

Horst Speichert

Praxis des IT-Rechts

Mit der allgegenwärtigen Computertechnik ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes> – Die Zeitschrift für Informations-Sicherheit (s. a. www.kes.info), die seit 1985 im SecuMedia Verlag erscheint. Die <kes> behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz.

IT-Sicherheit – Make or Buy

Von Marco Kleiner, Lucas Müller und Mario Köhler

Mehr IT-Sicherheit durch Pen-Tests

Von Enno Rey, Michael Thumann und Dominick Baier

Der IT Security Manager

Von Heinrich Kersten und Gerhard Klett

ITIL Security Management realisieren

Von Jochen Brunnstein

IT-Risiko-Management mit System

Von Hans-Peter Königs

IT-Sicherheit kompakt und verständlich

Von Bernhard C. Witt

Praxis des IT-Rechts

Von Horst Speichert

Horst Speichert

Praxis des IT-Rechts

**Praktische Rechtsfragen
der IT-Sicherheit
und Internetnutzung**

Herausgegeben von Stephen Fedtke

2., aktualisierte und erweiterte Auflage

Mit 12 Abbildungen



Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <<http://dnb.d-nb.de>> abrufbar.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne von Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

Das in diesem Werk enthaltene Programm-Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor übernimmt infolgedessen keine Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

1. Auflage 2004

2., aktualisierte und erweiterte Auflage Mai 2007

Alle Rechte vorbehalten

© Friedr. Vieweg & Sohn Verlag | GWV Fachverlage GmbH, Wiesbaden 2007

Lektorat: Sybille Thelen | Andrea Broßler

Der Vieweg Verlag ist ein Unternehmen von Springer Science+Business Media.

www.vieweg.de



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Konzeption und Layout des Umschlags: Ulrike Weigel, www.CorporateDesignGroup.de

Umschlagbild: Nina Faber de.sign, Wiesbaden

Druck- und buchbinderische Verarbeitung: MercedesDruck, Berlin

Printed in Germany

ISBN 978-3-8348-0112-8

Vorwort 2. Auflage

Die zweite, aktualisierte und erweiterte Auflage wurde ergänzt durch aktuelle Problemstellungen wie etwa Phishing, Voice over IP, https-Scanning oder die neuen Rundfunkgebühren auf Computer. Das Recht der Informationssicherheit ist stark im Fluss und entwickelt sich permanent weiter. Auch der Gesetzgeber erlässt fortlaufend neue Bestimmungen, die einzuarbeiten waren. Zuletzt das neue Telemediengesetz oder das Gesetz über elektronische Handelsregister, das nun auch in E-Mails die Pflichtangaben der Geschäftsbriefe vorschreibt. Vieles davon ist stark umstritten, z.B. die neue Strafbarkeit der Hackertools gemäß § 202c StGB. Das Risikomanagement mit Basel II und Sarbanes Oxley wird vertieft dargestellt, da SOX über EU-Richtlinien auch nach Deutschland kommen wird. Neue Standards für Informationssicherheit und Zertifizierung nach ISO 2700x wurden ergänzt. Auch die zweite Auflage gibt dem Leser wieder zahlreiche Musterbeispiele und praktische Orientierungshilfen für die rechtlichen Probleme im IT-Bereich. Neu aufgenommen wurde auf vielfachen Wunsch ein IT-Rechts-Leitfaden für den Schnellüberblick.

Stuttgart, im Mai 2007

Horst Speichert

Vorwort 1. Auflage

Zunehmend durchdringt die Informationstechnologie alle Lebens- und Arbeitsbereiche, so dass mit Recht von einer revolutionären Entwicklung gesprochen wird. Für das IT-Recht ergibt sich zwangsläufig ein ausgeprägter Querschnittscharakter. Der aufzuspannende Bogen reicht vom allgemeinen Teil des Bürgerlichen Rechts, über weite Felder des Arbeits- und Wirtschaftsrechts bis hin zu straf- und öffentlich-rechtlichen Themen, etwa wenn es um Datenschutzfragen geht. Das IT-Recht sprengt die sonst übliche Dreiteilung des Rechtslebens in Zivil-, Straf- und Öffentliches Recht und lässt sich kaum in einem klar umgrenzten Rechtsgebiet fassen. Es insgesamt darstellen zu wollen, erscheint angesichts der Breite der Disziplin als gewaltige Aufgabe. Praxisnahe Auswahl der Themen und Beschränkung auf das Wesentliche taten deshalb Not. Dabei konnte gewinnbringend auf eine langjährige Seminar- und Vortragstätigkeit vor den Praktikern der IT zurückgegriffen werden. Die hierbei aufgeworfenen vielfältigen Fragen sind zugleich Fundus und Fokus der vorliegenden Darstellung.

Die Entwicklung in der IT befindet sich ständig im Fluss. Noch längst nicht sind die technischen und organisatorischen Rahmenbedingungen zu greifbaren Formen erstarrt. Eine rechtsdogmatische Durchdringung der IT insgesamt erscheint im Moment nur schwer möglich. Nichts desto trotz benötigt die Praxis die notwendigen Spielregeln, um effektiv arbeiten zu können. Nirgendwo wird das deutlicher als im Bereich der IT-Sicherheit, wo die technische Entwicklung aufgrund der ausgeprägten Gefährdungslage weit fortgeschritten ist. Die aufgeworfenen Rechtsfragen – insbesondere zu Haftung und Datenschutz – führen in Unternehmen und Behörden zu großer Verunsicherung. Hier will das Buch durch die Darstellung der juristischen Zusammenhänge praktische Lösungswege aufzeigen.

