
		2.2.2 Identitätsfunktion und Zertifizierung	52	36

	Seite	Randnummer
3. Die Rolle der Zertifizierungsdiensteanbieter	52	37–44
3.1 Akkreditierung	52	38
3.2 Inhalt qualifizierter Signaturzertifikate	52	39– 41
3.2.1 Akkreditierter Zertifizierungsdiensteanbieter	53	40
3.2.2 Nicht akkreditierter Zertifizierungsdiensteanbieter	53	41
3.3 Aufbewahrung qualifizierter Signaturzertifikate	53	42
3.4 Haftung des Zertifizierers	54	43
3.5 Fazit	54	44

2. Kapitel: Datenschutzrecht

§ 1	**Grundsätze des Datenschutzrechts**		55	45– 54
	I.	Definition personenbezogene Daten	55	46– 47
	II.	Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung	56	48– 50
	III.	Grundsatz der Datenvermeidung und Datensparsamkeit	57	51
	IV.	Datengeheimnis	58	52– 54
§ 2	**Acht goldene Regeln zur Sicherheit personenbezogener Daten**		59	55–100
	I.	Zutrittskontrolle (Nr. 1 der Anlage zu § 9 BDSG)	61	59– 63
	II.	Zugangskontrolle (Nr. 2 der Anlage zu § 9 BDSG)	63	64– 67
	III.	Zugriffskontrolle (Nr. 3 der Anlage zu § 9 BDSG)	66	68– 71
	IV.	Weitergabekontrolle (Nr. 4 der Anlage zu § 9 BDSG)	68	72– 75
	V.	Eingabekontrolle (Nr. 5 der Anlage zu § 9 BDSG)	70	76– 79
	VI.	Auftragskontrolle (Nr. 6 der Anlage zu § 9 BDSG)	72	80– 84
	VII.	Verfügbarkeitskontrolle (Nr. 7 der Anlage zu § 9 BDSG)	75	85– 88
	VIII.	Datentrennung (Nr. 8 der Anlage zu § 9 BDSG)	76	89– 91
	IX.	Umfang der zu ergreifenden technischen und organisatorischen Maßnahmen	77	92–100
§ 3	**Auftragsdatenverarbeitung**		81	101–117
§ 4	**Der Datenschutzbeauftragte**		86	118–129
	I.	Bestellung	86	118–120
	II.	Aufgaben	87	121–129

		Seite	Randnummer
§ 5	**Sanktionen bei Verstoß gegen Datenschutzrecht**	89	130–134
I.	Aufsichtsbehörden	89	130–132
II.	Haftung (§ 7 BDSG)	91	133
III.	Bußgeld (§ 43 BDSG)	91	134
§ 6	**Datenschutzaudit**	91	135–141

3. Kapitel: Gesellschaftsrecht

§ 1	**Einführung**	94	142
§ 2	**Organisation der IT Sicherheit im Unternehmen**	94	143–227
I.	Allgemeines zur Geschäftsführung und Vertretung	94	143–147
	1. Begriff und Wesen der Geschäftsführung	94	144
	2. Begriff und Wesen der Vertretung	95	145–147
II.	Zuständigkeit für die Geschäftsführung	96	148–165
	1. Gesellschaft mit beschränkter Haftung (GmbH)	96	149–152
	1.1 Die Organe der GmbH	96	149
	1.2 Funktion und Aufgabe der Geschäftsführer	96	150
	1.3 Funktion und Aufgabe der Gesellschafterversammlung	97	151–152
	2. Aktiengesellschaft (AG)	98	153–157
	2.1 Die Organe der AG	98	154
	2.2 Funktion des Vorstandes	99	155
	2.3 Der Aufsichtsrat	99	156
	2.4 Die Hauptversammlung	99	157
	3. Personengesellschaften	100	158–165
	3.1 Die Struktur der Personengesellschaft	100	159–161
	3.2 Grundtypen der Personengesellschaft	101	162
	3.3 Geschäftsführung durch die persönlich haftenden Gesellschafter	101	163–164
	3.4 Die Stellung der Kommanditisten	102	165
III.	Allgemeine Grundsätze der Geschäftsführung	103	166–182
	1. Die Geschäftsführung als einheitliches Leitungsorgan	103	167–168
	2. Allzuständigkeit des Geschäftsführungsorgans	104	169–170
	3. Möglichkeit der Delegation auf den nachgeordneten Bereich	105	171–173
	3.1 Voraussetzungen der Delegation	105	172
	3.2 Restverantwortung der Geschäftsführung bei der Delegation	106	173
	4. Geschäftsordnung und Arbeitsteilung innerhalb der Geschäftsführung	106	174–182
	4.1 Ressort- und Spartenorganisation	107	175
	4.2 Persönliche Anforderungen an das Geschäftsführungsmitglied	107	176

