

# Recht der IT-Sicherheit

von

Prof. Dr. Bernd Holznel, Lars Dietze, Stephanie Kussel, Matthias Sonntag

1. Auflage

[Recht der IT-Sicherheit – Holznel / Dietze / Kussel / et al.](#)

schnell und portofrei erhältlich bei [beck-shop.de](http://beck-shop.de) DIE FACHBUCHHANDLUNG

Thematische Gliederung:

[Informationsrecht, Neue Medien](#)



Verlag C.H. Beck München 2003

Verlag C.H. Beck im Internet:

[www.beck.de](http://www.beck.de)

ISBN 978 3 406 49545 8

## Inhaltsübersicht

Vorwort . . . . .	V
Inhaltsverzeichnis . . . . .	IX
Abbildungsverzeichnis . . . . .	XIX
Abkürzungsverzeichnis . . . . .	XXI
<b>Erster Teil. Grundlagen . . . . .</b>	<b>1</b>
§ 1. Einführung . . . . .	1
§ 2. Was ist IT-Sicherheit? . . . . .	11
§ 3. Bedrohungen der IT-Sicherheit . . . . .	16
§ 4. Instrumente zur Verbesserung der IT-Sicherheit . . . . .	28
<b>Zweiter Teil. Bausteine der IT-Sicherungsinfrastruktur . . . . .</b>	<b>49</b>
§ 5. Elektronische Signaturen . . . . .	49
§ 6. Verschlüsselung zum Schutz der Vertraulichkeit . . . . .	87
<b>Dritter Teil. Sanktionierung von Angriffen auf die IT-Infrastruktur . . . . .</b>	<b>103</b>
§ 7. Strafrechtlicher Schutz der IT-Sicherheit . . . . .	103
<b>Vierter Teil. Fernmeldegeheimnis und Datenschutz . . . . .</b>	<b>135</b>
§ 8. Fernmeldegeheimnis und Überwachung der Telekommunikation . . . . .	135
§ 9. Datenschutz im Bereich der Informationstechnologien . . . . .	166
<b>Fünfter Teil. Ausgewählte Anwendungsbereiche . . . . .</b>	<b>199</b>
§ 10. E-Democracy ( <i>Anika Hanßmann</i> ) . . . . .	199
§ 11. E-Government ( <i>Christoph Werthmann</i> ) . . . . .	216
Sachverzeichnis . . . . .	231

**beck-shop.de**

## Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Inhaltsverzeichnis	IX
Abbildungsverzeichnis	XIX
Abkürzungsverzeichnis	XXI
<b>Erster Teil. Grundlagen</b>	<b>1</b>
§ 1. Einführung	1
I. Chancen und Risiken der IT	1
II. Entwicklungen der Informations- und Rechnertechnik	4
1. Rechnertechnik	4
2. Telekommunikationstechnik	5
3. Internet	6
III. Nutzungsmöglichkeiten	7
IV. Sicherheitsvorfälle	8
V. Gang der Darstellung	9
§ 2. Was ist IT-Sicherheit?	11
I. Begriffsbestimmungen	11
1. Rechtliche Definition	11
2. Technische Definitionen	11
II. Schutzziele	12
1. Einleitung	12
2. Schutz der Verfügbarkeit	13
3. Schutz der Integrität	13
4. Schutz der Vertraulichkeit	13
5. Schutz der Authentizität	14
6. Qualitätsprüfung und -bestätigung	14
7. Schutz des informationellen Selbstbestimmungsrechts	14
8. Interdependenzen der IT-Sicherheitsziele	15
§ 3. Bedrohungen der IT-Sicherheit	16
I. Aufbau von IT-Systemen	16
1. Betriebssystem	16
2. Rechnernetze	17
II. Risiken für die IT-Sicherheit	19
1. Unbeabsichtigte Störungen	19
2. Beabsichtigte Angriffe	20
a) Aktive Angriffe	21
aa) Trojanische Pferde	21
bb) Viren	22