Das Buch wendet sich an all diejenigen, welche als Entscheidungsträger, Techniker, Juristen oder Studierende mit dem IT-Recht praxisnah umgehen wollen. Um Kosten und Umfang des Buches überschaubar zu halten, wurde auf den Abdruck der zahlreichen gesetzlichen Vorschriften im Anhang verzichtet. Stattdessen stehen die für den IT-Sektor einschlägigen Gesetze und Verordnungen unter www.speichert.de unter dem Stichwort

„Internetservice“ zum Aufruf und Download bereit. Ich bin für Hinweise und Verbesserungsvorschläge sowohl aus dem technischen wie auch aus dem juristischen Umfeld stets dankbar und unter der Adresse Mailadresse horst@speichert.de zu erreichen.

Zu Beginn mag der interdisziplinäre Charakter aus Technik und Recht dem Nichtjuristen und Juristen gleichermaßen Schwierigkeiten bereiten. Soweit möglich, wird deshalb auf rechtsdogmatische Detailtiefe und überladene Begrifflichkeiten zu Gunsten einer verständlichen Darstellung verzichtet. Wer die Anfangshürden überwunden hat, dem eröffnet sich mit dem IT-Recht nicht nur ein spannendes Rechtsgebiet, sondern die schillernde Welt der neuen Medien.

Stuttgart, im September 2004

Horst Speichert

Inhaltsverzeichnis

1	Verträge im elektronischen Geschäftsverkehr.....	1
1.1	Vertragsschluss im Netz.....	1
1.1.1	Angebot und Annahme	1
1.1.2	Beweisschwierigkeiten	3
1.1.3	Zugang der Willenserklärungen, insbesondere von E-Mails.....	8
1.1.4	Fazit.....	13
1.2	Online-AGB.....	13
1.2.1	Kriterien wirksamer Einbeziehung	14
1.2.2	Einbeziehungsnachweis	15
1.2.3	Gesetzliche Inhaltskontrolle	16
1.2.4	Besonderheiten bei Unternehmen/Kaufleuten	16
2	Digitale Signatur und elektronische Form.....	19
2.1	Erweiterung der Formvorschriften.....	19
2.2	Probleme des E-Commerce.....	20
2.3	Die elektronische Form	21
2.4	Technische Voraussetzungen nach dem Signaturgesetz	22
2.5	Die Textform.....	23
2.6	Beweisführung mit der elektronischen Form	26
2.7	Übermittlung von Schriftsätzen im Gerichtsverfahren	28
3	Online-Handel.....	31
3.1	Allgemeine Informationspflichten	31
3.1.1	Impressumpflicht	31
3.1.2	Besondere Informationspflichten bei kommerzieller Kommunikation	36
3.1.3	Pflichten im elektronischen Geschäftsverkehr.....	36
3.1.4	Pflichtangaben in E-Mails	37
3.2	Fernabsatzbestimmungen.....	40
3.2.1	Gesetzliche Grundlagen	40

3.2.2	Persönlicher Anwendungsbereich	40
3.2.3	Sachlicher Anwendungsbereich	41
3.2.4	Verhältnis zu anderen Verbraucherschutzbestimmungen.....	44
3.2.5	Spezielle Informationspflichten gegenüber dem Verbraucher	45
3.2.6	Widerrufsrecht.....	47
3.2.7	Beweislast.....	50
3.2.8	Praktische Umsetzung	50
3.3	Rechtsfragen bei Online-Auktionen	53
3.3.1	Verbraucher oder Unternehmer.....	53
3.3.2	Zustandekommen des Vertrages.....	54
3.3.3	Scheingebote	55
3.3.4	Zulässigkeit von Hilfsmitteln.....	56
3.3.5	Minderjährige Geschäftspartner	56
3.3.6	Widerrufsrecht nach Fernabsatzrecht	57
3.3.7	Gewährleistungsansprüche	58
3.3.8	Kollision mit Marken- und Schutzrechten.....	59
3.3.9	Transportrisiko	59
3.3.10	Zahlungsmodalitäten	60
3.3.11	Missbrauchsfälle	61
3.4	Das neue Telemediengesetz (TMG)	62
4	Haftungsfragen	67
4.1	Problemstellung – haftungsrelevante Inhalte.....	67
4.2	Das Haftungsszenario	68
4.3	Die Haftung nach dem TDG.....	70
4.3.1	Gesetzliche Regelung	71
4.3.2	Haftungsprivilegierung	71
4.3.3	Teledienste	72
4.4	Haftung für eigene Inhalte.....	73
4.5	Haftung für Fremdinhalte.....	74
4.5.1	Kenntnis als Voraussetzung	74
4.5.2	Aktive Nachforschung	75
4.5.3	Evidenzhaftung für Schadensersatz	76

4.5.4	Kenntniszurechnung	77
4.5.5	Weisungsverhältnisse	78
4.5.6	Zumutbarkeit der Sperrung	79
4.5.7	Absolute Haftungsprivilegierung	81
4.5.8	Persönliche Haftung von Mitarbeitern	82
4.5.9	Allgemeine Störerhaftung	83
4.6	Verkehrssicherungspflichten und Organisationsverschulden	84
4.7	Haftung für Links	87
4.8	Haftung für Viren	89
4.8.1	Erscheinungsformen	89
4.8.2	Deliktische Ansprüche	91
4.8.3	Umfang der Verkehrspflichten	92
4.8.4	Vertragliche Ansprüche	95
4.8.5	Einwendungen gegen Schadensersatzansprüche	95
4.8.6	Verantwortlichkeit der Mitarbeiter	97
4.9	Haftungsausschlüsse	97
4.9.1	Disclaimer	97
4.9.2	Allgemeine Geschäftsbedingungen	98
4.10	Das IT-Sicherheitskonzept	99
4.10.1	Ganzheitliche IT-Sicherheit	99
4.10.2	Maßnahmen zur Haftungsprävention	102
5	Internetnutzung am Arbeitsplatz	107
5.1	Private oder dienstliche Internetnutzung	107
5.2	Erlaubte oder verbotene Privatnutzung	108
5.2.1	Ausdrückliche Erlaubnis	108
5.2.2	Konkludente Erlaubnis	109
5.2.3	Betriebliche Übung (Betriebsübung)	110
5.2.4	Beseitigung der Erlaubnis	112
5.2.5	Umfang der Erlaubnis	114
5.3	Missbrauch und Pflichtverstöße	116
5.4	Arbeitsrechtliche Sanktionen bei Pflichtverstößen	119
5.4.1	Unverbindlicher Hinweis und Abmahnung	119