		Seite	Randnummer
	4.3 Restverantwortung, Kontroll- und Eingriffspflichten	107	177
	4.4 Form der Geschäftsverteilung	108	178
	4.5 Kernbereich der Geschäftsführung	109	179
	4.6 Auswirkungen des Risikomanagements auf die Organisation der Geschäftsführung	110	180–182
IV.	Geschäftsführung und IT-Sicherheit	111	183–197
	1. IT-Sicherheit als Kernbereichsaufgabe der Geschäftsführung	112	184
	2. Anforderungen an die Organisation der Geschäftsführung im IT-Bereich	112	185–191
	2.1 Erfasste Unternehmen	112	185
	2.2 Kernbereich der Geschäftsführung im Bereich IT	113	186
	2.3 Möglichkeit der Ressort- und Spartenverteilung	113	187–191
	2.3.1 Grenzen der Geschäftsverteilung	114	188
	2.3.2 Notwendigkeit der Geschäftsverteilung im Bereich IT-Sicherheit	114	189
	2.3.3 Ausgestaltung der Geschäftsordnung im Bereich IT-Sicherheit	114	190
	2.3.4 Restverantwortung der Gesamtgeschäftsführung	115	191
	3. Delegation von IT Aufgaben	115	192–196
	3.1 Grenzen der Delegationsmöglichkeit	115	192
	3.2 Voraussetzungen wirksamer Delegation	115	193–195
	3.2.1 Personalauswahl	116	194
	3.2.2 Schaffung einer Organisationsstruktur	116	195
	3.3 Restverantwortung der Geschäftsführung trotz Delegation	116	196
	4. Zusammenfassung	117	197
V.	IT-Sicherheit als Aufgabe für die Kontrollorgane	117	198–203
	1. Wesen des Aufsichtsrates in deutschen Gesellschaften	117	199
	2. Überblick über die Aufgaben des Aufsichtsrates	118	200
	3. IT-Sicherheit im Aufsichtsrat	119	201–203
VI.	IT-Sicherheit und Organhaftung	120	204–227
	1. Grundprinzipien der Organhaftung	120	204
	2. Organhaftung bei Kapitalgesellschaften	120	205–221
	2.1 Haftung gegenüber der Gesellschaft	121	206–218
	2.1.1 Gläubiger der Ansprüche	121	206
	2.1.2 Pflichtverletzung und Business Judgement Rule	121	207–208

	Seite	Randnummer
2.1.3 Verschulden	123	209–211
2.1.4 Schaden	124	212
2.1.5 Haftungsumfang und Geltendmachung der Ansprüche	124	213–215
2.1.6 Darlegungs- und Beweislast	125	216–218
2.2 Haftung gegenüber Gesellschaftern und Dritten	127	219–220
2.3 Haftung des Aufsichtsrates	127	221
3. Geschäftsführungshaftung bei Personengesellschaften	128	222–227
3.1 Haftung gegenüber Dritten	128	223
3.2 Binnenhaftung in der Gesellschaft	128	224–226
3.3 Besonderheiten bei der Kapitalgesellschaft & Co.	130	227
§ 3 IT-Sicherheit im Konzern	130	228–237
I. Bedeutung des Konzernrechts	130	229
II. Möglichkeiten und Grenzen von Weisungen und Kooperationen im Konzern	132	230–232
1. Grenzen der Einflussnahmemöglichkeit	132	230
2. Qualifiziert faktische Konzernierung	132	231
3. Sonstige Pflichten im Konzern	133	232
III. IT Themen im Konzern	133	233–237
1. Sicherstellung funktionsfähiger IT in jeder Gesellschaft	133	234
2. Dokumentationserfordernisse bei Inter-Company-Verträgen	134	235
3. Organisationsanforderungen der IT unter dem Blickwinkel des Konzernrechts	134	236–237
4. Kapitel: Strafrecht		
§ 1 Straftaten von Mitarbeitern im Zusammenhang mit der Unternehmens-IT	136	239–289
I. Verbotene Inhalte	136	240–248
1. Volksverhetzung (§ 130 StGB)	136	240–241
2. Anleitung zu Straftaten (§ 130a StGB)	138	242–243
3. Gewaltdarstellung (§ 131 StGB)	139	244
4. Verbreitung, Erwerb und Besitz kinderpornographischer Schriften (§ 184b StGB)	140	245–248
II. Spezifische Computerdelikte	142	249–280
1. Ausspähen von Daten (§ 202a StGB)	142	249–258
2. Computerbetrug (§ 263a StGB)	145	259–263
3. Fälschung beweiserheblicher Daten (§§ 269, 270 StGB)	147	264–268
4. Urkundenunterdrückung (§ 274 StGB)	148	269–270