cc) Würmer	23
dd) Maskerade	23
ee) Denial of Service-Attacken	24
ff) Buffer-Overrun	24
b) Passive Angriffe	25
c) Zusammenfassende Übersicht über die Gefahrenquellen	25
d) Externe und interne Täter	26
§ 4. Instrumente zur Verbesserung der IT-Sicherheit	28
I. Technische Lösungsansätze	29
1. Einleitung	29
2. Maßnahmen zur Rechnersicherheit	29
3. Verschlüsselung	30
4. Elektronische Signaturen	30
5. Anonymisierung	31
6. Firewalls	32
7. Intrusion Detection Systeme	32
8. Anti Viren-Programme	33
9. Chipkarten	33
10. Biometrie	34
11. Sonstige Schutzmaßnahmen	34
12. Zusammenfassung	34
II. Rechtliche Lösungsansätze	35
1. Hoheitliche Maßnahmen	35
a) Zielvorgaben und Sicherheitsstandards	35
b) Ordnungsrechtliche Kontrollinstrumente	36
c) Ordnungsrechtliche Verhaltenspflichten	36
d) Sanktionen bei mangelnder Normbefolgung	36
aa) Strafrecht	36
bb) Ordnungswidrigkeitenrecht	37
cc) Haftungsrecht	37
2. Maßnahmen der indirekten Verhaltenssteuerung	37
III. Technische Regelwerke	38
1. Funktion technischer Regelsetzung	38
2. IT-Sicherheitskriterien	39
a) Zielsetzung	39
b) Bedeutsame Kriterienkataloge	39
aa) Nationale IT-Sicherheitskriterien	39
bb) Europäische IT-Sicherheitskriterien	39
cc) Internationale IT-Sicherheitskriterien	40
(1) ISO 15408	40
(2) Common Criteria	40
3. IT-Sicherheitsevaluierung und -zertifizierung in der Praxis	40
4. Rechtliche Wirkung technischer Regelwerke	42
IV. Für die IT-Sicherheit zuständige Behörden	43

1. Bundesamt für Sicherheit in der Informationstechnik . . . . .	43
a) Entstehungsgeschichte . . . . .	43
b) Zielsetzung und Handlungsauftrag . . . . .	44
2. Aufsichtsbehörden für den Datenschutz . . . . .	44
3. Regulierungsbehörde für Telekommunikation und Post . . . . .	45
a) Zuständigkeiten im Bereich der elektronischen Signatur . . . . .	45
b) Zuständigkeiten im Bereich des Datenschutzes . . . . .	46
c) Zuständigkeiten im Bereich der Telekommunikations- infrastruktur . . . . .	46
aa) Genehmigungsvorbehalt . . . . .	46
bb) Erstellung eines Sicherheitskatalogs . . . . .	46
cc) IT-spezifische Kontrollbefugnisse . . . . .	47
<b>Zweiter Teil. Bausteine der IT-Sicherungsinfrastruktur . . . . .</b>	<b>49</b>
§ 5. Elektronische Signaturen . . . . .	49
I. Einleitung . . . . .	49
II. Technische Grundlagen . . . . .	50
III. Rechtliche Rahmenbedingungen für elektronische Signaturen . . . . .	52
IV. Rechtsrahmen für den Einsatz elektronischer Signaturen (SigG/SigV) . . . . .	54
1. Hierarchieebenen für elektronische Signaturen . . . . .	55
a) Einfache Signaturen . . . . .	56
b) Fortgeschrittene Signaturen . . . . .	56
c) Qualifizierte Signaturen . . . . .	57
d) Qualifizierte Signaturen mit Anbieter-Akkreditierung . . . . .	58
2. Organisationsstruktur für Zertifizierungsdiensteanbieter . . . . .	59
a) Begriff des Zertifizierungsdiensteanbieters . . . . .	59
b) Einrichtung und Betrieb eines Zertifizierungsdienstes . . . . .	60
aa) Einrichtung . . . . .	60
(1) Personelle Voraussetzungen . . . . .	60
(2) Sachliche Voraussetzungen . . . . .	60
bb) Zertifikatsmanagement . . . . .	61
(1) Ausstellung von Zertifikaten . . . . .	61
(a) Antrag . . . . .	61
(b) Identifizierung . . . . .	62
(c) Schlüsselerzeugung . . . . .	62
(d) Personalisierung . . . . .	62
(e) Zertifizierung . . . . .	62
(f) Unterrichtung des Zertifikatsinhabers . . . . .	63
(g) Nachprüfbarkeit im Zertifikatsverzeichnis . . . . .	64
(2) Verwaltung der Zertifikate . . . . .	64
(a) Dokumentation der Zertifikatsausstellung . . . . .	65