5.4.2	Fristgebundene Kündigung	121
5.4.3	Fristlose Kündigung	123
5.4.4	Verdachtskündigung	125
5.5	Zivilrechtliche Folgen – Schadensersatz	126
5.5.1	Schadensersatzpflicht des Arbeitnehmers	126
5.5.2	Haftungsmilderung wegen gefahrgeneigter Tätigkeit	128
5.6	Rundfunkgebühren auf Computer	131
5.6.1	Neuartige Rundfunkgeräte	131
5.6.2	Herkömmliche Rundfunkgeräte	132
5.6.3	GEZ-Filter	133
5.6.4	Gebühren und Zweitgerätebefreiung	133
5.6.5	Verschiedene Standorte	134
5.6.6	Telearbeit, Freiberufler	135
5.6.7	Sanktionen bei Verstoß	136
5.6.8	Fallbeispiele	136
6	Datenschutz und Kontrolle	139
6.1	Datenschutz – Grundbegriffe	139
6.1.1	Datenschutzgesetze	139
6.1.2	Rechtsprechung	140
6.1.3	Personenbezogene Daten	141
6.1.4	Gebot der Zweckbindung	143
6.1.5	Präventives Verbot mit Erlaubnisvorbehalt	143
6.1.6	Datenschutzverletzungen	145
6.1.7	Der Datenschutzbeauftragte	147
6.2	Erlaubte Privatnutzung – Datenschutz nach TK-Recht	151
6.2.1	Grundvoraussetzungen des TKG-Datenschutzes	151
6.2.2	Anwendbarkeit auf den Arbeitgeber	151
6.3	Datenschutzpflicht nach TK-Recht	154
6.3.1	Reichweite des Fernmeldegeheimnisses	155
6.3.2	Zulässige Kontrolle trotz Fernmeldegeheimnis	156
6.3.3	Modifizierende Vereinbarungen	158
6.3.4	TKÜV und Vorratsdatenspeicherung	160

6.4	Anwendbarkeit des Teledienstedatenschutzgesetzes (TDDSG)	162
6.5	Unerlaubte oder dienstliche Nutzung – Datenschutz nach dem Bundesdatenschutzgesetz (BDSG)	164
6.5.1	Anwendungsbereich des BDSG	164
6.5.2	Anwendungsvoraussetzungen des BDSG	165
6.6	Vorgaben und Datenschutzpflichten aus dem BDSG	166
6.6.1	Vertraglicher Zweck.....	167
6.6.2	Das Abwägungsgebot	167
6.6.3	Verhältnismäßigkeitsprinzip	169
6.6.4	Allgemein zugängliche Daten	171
6.6.5	Andere Rechtsvorschriften.....	171
6.6.6	Einwilligung des Betroffenen.....	171
6.6.7	Benachrichtigung, Auskunft, Löschung.....	172
6.7	Datenschutzkonforme Mitarbeiterkontrolle	173
6.8	Richtige Reaktion auf Missbrauch.....	178
6.9	Beweisverwertungsverbote	180
6.10	Rechtliche Gestaltung des Datenschutzes.....	181
6.10.1	Die Betriebs- bzw. Dienstvereinbarung – Voraussetzungen und Wirkung	182
6.10.2	Betriebs- bzw. Dienstvereinbarung für die Internetnutzung – Mitbestimmungsrechte	184
6.10.3	Checkliste: Notwendige Regelungspunkte einer Betriebsvereinbarung	185
6.10.4	Formulierungsbeispiel einer Betriebsvereinbarung	186
7	Rechtmäßige Filtersysteme	203
7.1	Rechtliche Zulässigkeit des Spammings.....	204
7.1.1	Deutsche Rechtslage	204
7.1.2	EU-Rechtslage.....	205
7.1.3	Juristische Abwehrmöglichkeiten.....	206
7.1.4	Wer kann gegen Spammer vorgehen?.....	207
7.1.5	Schadensersatz	207
7.1.6	Gegen wen macht ein Vorgehen Sinn?	208
7.1.7	Kostentragung	209

7.2	Rechtsaspekte des Spam-Filters	209
7.2.1	Reine Markierung.....	210
7.2.2	Mailunterdrückung durch Aussortieren und Löschen	210
7.2.3	Einsichtnahme in den Spamordner.....	213
7.2.4	Verantwortlichkeit des Administrators.....	213
7.2.5	Zugang der „false positives“	214
7.2.6	Kaufmännisches Bestätigungsschreiben	215
7.2.7	Fazit.....	216
7.3	Haftungsfragen des Spamfilters	217
7.3.1	Filterpflicht des E-Mail-Providers	217
7.3.2	Filtern durch den Provider	217
7.3.3	Filtern durch den Empfänger	218
7.3.4	Filterpflicht des Empfängers.....	219
7.4	Rechtliche Leitlinien https-Scanning.....	220
7.4.1	Konstellationen in der Praxis	220
7.4.2	Technisches Verfahren	222
7.4.3	Mögliche Straftatbestände.....	222
7.4.4	Datenschutzrechtliche Zulässigkeit.....	224
7.4.5	Best Practice Beispiel.....	225
8	Anwendbares Recht und Gerichtszuständigkeit.....	227
8.1	Problemstellung	227
8.2	Gerichtsstand im Zivilrecht	228
8.2.1	Wohnsitz und Niederlassung	228
8.2.2	Vertragliche Ansprüche	229
8.2.3	Unerlaubte Handlungen	230
8.3	Anwendbares Recht – unerlaubte Handlungen.....	231
8.3.1	Tatortprinzip und Deliktsstatut	231
8.3.2	Marken- und Domainrecht	233
8.3.3	Wettbewerbsrecht	233
8.3.4	Produkt- oder Produzentenhaftung	235
8.3.5	Datenschutz.....	235
8.4	Anwendbares Recht – Vertragsbeziehungen	236