		Seite	Randnummer
	5. Datenveränderung (§ 303a StGB)	149	271–276
	6. Computersabotage (§ 303b StGB)	151	277–280
III.	Telekommunikationsbezogene Delikte	152	281–289
	1. Verletzung des Fernmeldegeheimnisses (§ 206 StGB)	152	281–288
	2. Störung von Telekommunikationsanlagen (§ 317 StGB)	155	289
§ 2	**Straftaten der Unternehmensleitung**	155	290–296
I.	Beihilfe (§ 27 StGB)	155	291–293
II.	Untreue (§ 266 StGB)	156	294–296

5. Kapitel: Vertragliche und deliktische Haftung

§ 1	**Einleitung**	159	297–311
I.	Allgemein	159	298–300
II.	Grundgedanken zivilrechtlicher Haftung	160	301–304
III.	Haftungsmaßstab des BGB und rechtliche Wirkung von IT-Sicherheitsstandards	161	305–311
§ 2	**Haftung für Herstellung, Planung und Vertrieb von Soft- bzw. Hardware**	165	312–339
I.	Haftung der Hersteller	165	313–334
	1. Vertragliche Haftung	166	314–327
	1.1 Gewährleistungsansprüche	166	315–320
	1.2 Weitere vertragliche Schadensersatzansprüche	167	321
	1.3 Outsourcing-Verträge	168	322–326
	1.4 Haftung für Verhalten Dritter	169	327
	2. Gesetzliche Haftung	170	328–333
	2.1 Deliktische Haftung	170	328
	2.1.1 Geschützte Rechtsgüter	170	328
	2.1.2 Verschulden	171	329–331
	2.1.3 Zurechnung des Verhaltens Dritter	172	332
	2.2 Produkthaftungsgesetz	172	333
	3. Verschulden Dritter	173	334
II.	Haftung von IT-Verkäufern	173	335–336
III.	Haftung für Planung und Installation	174	337
IV.	Mitverschulden	174	338–339
§ 3	**Haftung von IT-Verwendern**	175	340–387
I.	Vertragliche Haftung	176	342–343
II.	Gesetzliche Haftung	177	344–353
	1. Deliktische Haftung	178	344–347
	1.1 Geschützte Rechtsgüter	178	344
	1.2 Verschulden	178	345–347
	2. Bundesdatenschutzgesetz	179	348–353

		Seite	Randnummer
III.	Grundsätzliche Anforderungen	182	354–371
	1. IT-Sicherheitsmanagement	182	356
	2. Organisation	183	357
	3. Personal	183	358–360
	4. Notfallvorsorge-Konzept	184	361
	5. Datensicherungskonzept	184	362–364
	6. Datenschutz	185	365
	7. Computer-Virenschutzkonzept	185	366
	8. Kryptokonzept	186	367
	9. Behandlung von Sicherheitsvorfällen	186	368
	10. Hard- und Softwaremanagement	186	369
	11. Outsourcing	187	370
	12. Zusammenfassung	187	371
IV.	Versand einer virenbelasteten Email	187	372–375
	1. Vertragliche Haftung	187	372
	2. Deliktische Haftung	187	373
	3. Verschulden	188	374
	4. Mitverschulden des E	188	375
V.	Grob fahrlässige Weiterverbreitung von Viren	189	376–377
VI.	WLAN	190	378–386
	1. Zivilrechtliche Ansprüche gegen „Schwarzsurfer“ in WLANs	190	378–381
	2. Störerhaftung von WLAN-Betreibern bei ungeschützter WLAN-Verbindung	191	382–386
VII.	Haftung der Unternehmensleitung gegenüber dem eigenen Unternehmen	192	387
§ 4	**Zusammenfassung**	193	388

6. Kapitel: Handels- und Steuerrecht

§ 1	**Handels- und steuerrechtliche Vorgaben an das IT-System**	198	393–458
I.	Einsatz von IT in der Rechnungslegung	198	393
II.	Handels- und steuerrechtliche Anforderungen an die IT-gestützte Rechnungslegung	198	394–458
	1. Allgemeine Rechtsgrundlagen für die IT-gestützte Rechnungslegung	198	394
	2. Grundsätze ordnungsgemäßer Buchführung	199	395–401
	3. Grundsätze ordnungsgemäßer EDV-gestützter Buchführungssysteme (GoBS)	200	402–434
	3.1 Journal- und Kontenfunktion	201	403–406
	3.1.1 Belegfunktion	201	404
	3.1.2 Journalfunktion	202	405
	3.1.3 Kontenfunktion	202	406
	3.2 Buchungen	203	407–409