(b) Pflege des Zertifikatsverzeichnisses . . . . .	65
(3) Zertifikatsübergabe bei Betriebseinstellung . . . . .	66
cc) Freiwillige Akkreditierung des Zertifizierungsdiensteanbieters . . . . .	67
(1) Erwerb der Akkreditierung . . . . .	67
(2) Aufhebung der Akkreditierung . . . . .	68
3. Aufsicht über die Zertifizierungsdiensteanbieter . . . . .	69
a) Verwaltungsrechtliches Instrumentarium . . . . .	69
b) Sanktionsmöglichkeiten . . . . .	69
4. Haftung des Zertifizierungsdiensteanbieters . . . . .	70
a) Haftung gegenüber dem Zertifikatsinhaber . . . . .	71
b) Haftung gegenüber Dritten . . . . .	71
c) Deckungsvorsorge für den Haftungsfall . . . . .	72
5. Sichere technische Produkte . . . . .	72
a) Sichere Signaturerstellungseinheiten . . . . .	73
b) Sichere Signaturanwendungskomponenten . . . . .	75
6. Akzeptanz ausländischer elektronischer Signaturen . . . . .	75
V. Rechtswirkungen elektronischer Signaturen . . . . .	78
1. Gleichstellung mit der eigenhändigen Unterschrift . . . . .	78
a) Formanpassung im Privatrecht . . . . .	78
b) Formanpassung im Öffentlichen Recht . . . . .	79
aa) Schriftformerfordernisse im öffentlichen Bereich . . . . .	79
bb) Änderung des VwVfG . . . . .	80
(1) Generalklausel des § 3a . . . . .	80
(2) Anforderungen an elektronische Verwaltungsakte . . . . .	80
2. Qualifiziert signierte Dokumente als Beweismittel . . . . .	81
a) Beweismittelqualität qualifiziert signierter Dokumente . . . . .	81
b) Beweiswert qualifiziert signierter Dokumente . . . . .	82
VI. Ausblick . . . . .	83
§ 6. Verschlüsselung zum Schutz der Vertraulichkeit . . . . .	87
I. Einleitung . . . . .	87
II. Technische Grundlagen . . . . .	88
1. Funktionsweise von Verschlüsselungsverfahren . . . . .	88
2. Symmetrische Verschlüsselung . . . . .	90
3. Asymmetrische Verschlüsselung . . . . .	90
4. Praktische Umsetzung . . . . .	91
III. Krypto-Debatte . . . . .	92
1. Regulierungsoptionen . . . . .	92
a) Verbot der Nutzung von Verschlüsselungstechniken für Private . . . . .	92
b) Key Recovery . . . . .	93
c) Key Escrow . . . . .	94
d) Verzicht auf jegliche gesetzliche Beschränkung . . . . .	94
2. Aktuelle Regulierungsansätze . . . . .	94