8.4.1	Rechtswahl	236
8.4.2	Prinzip der engsten Verbindung.....	237
8.4.3	Verbraucherschutz	237
9	Risikomanagement, Standards und Zertifizierung.....	241
9.1	Verpflichtungen zur IT-Sicherheit.....	241
9.1.1	Privat- und Geschäftsgeheimnisse	241
9.1.2	Personenbezogene Daten.....	244
9.2	Risikomanagement nach KonTraG	244
9.2.1	Ziele und Zweck des KonTraG.....	245
9.2.2	Lage- und Risikobericht.....	245
9.2.3	Anwendungsbereich des KonTraG.....	248
9.2.4	Risikomanagement – Überwachungssystem	249
9.2.5	Haftung der Geschäftsleitung.....	251
9.2.6	Beweislast.....	253
9.2.7	Prüfung durch Aufsichtsrat und Abschlussprüfer	254
9.3	SOX – Sarbanes Oxley Act.....	256
9.3.1	Zweck von SOX.....	256
9.3.2	Anwendungsbereich	257
9.3.3	Section 404 und internes Kontrollsystem	257
9.3.4	Behördliche Überwachung und Regelwerke	259
9.3.5	SOX in der EU.....	260
9.4	Zertifizierung von IT-Sicherheit	260
9.4.1	Vorteile und Standards	261
9.4.2	IT-Grundschutz nach BSI	262
9.5	Vorgaben nach Basel II.....	264
9.5.1	Ratingverfahren für den Kreditnehmer.....	264
9.5.2	Anforderungen an den Kreditgeber.....	265
9.5.3	MaRisk – gesetzliches Regelwerk für Informationssicherheit	265
9.6	Juristische Sicherheit.....	270
9.6.1	Rechtliche Gestaltung	270
9.6.2	Risikomanagement.....	271
9.6.3	Datenschutzkonzept	271

9.6.4	Beratung, Schulung, Workshops.....	272
10	Outsourcing von IT-Dienstleistungen.....	273
10.1	Ausgangslage	273
10.2	Was ist Outsourcing?	274
10.3	Rangliste der Outsourcing-Vorteile.....	275
10.4	Rangliste der ausgelagerten Bereiche.....	275
10.5	Erscheinungsformen	275
10.6	Vorbereitungsphase und Entscheidung.....	277
10.7	Anbietersauswahl	278
10.8	Vertragsgestaltung.....	279
10.8.1	Service Level Agreements.....	279
10.8.2	Das Erfolgskriterium: Werk- oder Dienstvertrag.....	281
10.8.3	Gemischter Vertrag	282
10.8.4	Gewährleistung	283
10.8.5	Schadensersatz	284
10.9	Berichtswesen/ Reporting	285
10.10	Rechtsfolgen	285
10.11	Rahmenvertrag	285
10.12	Transitionsphase	286
10.13	Ausstiegsszenario, Vertragsbeendigung	287
10.14	Die häufigsten Outsourcing-Fehler.....	289
11	Archivierungspflichten, Storage, Backup.....	291
11.1	Handelsrechtliche Aufbewahrungspflichten	291
11.1.1	Einsetzbare Datenträger (verwendbare Speichermedien).....	292
11.1.2	Aufbewahrungsfristen nach Handelsrecht.....	293
11.2	Steuerrechtliche Aufbewahrungspflichten.....	293
11.2.1	Einsetzbare Datenträger (verwendbare Speichermedien).....	294
11.2.2	Außenprüfung	294
11.2.3	Rechnungen und Vorsteuerabzug.....	295
11.2.4	Aufbewahrungsfristen nach Steuerrecht.....	295
11.3	Gesetzliche Aufbewahrungspflichten aufgrund sonstiger Vorschriften	296

11.4	Vorlegungspflichten und Beweislast im Prozess	296
11.5	Strafrechtliche Sanktionen.....	298
11.6	Kollision mit dem Datenschutz, insbesondere die E-Mail-Archivierung....	299
12	Hacker, Phishing, Spyware	303
12.1	Phishing	303
12.1.1	Zivilrechtliche Haftung	304
12.1.2	Haftung ohne Verschulden	305
12.1.3	Verschuldensabhängige Haftung	305
12.1.4	Strafbarkeit des Phishing	309
12.2	Hacker-Strafrecht	311
12.2.1	Ausspähen von Daten, § 202a StGB	311
12.2.2	Datenveränderung, § 303a StGB	313
12.2.3	Computersabotage, § 303b StGB.....	314
12.2.4	Strafbarkeit von Hacker-Tools, § 202c StGB.....	314
13	Voice over IP, Internettelefonie	317
13.1	Überblick: Gefahren von Voice over IP	318
13.2	Angriffe auf Voice over IP	318
13.2.1	Viren und Trojaner	318
13.2.2	VoIP-Spoofing	319
13.2.3	Möglichkeiten der Sicherung	319
13.3	Rechtliche Sicherheit bei VoIP	320
13.3.1	Eckpunkte zur VoIP-Regulierung	320
13.3.2	Notrufverpflichtung.....	321
13.3.3	Telekommunikations-Überwachung, TKÜV	321
13.3.4	Sicherheitsanforderungen an VoIP	322
13.3.5	Fernmeldegeheimnis.....	323
13.3.6	Betriebsverfassungsrecht	324
13.3.7	VoIP-Spamming, SPIT.....	324
13.3.8	Regulierung von VoIP	324