	Seite	Randnummer
3.3 Internes Kontrollsystem (IKS)	204	410–414
3.4 Datensicherheit und Datenschutz	205	415–423
3.5 Dokumentation und Prüfbarkeit	208	424–428
3.6 Aufbewahrungsflichten und -fristen	209	429–433
3.7 Verantwortlichkeit	210	434
4. GoB bei Einsatz von e-commerce	211	435–444
4.1 Sicherheit und Ordnungsgemäßheit der Buchführung	211	436
4.2 Verfügbarkeit des IT-Systems	212	437
4.3 Vertraulichkeit	212	438
4.4 Authentizität	212	439
4.5 Verbindlichkeit	212	440
4.6 Vollständigkeit	213	441
4.7 Richtigkeit	213	442
4.8 Zeitgerechtheit	214	443
4.9 Nachvollziehbarkeit	214	444
5. Die elektronische Rechnung	214	445–458
5.1 Elektronischer Datenaustausch (EDI)	215	449
5.2 Qualifizierte elektronische Signatur	216	450–453
5.3 Rechnungsübermittlung	217	454–556
5.4 Aufbewahrung	218	457
5.5 Internationaler Einsatz elektronischer Rechnungen	219	458
§ 2 Digitaler Datenzugriff und Prüfbarkeit digitaler Unterlagen durch die Finanzverwaltung	219	459–472
I. Zulässigkeit des digitalen Datenzugriffs	219	459–464
1. Unmittelbarer Datenzugriff	220	460–461
2. Mittelbarer Datenzugriff	221	462
3. Datenträgerüberlassung	221	463
4. Ermessensentscheidung	222	464
II. Prüfungssoftware IDEA	222	465
III. Umfang des Datenzugriffs	223	466
IV. Archivierungspflichten	224	467–471
V. Rechtsfolgen bei Verstoß gegen den digitalen Datenzugriff	225	472
7. Kapitel: Urheberrecht – DRM		
§ 1 Einführung	226	473
I. Hintergrund	226	473–474
II. Begrifflichkeiten	226	475
III. Erscheinungsformen	227	476–488
1. Kontrolle des Zugangs bzw. der Nutzung	228	476
1.1 Zugangskontrollsysteme	228	477
1.2 Nutzungskontrollsysteme	228	478

	Seite	Randnummer
2. Technische Differenzierung	229	479
2.1 Kopierschutz für Datenträger	229	479
2.2 Kennzeichnung von Daten	229	480–484
2.3 kryptographische Sicherung für Daten	230	485
3. Praxisbeispiele	230	486
3.1 Microsoft Windows Media Rights Manager (WMRM)	230	486
3.2 Fairplay (Apple iTunes)	231	487
3.3 Control Scrambling System (CSS) bei DVDs	231	488
§ 2 Rechtliche Gesichtspunkte	231	489–525
I. Urheberrecht	231	489–518
1. Die Regelungen der §§ 95a ff. UrhG	231	490–512
1.1 Hintergrund	231	490
1.2 § 95a UrhG	232	491–499
1.2.1 Schutzumfang – § 95a Abs. 1 und Abs. 2 UrhG	232	491–495
1.2.2 Verbotene Vorbereitungshandlungen, § 95a Abs. 3 UrhG	234	496
1.2.3 Rechtsfolgen eines Verstoßes gegen § 95a UrhG	235	497–499
1.3 Durchsetzung von Schrankenbestimmungen, § 95b UrhG	237	500–504
1.3.1 Sinn und Zweck	237	500
1.3.2 Begünstigte	237	501
1.3.3 Umsetzung in der Praxis	238	502
1.3.4 Rechtliche Durchsetzung	238	503
1.3.5 Einschränkung des § 95b Abs. 3 UrhG	238	504
1.4 Schutz der zur Rechtewahrnehmung erforderlichen Informationen – § 95c UrhG	239	505
1.5 Hinweispflicht, § 95d UrhG	240	506–510
1.6 Problem der Pauschalvergütung/Doppelvergütung	241	511–512
1.6.1 Hintergrund	241	511
1.6.2 Reaktion des Gesetzgebers	241	512
2. DRM bei Software, § 69a ff. UrhG	242	513–518
2.1 Abgrenzung zu § 95a ff. UrhG	242	514
2.2 Schutzumfang und verbotene Handlungen	243	515
2.3 Schutz gegen Umgehungsprodukte, § 69f Abs. 2 UrhG	243	516
2.4 Keine § 95c UrhG entsprechende Norm	244	517
2.5 Schrankenregelung	244	518
II. ZKDSG	245	519–524
1. Hintergrund	245	519

		Seite	Randnummer
2.	Anwendungsbereich	245	520
3.	Verbote	246	521–522
4.	Sanktionen bei Verstoß	246	523
5.	Abgrenzung vom UrhG	246	524
III.	Datenschutz	247	525

8. Kapitel: Wettbewerbsrecht

§ 1	**Unzumutbare Belästigungen § 7 UWG**	249	527
§ 2	**Betriebsspionage § 17 Abs. 2 UWG**	250	528–529
§ 3	**Verwertung von Vorlagen § 18 UWG**	250	530
§ 4	**„Vorteil durch Rechtsbruch" § 4 Nr. 11 UWG**	251	531–532