a) Eckwertepapier zur deutschen Krypto-Politik . . . . .	94
b) Strafrechtliche Sanktionierung der Verschlüsselung . . . . .	95
c) Entschlüsselungspflichten . . . . .	96
d) EU Krypto-Politik . . . . .	96
e) Internationale Krypto-Politik . . . . .	97
IV. Import-/Exportkontrollen . . . . .	98
1. Wassenaar Arrangement . . . . .	98
2. EU Dual Use-Verordnung . . . . .	99
a) Genehmigungspflicht einer Ausfuhr . . . . .	99
b) Zweistufige Prüfung . . . . .	100
c) Genehmigungsverfahren . . . . .	101
<b>Dritter Teil. Sanktionierung von Angriffen auf die IT-Infrastruktur</b>	<b>103</b>
§ 7. Strafrechtlicher Schutz der IT-Sicherheit . . . . .	103
I. Einleitung . . . . .	103
II. Delikte zum Schutz des Tatobjekts „Daten“ . . . . .	106
1. Ausspähen von Daten . . . . .	106
a) Tatobjekt: Daten . . . . .	107
b) Besondere Dateneigenschaften . . . . .	107
c) Taterfolg: Sich oder einem anderen verschaffen . . . . .	108
d) Sonderproblem: Hacking . . . . .	108
2. Datenveränderung . . . . .	109
a) Tatobjekt: Daten . . . . .	109
b) Tathandlungen . . . . .	110
3. Computersabotage . . . . .	111
a) Tatobjekt: Datenverarbeitung . . . . .	111
b) Besonderes Merkmal: Von wesentlicher Bedeutung . . . . .	111
c) Verursachung einer Störung . . . . .	111
4. Fälschung beweisheblicher Daten . . . . .	112
a) Tatobjekt: Daten . . . . .	113
b) Besonderes Merkmal: Beweiserheblichkeit . . . . .	114
c) Tathandlungen . . . . .	114
d) Täuschungsabsicht . . . . .	114
5. Unterdrücken beweisheblicher Daten . . . . .	115
a) Besonderes Merkmal: Beweisführungsbefugnis . . . . .	115
b) Nachteilszufügungsabsicht . . . . .	116
III. Delikte zum Schutz des Tatobjekts „Technische Aufzeichnung“ . . . . .	116
1. Fälschung technischer Aufzeichnungen . . . . .	116
a) Tatobjekt: Technische Aufzeichnung . . . . .	117
b) Besonderes Merkmal: Unecht . . . . .	117
c) Tathandlungen . . . . .	118
d) Täuschungsabsicht . . . . .	118
2. Unterdrücken technischer Aufzeichnungen . . . . .	119



a) Tatobjekt: Dem Täter nicht gehörende technische Aufzeichnung . . . . .	119
b) Tathandlung . . . . .	119
c) Nachteilszfügungsabsicht . . . . .	120
IV. Fernmeldegeheimnis und Datenschutzstrafrecht . . . . .	120
1. Verletzung des Fernmeldegeheimnisses . . . . .	120
a) Tathandlung: Mitteilung über Tatsachen . . . . .	121
b) Fernmeldegeheimnis . . . . .	121
c) Unbefugt . . . . .	122
d) Rechtswidrigkeit . . . . .	122
e) Unterdrücken der Sendung . . . . .	123
2. Datenschutzstrafrecht . . . . .	123
V. Sonstige Schutzgüter . . . . .	125
1. Computerbetrug . . . . .	125
a) Tathandlungen . . . . .	126
b) Täterfolg . . . . .	126
c) Subjektiver Tatbestand . . . . .	127
2. Störung von Telekommunikationsanlagen . . . . .	127
a) Telekommunikationsanlagen . . . . .	127
b) Täterfolg . . . . .	128
c) Subjektiver Tatbestand . . . . .	128
VI. Cybercrime-Convention . . . . .	128
1. Rechtswidriger Zugriff . . . . .	129
2. Rechtswidriges Abfangen . . . . .	129
3. Eingriffe in Daten . . . . .	130
4. Eingriffe in das System . . . . .	130
5. Missbrauch von Vorrichtungen . . . . .	130
6. Computerurkundenfälschung . . . . .	131
7. Computerbetrug . . . . .	132
<b>Vierter Teil. Fernmeldegeheimnis und Datenschutz . . . . .</b>	<b>135</b>
§ 8. Fernmeldegeheimnis und Überwachung der Telekommunikation . . . . .	135
I. Verfassungsrechtliche Grundlagen . . . . .	136
1. Schutzbereich . . . . .	136
2. Schranken des Fernmeldegeheimnisses . . . . .	137
II. Überwachung durch Strafverfolgungsbehörden . . . . .	137
1. Überwachung der Inhalts- und Verbindungsdaten . . . . .	137
a) Zu überwachender Personenkreis . . . . .	138
b) Straftatenkatalog . . . . .	138
c) Anordnungsbefugnis . . . . .	140
d) Verpflichtetenkreis . . . . .	141
e) Verwertung von Zufallsfunden . . . . .	141
f) Eingeschränkte Rechtsschutzmöglichkeit . . . . .	141