14	IT-Rechts-Leitfaden	327
14.1	Mit Rechtssicherheit zur Informationssicherheit	327
14.2	Haftungsfragen – Alles was Recht ist!	328
14.2.1	Strafverfolgung und Auskunftspflichten	328
14.2.2	Verkehrssicherungspflichten	329
14.2.3	Störerhaftung für ungesicherte Netzwerke, offene W-LAN.....	332
14.2.4	Haftungsszenario.....	333
14.2.5	Rechtsfolgen	333
14.2.6	Eigenhaftung der Mitarbeiter.....	334
14.2.7	Haftung nach TDG	336
14.3	Compliance und Risikomanagement.....	336
14.3.1	Haftung der Geschäftsleitung nach KonTraG	336
14.3.2	Anerkannte Standards und Zertifizierung.....	337
14.3.3	Vorgaben nach Basel II	338
14.3.4	Compliance nach SOX.....	340
14.4	Archivierungspflichten – mit Sicherheit Recht behalten!	342
14.4.1	Handelsrechtliche Pflichten.....	342
14.4.2	Steuerrechtliche Pflichten	343
14.4.3	Ordnungsgemäße Buchführung nach GoBS.....	343
14.4.4	Elektronische Betriebsprüfung nach GDPdU.....	344
14.4.5	Digitale Rechnungen	345
14.4.6	Archivierung im Eigeninteresse	346
14.5	Rechtssichere https-Scanserver	346
14.5.1	Zulässigkeitsvoraussetzungen	347
14.5.2	Best Practice-Beispiel.....	348
14.6	Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis?	348
14.6.1	Private Nutzung, Fernmeldegeheimnis.....	348
14.6.2	Dienstliche Nutzung, unerlaubte Privatnutzung	349
14.6.3	Interessenausgleich durch rechtliche Gestaltung.....	350
14.6.4	Mitbestimmung der Betriebs- und Personalräte.....	351
14.6.5	Betriebs- oder Dienstvereinbarungen	351
14.7	Checkliste	353
	Sachwortverzeichnis	355

1.1 Vertragsschluss im Netz

Verträge werden nicht nur schriftlich, sondern in allen denkbaren Lebenssituationen geschlossen. Mit der zunehmenden Bedeutung der digitalen Medien steigt parallel auch die Anzahl der elektronischen Vertragsabschlüsse.

1.1.1 Angebot und Annahme

Es gilt zunächst zu klären, aus welchen rechtlich relevanten Bausteinen ein Vertrag besteht.

1.1.1.1 Zwei übereinstimmende Willenserklärungen

Grundsatz

Voraussetzung für einen Vertragsschluss sind zwei übereinstimmende, auf den Vertragsschluss gerichtete Willenserklärungen der beteiligten Personen nach §§ 145 ff. BGB: das **Angebot** (Antrag) und die **Annahme**. Diese beiden übereinstimmenden Willenserklärungen – etwa das Kaufangebot des Verkäufers und die entsprechende Annahmeerklärung des Käufers – müssen den beteiligten Parteien **wechselseitig** zugehen. Durch den **Zugang** sind die Voraussetzungen für den Vertragsschluss erfüllt.

Elektronische Erklärungen

Auch eine Computererklärung ist nach heute herrschender Meinung eine Willenserklärung. Die Willenserklärungen können auch online, z. B. durch die elektronische Übermittlung einer Datei im Internet (z. B. eine E-Mail) oder durch **Mausklick** abgegeben und wirksam werden (so etwa BGH NJW 2002, 363 in der Entscheidung ricardo.de).

invitatio ad offerendum

Die bloße Bewerbung oder Präsentation eines Produkts im Internet ist genauso wenig wie die Schaufensterauslage im Ladengeschäft bereits ein rechtsverbindliches Angebot des Verkäufers, sondern die **bloße Aufforderung** an einen potentiellen Käufer,

seinerseits ein Angebot abzugeben; sogenannte „*invitatio ad offendum*“, also Einladung zum Angebot.

Mit der Eröffnung eines Webshops gibt der Onlineanbieter also noch keine wirksamen Willenserklärungen ab. Selbst wenn das automatisierte Kundeninformationssystem des Webshops auf Anfrage eine **individuell zugeschnittene** Produktauswahl und Preisbestimmung vornimmt, liegt noch kein rechtswirksames Angebot vor.

*Verbindliches
Angebot*

Eine Webseite hat nur ganz ausnahmsweise eine derart konkrete, rechtsverbindliche Wirkung, dass in ihr bereits ein verbindliches Vertragsangebot zu sehen ist. Ob die bloße Aufforderung zur Abgabe eines Angebots oder aber bereits ein verbindliches Angebot vorliegt, beurteilt sich danach, wie der Besteller (Kunde) den Inhalt der Webseite nach Treu und Glauben unter Berücksichtigung der Verkehrssitte verstehen darf.

*Solange
Vorrat
reicht*

Beim klassischen **Warenautomaten** wird das Rechtsgeschäft ebenfalls vollautomatisch abgewickelt, ohne dass ein menschlicher Vertreter des Verkäufers an dem Vorgang willentlich teilnimmt. Das Aufstellen des Automaten gilt solange als Angebot, wie Waren im Automaten vorhanden sind.

Diese Grundsätze lassen sich auf den **Onlinebereich** übertragen, sofern wie beim Warenautomaten die Vertragsabwicklung vollautomatisch abläuft. Die elektronisch abgegebenen Willenserklärungen stehen auch hier jeweils unter dem Vorbehalt „solange der Vorrat reicht“. Dies gilt für Warenbestellungen aller Art, aber auch für Downloads oder Bestellungen „on demand“ bezüglich Büchern oder Filmen, sofern die Anzahl begrenzt ist. Anders verhält es sich allerdings, wenn in die Vertragsabwicklung menschliche Mitarbeiter des Onlineanbieters eingebunden sind. Hier sind rechtsverbindliche Angebote auch abgegeben, wenn der Warenbestand erschöpft ist.