9. Kapitel: Gewerberecht

§ 1	**Sinn und Zweck der Gewerbeuntersagung nach § 35 Gewerbeordnung (GewO)**	253	533–534
§ 2	**Voraussetzungen der Gewerbeuntersagung**	255	535–541
I.	Betrieb eines Gewerbes	255	535
II.	Unzuverlässigkeit	255	536–540
1.	Definition der Unzuverlässigkeit	255	536–537
2.	Fallgruppen für die Unzuverlässigkeit	256	538–540
2.1	Straftaten und Ordnungswidrigkeiten	256	538
2.2	Mangelnde Sachkunde	257	539
2.3	Nachlässigkeiten bei der IT-Sicherheit als eigene Fallgruppe?	258	540
III.	Erforderlichkeit	258	541
§ 3	**Adressat der Untersagungsverfügung**	259	542
§ 4	**Zuständige Behörde**	259	543–544
§ 5	**Bindung an strafrechtliche Entscheidungen**	260	545
§ 6	**Folgen der Untersagungsverfügung**	260	546–548
I.	Wirkung	260	546
II.	Durchsetzung	261	547
III.	Konsequenzen bei Zuwiderhandlung	261	548

10. Kapitel: Vergaberecht

§ 1	**Einführung in das Vergaberecht**	262	549–559
I.	Sinn und Zweck des Vergaberechts	262	549
II.	Rechtsgrundlagen des Vergaberechts	263	550–555
1.	Rechtsgrundlagen für EU-weite Vergabeverfahren	263	550–554
2.	Rechtsgrundlagen für das nationale Vergabeverfahren	264	555

		Seite	Randnummer
III.	Ablauf des Vergabeverfahrens	264	556–559
§ 2	**IT-Sicherheit in der Leistungsbeschreibung öffentlicher Auftraggeber**	266	560–564
§ 3	**IT-Sicherheit bei Wertung der Angebote durch öffentliche Auftraggeber**	268	565–574
I.	Fachkunde, Leistungsfähigkeit, Zuverlässigkeit	268	565–570
II.	Das wirtschaftlichste Angebot	270	571–574

11. Kapitel: Arbeitsrecht

§ 1	**Überblick**	272	575–577
§ 2	**Pflichten des Arbeitnehmers**	273	578–618
I.	Rechtsgrundlage	273	578
II.	Weisungsrecht des Arbeitgebers	274	579
III.	Grenzen des Weisungsrechtes	274	580–588
	1. Arbeitsvertrag	274	581–582
	2. Betriebliche Mitbestimmung	276	583
	3. Tarifvertrag	276	584
	4. Gesetz	277	585–587
	4.1 Grenze des billigen Ermessens	277	586
	4.2 Sonstige Normen	277	587
	5. Verfassung	277	588
IV.	Unterrichtung und Schulung des Arbeitnehmers	278	589–590
V.	Überwachung des Arbeitnehmers	279	591–618
	1. Rechtlicher Zwang – Rechtliche Hürden	279	591
	2. Überwachung des Datenverkehrs	280	592–609
	2.1 Grundsätze	280	593–609
	2.1.1 Dienstliche Nutzung	280	594–597
	2.1.2 Privatnutzung	282	598–605
	2.1.3 Private Nutzung und Fernmeldegeheimnis	285	606
	2.1.4 Exkurs: Filterung von E-Mails	286	607–609
	2.2 Betriebliche Mitbestimmung	287	610–613
	2.3 Folgen rechtswidriger Überwachung	293	614
	2.4 Empfehlungen für die Praxis	293	615–618
§ 3	**Sanktionierung von Pflichtverletzungen**	296	619–632
I.	Ermahnung	296	620
II.	Abmahnung	296	621–624
	1. Form und Inhalt	297	622–623
	2. Rechtsschutz	297	624
III.	Kündigung	298	625–632
	1. Voraussetzungen	298	626–630
	1.1 Grund	298	626–629
	1.1.1 Personenbedingter Grund	298	626

		Seite	Randnummer
	1.1.2 Verhaltensbedingter Grund	299	627–629
	1.2 Abmahnung	300	630
	2. Form und Inhalt	301	631
	3. Rechtsschutz	301	632
§ 4	**Haftung des Arbeitnehmers**	301	633–648
I.	Rechtsgrundlage	302	635–638
II.	Grundsätze der schadensgeneigten Arbeit	304	639–648
	1. Begünstigter Personenkreis	304	639
	2. Privilegierte Tätigkeit	304	640
	3. Schadenverteilung zwischen Arbeitnehmer und Arbeitgeber	305	641–646
	4. Freistellungsverpflichtung des Arbeitgebers	307	647
	5. Vertragliche Gestaltung	308	648
§ 5	**Elektronische Personalakte**	308	649–667
I.	Allgemeines	309	650–653
	1. Definition	309	650
	2. Personalinformationssyteme	309	651
	3. Pflichten des Arbeitgebers	309	652–653
II.	Recht zur Einsichtnahme	311	654
	1. Arbeitnehmer	311	654
	2. Betriebsrat	312	656–657
III.	Elektronische Personaldatenverwaltung	312	658
	1. Form und Gestaltung	312	658
	2. Datensicherheit	313	659–663
	2.1 Bundesdatenschutzgesetz	313	659
	2.2 Erhebung und Verarbeitung von Personaldaten	313	660–662
	2.3 Rechte des Arbeitnehmers	315	663
IV.	Mitbestimmung des Betriebsrats	316	664
	1. Unterrichtung und Beratung	316	664
	2. Überwachung	316	665–666
	3. Datenschutzbeauftragter	317	667