g) Erweiterung auf Verbindungsdaten aktiv geschalteter Handys	142
2. Überwachung der Verbindungsdaten	142
a) Verbindungsdaten	142
b) Bedeutung der Verbindungsdaten	143
c) Zielwahlsuche	144
d) Funkzellenabfrage	144
3. Überwachung des Standorts, Ermittlung der Geräte- und Kartennummer	145
a) Rechtliche Voraussetzungen	145
b) IMSI-Catcher	145
III. Fernmeldeüberwachung durch Geheimdienste	147
1. Überwachung der Inhaltsdaten in Einzelfällen	147
a) Anordnungsbefugnis	148
b) Eingeschränkte Rechtsschutzmöglichkeiten	148
2. Überwachung der Verbindungsdaten	149
3. Strategische Beschränkungen	150
4. Überwachung der Bewegungsdaten	150
IV. Überwachung durch Zollkriminalämter	150
V. Abfrage der Bestandsdaten	152
1. Auskunftersuchen im Einzelfall	152
2. Automatisierte Auskunftserteilung	154
VI. Mitwirkungspflichten der TK-Anbieter	155
1. Anforderungen des § 88 TKG	155
2. Ausgestaltung durch die TKÜV	157
a) Pflichtenkatalog	157
b) Beschränkung des Pflichtenkatalogs	158
c) Befreiung vom Pflichtenkatalog	159
VII. Internationale Überwachungsvorschriften	160
1. Cybercrime-Convention	160
2. Europäisches Rechtshilfeabkommen	162
VIII. Zusammenfassung	163
§ 9. Datenschutz im Bereich der Informationstechnologien	166
I. Einleitung	166
II. Einführung in das Datenschutzrecht	167
1. Das Recht auf informationelle Selbstbestimmung	167
a) Schutzbereich	167
b) Eingriff und Rechtfertigung	168
c) Mittelbare Drittwirkung	168
2. Der deutsche Rechtsrahmen für den Datenschutz	169
a) Die Regelungsstruktur des Datenschutzrechts	169
b) Die Grundstruktur des BDSG	170
aa) Anwendungsbereich	170
(1) Personenbezogene Daten	170

(2) Erfasste Verarbeitungsphasen . . . . .	172
(3) Adressatenkreis . . . . .	172
(a) Öffentliche Stellen . . . . .	172
(b) Nicht-öffentliche Stellen . . . . .	173
bb) Grundregel der Datenverarbeitung . . . . .	173
(1) Gesetzliche Erlaubnisnormen . . . . .	174
(2) Einwilligung . . . . .	175
cc) Datenschutzrechte des Betroffenen . . . . .	175
(1) Kontrollrechte . . . . .	175
(2) Schadensersatz . . . . .	176
dd) Sicherung des Datenschutzes . . . . .	177
(1) Aufsicht und Sanktionen . . . . .	177
(2) Maßnahmen der Datensicherung . . . . .	178
II. Datenschutz im Bereich der Informations- und Kommunika- tionsmedien . . . . .	180
1. Anwendbares Recht . . . . .	180
a) Abgrenzung der Datenebenen . . . . .	181
b) Abgrenzung der Dienstekategorien . . . . .	182
2. Zulässigkeit der Datenverarbeitung bei Telediensten . . . . .	184
a) Bestandsdaten . . . . .	184
aa) Begriff . . . . .	184
bb) Zulässiges Maß der Datenerhebung, -verarbeitung und -nutzung . . . . .	184
b) Nutzungsdaten . . . . .	185
aa) Begriff . . . . .	185
bb) Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung . . . . .	185
cc) Sonderproblem: Erstellung von Persönlichkeits- profilen . . . . .	186
c) Inhaltsdaten . . . . .	186
d) Zusammenfassung . . . . .	186
3. Datenschutzpflichten der Diensteanbieter . . . . .	188
a) Organisatorische und technische Schutzmaßnahmen . . . . .	188
aa) Jederzeitiger Verbindungsabbruch . . . . .	188
bb) Schutz gegen Kenntnisnahme Dritter . . . . .	188
cc) Getrennte Datenverarbeitung . . . . .	189
dd) Anzeige der Weitervermittlung . . . . .	189
ee) Anonyme oder pseudonyme Dienstenutzung und -bezahlung . . . . .	190
b) Informationspflichten . . . . .	191
aa) Datenschutzhinweis . . . . .	191
(1) Gegenstand der Unterrichtung . . . . .	191
(2) Zeitpunkt der Unterrichtung . . . . .	191
(3) Pflicht jederzeitiger Abrufbarkeit . . . . .	192