*Wirksames
Angebot*

Regelmäßig wird man also sagen können, dass die Produktpräsentation auf der Webseite lediglich zur Abgabe eines Angebots auffordert. Das Angebot zum Kaufvertrag gibt dann der bestellende Käufer ab, das durch eine Annahmeerklärung des Anbieters bestätigt wird, so dass der Kaufvertrag zum Abschluss kommt.

Faxbestätigung

Verlangt der Onlineanbieter vom Käufer eine Faxbestätigung der Bestellung, so hat diese keine rechtsbegründende Wirkung, auch hier kommt der Vertrag mit der Annahmeerklärung des Anbieters

zustande. Die Faxbestätigung des Käufers dient dem Anbieter nur zur Sicherung und **Beweiserleichterung**. Sie ist Voraussetzung dafür, dass er die Ware ausliefert.

1.1.1.2

Kaufmännisches Bestätigungsschreiben

*Beredtes
Schweigen*

Abweichend vom Regelfall der Notwendigkeit zweier übereinstimmender Willenserklärungen, gelten für den Kaufmann aufgrund seiner geringeren Schutzwürdigkeit Besonderheiten. Beim sogenannten „kaufmännischen Bestätigungsschreiben“ führt schon das Schweigen eines Kaufmannes zu Rechtsfolgen.

*Fixierung
Vertragsinhalt*

Wird unter Kaufleuten ein Geschäft zunächst mündlich abgeschlossen, beispielsweise auf der Messe, so ist es nach dem Vertragsschluss per Handschlag üblich, dem Geschäftspartner ein sogenanntes kaufmännisches Bestätigungsschreiben zur (schriftlichen) Fixierung der maßgeblichen Vertragsinhalte zuzusenden. Schweigt die Gegenseite auf den Erhalt eines solchen kaufmännischen Bestätigungsschreibens, so gilt der Vertrag mit dem Inhalt des Schreibens als zustande gekommen (vgl. hierzu auch unten Kapitel 7.2.6 zu den besonderen Auswirkungen beim Einsatz eines Spamfilters). Hierbei wird deutlich, dass zumindest unter Kaufleuten Verträge nicht nur gegenseitig zustande kommen, sondern auch **einseitig beeinflusst** werden können. Die zu diesem beredten Schweigen entwickelten gewohnheitsrechtlichen Grundsätze sind auch auf die E-Mail-Kommunikation übertragbar.

1.1.2

Beweisschwierigkeiten

Das theoretische Vorliegen der Voraussetzungen des Vertragsschlusses nützt jedoch wenig, wenn sie nicht bewiesen werden können. Zwischen Recht haben und Recht bekommen muss in der Praxis vor allem deshalb unterschieden werden, weil wer Recht haben will, sein Recht auch beweisen muss. In der Regel muss der Anspruchsteller alle Voraussetzungen für seinen Anspruch auch darlegen und beweisen können.

1.1.2.1

Ausgangssituation

Beweisschwierigkeiten bestehen vor allem bei Online-Bestellungen, bei denen anders als im normalen Ladengeschäft regelmäßig keine unterstützenden **Zeugenaussagen** herangezogen werden können.

*Beweis
Internetzugang*

Will also zum Beispiel der Internetprovider gegenüber dem Nutzer eine Dienstleistung abrechnen, so muss er u. a. Beweis dar-

über führen, dass gerade mit diesem Nutzer ein Vertrag zustande gekommen ist. Die belegte Tatsache, dass das Geschäft über einen **bestimmten Internetzugang** abgewickelt wurde, beweist noch nicht, dass gerade der Zugangsinhaber auch der Geschäftspartner des Internetproviders ist. Der Dienstleister kann aber regelmäßig nur Beweis darüber führen, wer Inhaber des Internetzuganges ist, nicht jedoch, wer die elektronische Bestellung oder sonstige Willenserklärung tatsächlich abgegeben hat. So etwa dann, wenn der Zugang von **mehreren Personen** benutzt wird (beispielsweise in einer studentischen WG etc.).

*Sichere
Zahlungs-
modalitäten*

Aus diesem Grunde ist der Dienstleister darauf angewiesen, von seinen Kunden sichere Zahlungsmodalitäten wie **Vorauskasse** oder **Kreditkarte** zu verlangen, weil er ansonsten seine Zahlungsforderungen nicht durchsetzen kann. Hieran krankt im wesentlichen der E-Commerce, da viele Nutzer nicht das **nötige Vertrauen** in die E-Commerce-Betreiber haben, um ihre Kreditkartennummer preiszugeben oder Vorauskasse zu leisten.

*Beweis
Vertragspartner*

So können die E-Commerce-Betreiber nicht **auf Rechnung** liefern, weil Ihre finanziellen Einbußen zu groß wären. Denn sie können im Zweifel nicht beweisen, wer eigentlich ihr Vertragspartner ist. Der in Anspruch genommene Schuldner kann einfach behaupten, nicht er habe die Dienstleistung bestellt und in Anspruch genommen, sondern z. B. ein Mitbewohner.

*Keine sichere
Beweisführung*

Es wird deutlich, dass unter der Beweisproblematik ein zukunfts-trächtiger Geschäftszweig wie das E-Business erheblich leidet. Dies liegt insbesondere darin begründet, dass mit elektronischen Dokumenten bisher keine sichere Beweisführung möglich ist. Abhilfe könnte hier nur die flächendeckende Einführung der **digitalen Signatur** schaffen.

1.1.2.2

Beweislast

Beweisregel

Grundsätzlich hat der Anspruchsteller – z. B. der Webshop-Betreiber (Verkäufer) oder Internetdienstleister, der einen Kaufpreisanspruch oder Zahlungsanspruch geltend macht – alle Voraussetzungen seines Anspruchs zu beweisen.