12. Kapitel: IT-Sicherheit und Basel II

§ 1	**Basel II und Eigenkapitalvorschriften für Kreditinstitute**	318	668–669
§ 2	**Rating-Systeme und ihre Auswirkungen auf die Unternehmens-IT**	319	670–680
I.	Externes und internes Rating	319	671–672
II.	Qualitative und quantitative Merkmale	319	673–676
III.	Auswirkungen auf die IT-Sicherheit	320	677–679
IV.	Maßnahmen zur Einführung eines Risikofrüherkennungssystems	321	680

		Seite	Randnummer
§ 3	**Basel II und IT-Anforderungen bei Banken**	322	681

13. Kapitel: Branchenspezifische Aspekte

§ 1	**Banken**	323	682–719
I.	Sinn und Zweck der Bankenaufsicht	323	682–683
II.	Vorgaben des KWG für die IT-Sicherheit	324	684–709
	1. Sicherheitsvorkehrungen für die EDV	325	687–692
	2. Interne Kontrollverfahren	328	693–698
	2.1 Internes Kontrollsystem	328	694–695
	2.2 Interne Revision	329	696–698
	3. Dokumentation der ausgeführten Geschäfte	331	699
	4. Outsourcing durch die Bank	331	700–709
III.	Maßnahmen bei Verstößen gegen § 25a KWG	335	710–719
	1. Vorrangige Maßnahmen	335	711–717
	1.1 Auskunftsersuchen der BaFin	335	711
	1.2 Sonderprüfung	336	712–715
	1.3 Anordnung organisatorischer Maßnahmen	337	716
	1.4 Einschränkung der Betriebserlaubnis	337	717
	2. Maßnahmen als letztes Mittel	337	718–719
§ 2	**Krankenhäuser**	338	720
I.	Ärztliche Schweigepflicht	338	721–724
II.	Datenschutzrechtliche Vorgaben für die Sicherheit von Patientendaten	340	725–732

14. Kapitel: Fazit

Teil II:

Technische und organisatorische Aspekte der IT-Sicherheit

15. Kapitel: Die Berücksichtigung der Informationssicherheit im Unternehmen

§ 1	**Grundbegriffe**	351	734–745
§ 2	**Schaffung der organisatorischen Voraussetzungen**	354	746–754
I.	Rahmenbedingungen	354	746
II.	Aufgaben des IT-Sicherheitsmanagements	354	747
III.	Wahrnehmen von Aufgaben des IT-Sicherheitsmanagements	355	748
IV.	Notwendige Voraussetzungen	355	749
V.	Aufbau einer IT-Sicherheitsorganisation	356	750–751
VI.	Rollen und Verantwortlichkeiten	357	752
VII.	Rollenkonflikte	357	753
VIII.	Der IT-Sicherheitsbeauftragte	357	754

		Seite	Randnummer
§ 3	**Das Informationssicherheits-Managementsystem**	358	755–760
I.	Etablieren eines IT-Sicherheitsprozesses	358	755
II.	Gestaltung relevanter Prozesse	358	756–759
III.	Einführung und Aktivierung der Prozesse	359	760
§ 4	**Die Bedeutung der Zertifizierung**	359	761