bb) Auskunftspflichten . . . . .	192
(1) Gegenstand der Auskunftserteilung . . . . .	193
(2) Verfahren der Auskunftserteilung . . . . .	193
c) Zusammenfassung . . . . .	193
4. Die Sicherung des Datenschutzes . . . . .	195
a) Aufsicht und Sanktionen . . . . .	195
b) Datenschutzaudit . . . . .	195
IV. Ausblick . . . . .	196
<b>Fünfter Teil. Ausgewählte Anwendungsbereiche . . . . .</b>	<b>199</b>
§ 10. E-Democracy . . . . .	199
I. Einleitung . . . . .	199
II. Bundestagswahlen per Internet . . . . .	200
1. Derzeitige Rechtslage . . . . .	200
a) Stimmabgabe mittels Wahlgerät . . . . .	200
b) Briefwahl . . . . .	201
2. Verfassungsrechtliche Anforderungen . . . . .	201
a) Allgemeinheit der Wahl . . . . .	201
b) Wahlfreiheit und Wahlgeheimnis . . . . .	202
aa) Einsatz asymmetrischer Kryptographie . . . . .	202
bb) Zusätzlicher Einsatz elektronischer Signaturen . . . . .	203
(1) Funktionsweise . . . . .	203
(2) Rechtliche Voraussetzungen . . . . .	203
cc) MIX-Modell . . . . .	204
dd) Einsatz blinder Signaturen . . . . .	206
ee) Zusammenfassung . . . . .	207
c) Gleichheit der Wahl . . . . .	209
d) Unmittelbarkeit der Wahl . . . . .	209
3. Plädoyer für ein Erprobungsgesetz . . . . .	210
a) Verfassungspolitische Abwägung . . . . .	210
b) Sicherheitstechnische Abwägung . . . . .	210
c) Zusammenfassung . . . . .	210
III. Weitere Einsatzmöglichkeiten von Internet-Wahlen . . . . .	211
IV. Online-Bürgerbeteiligung bei staatlichen Entscheidungs- prozessen . . . . .	212
1. Bürgerbeteiligung in Planungsprozessen . . . . .	212
2. Gesetzgebungsverfahren . . . . .	213
V. Zusammenfassung . . . . .	214
§ 11. E-Government . . . . .	216
I. Einleitung . . . . .	216
II. Online-Transaktionsdienste in der Praxis . . . . .	219
1. Geeignete Verwaltungsvorgänge . . . . .	219
2. Mehrwert für den Bürger . . . . .	220

XVIII	<i>Inhaltsverzeichnis</i>	
	3. Hürden	220
	4. Pilotprojekte	221
III.	Rechtliche Möglichkeiten und Grenzen	221
	1. Verwaltungsverfahren ohne besondere Formerfordernisse	221
	2. Schriftformerfordernis	222
	a) Bürger	222
	b) Verwaltung	222
	aa) Voraussetzungen für das Ersetzen des Schriftform- erfordernisses	223
	(1) Sicherstellung der Identität	223
	(2) Sicherstellung der Unversehrtheit	223
	(3) Sicherstellung des Beweiswertes	223
	(4) Warn-, Aufklärungs- und Schutzfunktion	224
	bb) Zusammenfassung	224
	3. Erfordernis der persönlichen Anwesenheit	225
	4. Bekanntgabe von Verwaltungsakten	225
	5. Nichtöffentlichkeit des Verwaltungsverfahrens	226
	6. Aktenführung und Archivierung	227
IV.	Elektronische Vergabe öffentlicher Aufträge	228
V.	Zusammenfassung	229
	Sachverzeichnis	231