Hierzu gehören insbesondere die drei Punkte:

- ist ein Vertrag wirksam zustande gekommen, also der Vertragsschluss
- mit wem ist der Vertrag zustande gekommen, also die Identität des Schuldners (Käufers)
- was wurde im Vertrag im Einzelnen vereinbart, insbesondere die Höhe des Kaufpreises, also der Vertragsinhalt

Identitätsprüfung

Die Identifizierung des Online-Bestellers von Waren oder Dienstleistungen wird regelmäßig über eine **Eingabepflicht** von Name, Adresse und sonstigen Kontaktdaten in eine Bildschirmmaske (Webformular) vor dem eigentlichen Geschäftsabschluss angestrebt. Ebenso regelmäßig führt der Anbieter jedoch keine gesicherte Identitätsprüfung durch, die letztlich nur über die Verwendung einer digitalen Signatur erfolgen könnte. Vielmehr verlässt sich der Anbieter darauf, dass die Eingabe der Kontaktdaten wahrheitsgemäß erfolgt. Dies birgt ein hohes **Fälschungsrisiko**, da im Internet ohne großen Aufwand fremde Namen verwendet, Mailadressen gefälscht oder fremde Zugangsberechtigungen genutzt werden können. Auch die Angabe der **Kreditkartennummer** bewirkt keinen sichern Identitätsnachweis, sondern schafft für den Anbieter lediglich Zahlungssicherheit bis zu dem von der Bank garantierten Betrag.

Identitätsnachweis

Muss der Anbieter im Falle der Zahlungsverweigerung die geforderten Nachweise bringen, so kann er in der Regel über eine Auskunft des Providers nur den Inhaber des Internetzugangs bzw. die IP-Adresse nachweisen, über die die Bestellung erfolgt ist. Dies genügt aber nicht, wenn der Zugangsinhaber einwendet, eine dritte Person habe (unerlaubt) seinen Namen und Zugang für die Bestellung verwendet. Allein der Nachweis des Zugangs und der IP-Adresse beweist also noch nicht die Identität des Bestellers. Kann der Anbieter somit den geforderten Nachweis nicht führen, kann er seinen Zahlungsanspruch gerichtlich auch **nicht durchsetzen**.

Beweiserleichterungen

Allerdings kommen dem Online-Anbieter gewisse Beweiserleichterungen zugute. Juristisch spricht man von Anscheinsbeweis (prima-facie-Beweis) oder Rechtsschein bis hin zur Beweislastumkehr.

1.1.2.3

Anscheinsbeweis

Definition

Ein Anscheinsbeweis (Beweisvermutung) ist gegeben, wenn bei **typischen Lebenssachverhalten** aufgrund ständiger Erfah-

rungswerte ein bestimmter Geschehensablauf vermutet werden kann.

Bei Kfz-Unfällen zum Beispiel gilt der Merksatz: „Wenn`s hinten schellt, gibt`s vorne Geld“. Wer also auf ein anderes Fahrzeug hinten auffährt, muss bezahlen, ohne dass der Geschädigte ein Verschulden des Auffahrenden nachweisen müsste. Dem Geschädigten wird die Beweislast von den Schultern genommen, weil aufgrund der **allgemeinen Lebenserfahrung** der hinten Auffahrende regelmäßig den Unfall verschuldet hat, da er nach den Straßenverkehrsregeln stets ein rechtzeitiges Bremsen sicherstellen muss. Sein Verschulden wird also zugunsten des Geschädigten vermutet.

Erschütterung

Der Anscheinsbeweis kann entkräftet werden, indem der Anspruchsgegner (Online-Besteller) Umstände vorträgt und beweist, die einem typischen Geschehensablauf widersprechen.

Kann z. B. der hinten Auffahrende beweisen, dass der Geschädigte ohne Anlass eine Vollbremsung gemacht hat, so ist der Anscheinsbeweis erschüttert, weil der typische Ablauf nicht mehr vermutet werden kann. Die Beweiserleichterung entfällt, vielmehr gilt wieder die **allgemeine Beweisregel**, wonach der Geschädigte das Verschulden des hinten Auffahrenden beweisen muss.

Passwortinhaber

Bei Online-Bestellungen gibt es zwar keine Beweisvermutung (Anscheinsbeweis) zu Lasten des Inhabers eines bloßen Internetzuganges. Wohl aber wird vermutet, dass der Passwortinhaber auch der Besteller ist. Kann also der Online-Anbieter beweisen, dass eine Bestellung über einen bestimmten **passwortgeschützten Account**, der zum Zwecke der Bestellung zuvor eingerichtet wurde, erfolgt ist, so wird vermutet, dass der Passwortinhaber die Waren oder Dienstleistungen auch bestellt hat.

Die hierfür maßgebliche Rechtsprechung stammt zum Teil noch aus dem Btx-Zeitalter, wo ebenfalls zu Lasten des sogenannten **Kennungsinhabers** vermutet wurde, dass Bestellungen über die Kennung auch vom Inhaber vorgenommen wurden.

1.1.2.4

Zurechnung

Anscheins- und Duldungsvollmacht

Zum gleichen Ergebnis gelangt die Rechtsprechung über die Rechtsfigur der Anscheins- oder Duldungsvollmacht (OLG Köln NJW-RR 1994, 177; OLG Oldenburg NJW 1993, 1400). Hier gilt der Grundsatz des Vertrauensschutzes. Sofern ein Besteller ein fremdes Passwort verwendet, erzeugt er beim Anbieter den glaubwürdigen Rechtsschein, dass er ein **rechtmäßiger Vertre-**

ter des Passwortinhabers ist (Anscheinsvollmacht). Möglicherweise handelt er sogar mit dessen stillschweigendem Einverständnis (Duldungsvollmacht).

Vertrauensschutz

Solange der Online-Anbieter **gutgläubig** von der Vertretungsmacht des Bestellers ausgehen durfte, wird sein Vertrauen in den erzeugten Rechtsschein geschützt. Denn der Passwortinhaber muss dafür sorgen, dass sein Passwort geheim bleibt und kein Missbrauch betrieben werden kann.