16. Kapitel: Erstellung, Implementierung und Anpassung eines IT-Sicherheitskonzepts im Unternehmen

§ 1	**Identifikation der Sicherheitsanforderungen**	361	762–768
I.	Erfassung und Einschätzung der Geschäftsprozesse	361	763
II.	Einschätzung der Kritikalität	362	764–768
	1. Erarbeiten eines Bewertungsschemas	362	765–766
	2. Verfahren für die Bewertung der Geschäftsprozesse	363	767–768
§ 2	**Definition der IT-Sicherheitsleitlinie**	363	769–771
I.	Einführung	363	769–770
II.	Form und Aufbau der IT-Sicherheitsleitlinie	364	771
§ 3	**Risikoanalyse**	365	772–773
I.	Detaillierte Untersuchung kritischer Geschäftsprozesse	365	772
II.	Verfahren zur Durchführung von Risikoanalysen	365	773
§ 4	**Maßnahmenplanung**	365	774–867
I.	Die IT-Sicherheitsvorgaben	366	775
II.	Gestaltung von Vorgaben	366	776
III.	Gültigkeit	366	777–779
IV.	Inhalt	367	780
V.	Strategische Ausrichtung der IT-Sicherheit	368	781–788
	1. Zentrale oder dezentrale Ausrichtung der IT-Sicherheitsorganisation	368	782
	2. Einbettung von Standards bei der Konzeption von IT-Sicherheitsmaßnahmen	369	783
	3. Perimeterschutz oder gestaffeltes Sicherheitskonzept	369	784
	4. Technik oder Organisation	370	785
	5. Nutzung von Kryptographie	370	786
	6. Zuweisung von Zuständigkeiten und Verantwortlichkeiten	370	787
	7. Krisenmanagement und Notfallvorsorgekonzept	370	788
VI.	IT-Sicherheitsorganisation	371	789–796

		Seite	Randnummer
	1. Etablierung eines IT-Sicherheitsmanagements	372	791
	2. Einrichtung von Gremien	373	792
	3. Etablieren eines Vorgehens bei IT-Sicherheitsvorfällen	373	793
	4. IT-Sicherheit im Umgang mit Geschäftspartnern und Externen	373	794
	5. Umgang mit Informationen und Betriebsmitteln	373	795
	6. Dokumentation IT-sicherheitsrelevanter Entscheidungen	374	796
VII.	IT-Sicherheit beim Einsatz von internem und externem Personal	374	797–802
	1. Sicherheitsüberprüfung von Mitarbeitern	374	798
	2. IT-Sicherheit in der Aufgabenausübung	374	799
	3. Verpflichtung	375	800
	4. Einarbeitung und Schulung	375	801
	5. Regelungen für Besucher	375	802
VIII.	Infrastruktursicherheit	375	803–807
	1. Definition von Sicherheitszonen	376	804
	2. Schutzmechanismen im Bereich der Infrastruktur	376	805
	3. Vorgaben für die Vergabe und Kontrolle von utrittsrechten	376	806
	4. Vermeidung von Kompromittierung, Diebstahl und Verlust von Ressourcen	376	807
IX.	Sicherheit im Umgang mit Informationen und Informationsmedien	377	808–811
	1. Einführung eines Verfahrens zur Kategorisierung und Kennzeichnung von Informationen	377	809
	2. Festlegung geregelter Abläufe für den Umgang mit Informationen und Informationsträgern	377	810
	3. Schutz von Informationen beim Austausch mit Externen	377	811
X.	IT-Sicherheit in der Telekommunikation	378	812–815
	1. Sicherheit im Betrieb von TK-Anlagen	378	813
	2. Restriktive Wartungs- und Zugriffsregelung für Telekommunikationseinrichtungen	378	814
	3. Nutzung von Authentisierungs- und Autorisierungsmechanismen	378	815
XI.	Authentisierung und Zugriffskontrolle	378	816–819
	1. Anforderungen für die Zugriffskontrolle und Einführung von Berechtigungsvergabeverfahren	378	816

		Seite	Randnummer
	2. Prüfung der Aktualität und Rechtmäßigkeit vergebener Berechtigungen	379	817
	3. Implementierung von Authentisierungsmechanismen	379	818
	4. Umgang mit Authentisierungsmitteln	379	819
XII.	Einsatz kryptographischer Verfahren und digitaler Signaturen	379	820–823
	1. Definition von Anforderungen an kryptographische Verfahren	380	821
	2. Auswahl und Einsatz kryptographischer Verfahren	380	822
	3. Etablierung von Vorgehensweisen zum Schlüsselmanagement	380	823
XIII.	Notfallvorsorge	381	824–828
	1. Etablierung eines Vorgehens zur Notfallvorsorge	381	825
	2. Erstellung und Umsetzung von Notfallplänen	381	826
	3. Regelmäßige Tests des Vorgehens bei Notfällen	382	827
	4. Priorisierung und Redundanz	382	828
XIV.	Aufbau von Netzen	382	829–832
	1. Planung des Netzes	382	830
	2. Sicherheit von Netzkoppelelementen	382	831
	3. Sicherheit und Netzmanagement	382	832
XV.	Absicherung von Außenanbindungen	383	833–837
	1. Etablierung von Maßnahmen zur Gewährleistung der Sicherheit des internen Netzes	383	834
	2. Kontrolle der Nutzung externer Netze und Dienste	383	835
	3. Nutzung von Authentisierungs- und Autorisierungsmechanismen	384	836
	4. VPNs und Verschlüsselung	384	837
XVI.	Systemsicherheit	384	838–843
	1. Schutz des Betriebssystems und der Systemdateien	384	839
	2. Etablierung eines Vorgehens zur Kontrolle von Systemänderungen	385	840
	3. Umsetzung von Schutzmechanismen gegen Viren/Schadsoftware	385	841
	4. Verfahren zur System- und Softwarepflege	385	842
	5. Sicherheit und Systemmanagement	385	843
XVII.	Anwendungssicherheit	385	844–847
	1. Reduktion von Zugriffsmöglichkeiten auf Anwendungen und Anwendungsdaten	385	845
	2. Sicherheit in der Anwendungsbetreuung	386	846

		Seite	Randnummer
	3. Sorgfalt und Kontrolle der Benutzung	386	847
XVIII.	IT-Sicherheit in der Entwicklung und Beschaffung	386	848–853
	1. IT-Sicherheitsanforderungen an die Entwicklung und Beschaffung	386	849
	2. Geregelter Entwicklungs- und Integrationsprozess	387	850
	3. Etablierung von Regeln für die Softwareentwicklung durch Externe	387	851
	4. Dokumentation der Entwicklung	387	852
	5. Etablierung eines Zertifizierungsprozesses	387	853
XIX.	IT-Sicherheit bei der Installation und im IT-Betrieb	387	854–857
	1. Dokumentation der Betriebsprozesse	388	855
	2. Umsetzung von IT-Sicherheitsanforderungen an die Installation und den Betrieb	388	856
	3. Datensicherungskonzept	388	857
XX.	IT-Sicherheitsüberwachung	388	858–860
	1. Protokollierung von IT-sicherheitsrelevanten Ereignissen	389	859
	2. Präventiverkennung IT-sicherheitsrelevanter Schwachstellen	389	860
XXI.	Einhaltung IT-sicherheitsrelevanter Vorgaben	389	861–864
	1. Identifikation relevanter Gesetze und Regelungen	389	861
	2. Berücksichtigung des Rechts an geistigem Eigentum, Lizenzrecht	389	862
	3. Berücksichtigung von Regulierungen zur Kryptographie	389	863
	4. Sammlung von Beweisen zu IT-Sicherheitsverstößen	390	864
XXII.	IT-Sicherheitsaudit und IT-Sicherheitsrevision	390	865–867
	1. Überprüfung der Einhaltung von IT-Sicherheitsbestimmungen	390	866
	2. Durchführung von IT-Sicherheitsaudits	391	867
§ 5	**Definition von Maßnahmen**	391	868
I.	Einbeziehung des IT-Sicherheitsmanagements	391	869
II.	Zuständigkeiten	392	870
III.	Konzeption notwendiger IT-Sicherheitsmaßnahmen	392	871–878
	1. Aufnahme des IT-Umfelds	392	872
	2. Zutreffende IT-Sicherheitsvorgaben	393	873
	3. Feststellen der Gefährdungsexposition	393	874
	4. Festlegen geeigneter IT-Sicherheitsmaßnahmen	394	875–878

		Seite	Randnummer
	4.1 Erstellung von Maßnahmenkatalogen	394	875–877
	4.2 Struktur der Maßnahmenkataloge	395	878
IV.	Alternative Vorgehensweisen	395	879
V.	Prüfung	395	880
§ 6	**Implementierung von Maßnahmen**	396	881–903
I.	Zielsetzung des Projektvorgehens	396	882
II.	Überblick über das Projektvorgehen	396	883–886
	1. Beschaffung und Entwicklung	396	884
	2. Integration	397	885
	3. Betrieb	397	886
III.	Abnahme	397	887
IV.	Mitwirkung des IT-Sicherheitsmanagements	397	888
V.	Steuerungselemente	397	889–899
	1. Definition des Projektziels	397	890
	2. Ressourceneinsatz	398	891
	3. Zeitplanung	398	892
	4. Budgetverantwortung	398	893
	5. Qualitätssicherung	398	894
	6. Kommunikation	398	895
	7. Projektrisiken	398	896
	8. Asset Management	398	897
	9. Change Management	399	898
	10. Problem Management/Fault Management	399	899
VI.	Prüfung der Implementierung	399	900–903
	1. Kontrollen für die Projektphase Beschaffung und Implementierung:	400	901
	2. Kontrollen für die Projektphase Integration:	400	902
	3. Kontrollen für die Projektphase Betrieb:	400	903
§ 7	**Überwachung von IT-Sicherheitsmaßnahmen**	401	904–907
I.	Kontrollfragen	401	905
II.	Revisionsleitlinie	402	906
III.	Revisionsbericht	402	907
§ 8	**Kontinuierliche Verbesserung der IT-Sicherheitsmaßnahmen**	402	908–912
I.	Bestimmung von Ursachen bereits aufgetretener Fehler	402	909
II.	Identifizierung potentieller Fehler und deren möglicher Ursachen	402	910
III.	Korrektur und Testing	402	911
IV.	Kommunikation der Ergebnisse	403	912
Literaturverzeichnis		405	
Rechtsprechungsverzeichnis		411	
Stichwortverzeichnis		413	