Rechtsschein

Solange der Rechtsschein besteht, werden die getätigten Geschäfte dem Passwortinhaber zugerechnet. Der Anbieter kann seine Zahlungsansprüche gegenüber dem Passwortinhaber durchsetzen. Erst wenn der Rechtsschein zerstört wird, etwa weil bestimmte Indizien auf einen Missbrauch hindeuten oder der Passwortinhaber die fehlende Vertretungsbefugnis des Bestellers mitteilt, erfolgt keine Zurechnung mehr. Der Online-Anbieter ist gewarnt und nicht mehr gutgläubig. Vertraut er weiterhin auf die Rechtmäßigkeit der Bestellungen, so ist dieses Vertrauen nicht mehr schutzwürdig, so dass der Passwortinhaber für die Zahlungsansprüche nicht mehr haftet.

Angestellte und Familienangehörige

Diese Gedanken der Zurechnung werden zum Teil auch auf den geschäftlichen und häuslichen Bereich übertragen. Sofern Angestellte oder Familienangehörige über den PC- oder Btx-Zugang Bestellungen vornehmen, wird der Bestellvorgang dem Zugangsinhaber (Arbeitgeber oder Eltern) zugerechnet. Dieser hätte die Möglichkeit, über einen Passwortschutz Missbräuche zu verhindern oder durch die Vergabe von Passwörtern den eigentlichen Besteller zu identifizieren. Der Zugangsinhaber ist daher **nicht schutzwürdig** und muss haften (OLG Köln, NJW 1994, 177). Auf den Internetzugang im allgemeinen sind diese Grundsätze aber nicht pauschal übertragbar (vgl. oben, Kapitel 1.1.2.1).

1.1.2.5

Sonstige Beweiserleichterungen

Ebenso kann die Beweislast im Einzelfall durch rechtliche Regeln oder durch die Lebenserfahrung erleichtert werden. So kann der Rechtsgedanke des § 282 BGB a. F. zu einer Umkehr jedenfalls der Darlegungslast führen, wenn es sich um Vorgänge allein aus der Sphäre des Bestellers handelt (OLG Frankfurt CR 2002, 720).

Beweiskraft im Einzelfall

Grundsätzlich gelten die dargestellten Regeln zur mangelnden bzw. eingeschränkten Beweiskraft von E-Mails. In einzelnen Ausnahmefällen spricht die Rechtsprechung E-Mails unter den

besonderen Umständen des Einzelfalles auch eine rechtswirksame Beweiskraft zu (z. B. ArbG Frankfurt CR 2002, 615).

1.1.3 Zugang der Willenserklärungen, insbesondere von E-Mails

Voraussetzung für einen wirksamen Vertragsschluss ist wie bereits erwähnt auch der wechselseitige Zugang von Angebot und Annahme, den ebenfalls der Onlineanbieter als Anspruchsteller zu beweisen hat.

1.1.3.1 Grundregeln des Zugangs

*Laufende
Onlinesitzung*

Sofern die Willenserklärung gegenüber einer **anwesenden Person** erfolgt, geht sie unmittelbar zu und wird wirksam. In einer laufenden Onlinesitzung beispielsweise geht die elektronische Erklärung, abweichend vom Zugang der E-Mail, unmittelbar zu, wenn sie bei der anderen Partei auf dem Bildschirm erscheint.

*Zugang unter
Abwesenden*

Wird die Willenserklärung in Form einer E-Mail abgegeben, so geschieht dies in Abwesenheit des Erklärungsempfängers. Gemäß § 130 Abs. 1 Satz 1 BGB werden Willenserklärungen unter Abwesenden erst im Zeitpunkt des Zuganges wirksam. Es ist deshalb zu klären, wann dieser Zugang erfolgt.

Zugangsregel

Eine Willenserklärung ist zugegangen, wenn sie so in den Machtbereich des Empfängers gelangt, dass dieser die **Möglichkeit der Kenntnisnahme** hat und unter normalen Umständen mit der Kenntnisnahme auch zu rechnen ist (BGH NJW 1980, 990). Hierfür spricht nun auch der Wortlaut des § 312 e Absatz 1 Satz 2 BGB, der laut Regierungsentwurf der Rechtsprechung zum Zugang von Willenserklärungen gemäß § 130 BGB entspricht (BT-Drucksache 14/6040 Seite 172). Er bestimmt: „Bestellung und Empfangsbestätigung gelten als zugegangen, wenn die Parteien, für die sie bestimmt sind, sie unter gewöhnlichen Umständen abrufen können“.

1.1.3.2 Machtbereiche und Risikoverteilung

*Zugriffs-
möglichkeit beim
Provider*

Von der **Verfügungsgewalt** (Zugriffsmöglichkeit) des Empfängers kann erst ausgegangen werden, wenn die E-Mail oder sonstige elektronische Erklärung im EDV-System des Empfängers aufgerufen werden kann, nicht jedoch schon dann, wenn sie beim Provider eingegangen ist. Der Provider ist nicht dem Machtbereich des Empfängers zuzurechnen. Denn der Empfän-

<i>Kein Zugang beim Provider</i>	ger kann seine E-Mails nicht unter allen Umständen beim Provider abholen, weil er im Zweifel keinen Einfluss auf den Provider hat. Etwa wenn der Provider in Insolvenz gerät oder der Zugang des Empfängers wegen Zahlungsverzug gesperrt wird. Die E-Mail-Verbindung könnte bereits wegen rückständiger Bagatellforderungen gesperrt werden. Der Empfänger steht einer solchen Sperrung zunächst hilflos gegenüber und muss gegebenenfalls die Wiederfreischaltung erst gerichtlich durchsetzen. Aus den gleichen Gründen kann der E-Mail-Provider auch nicht als Empfangsbote oder Empfangsvertreter des Empfängers angesehen werden. Zum Teil wird in der juristischen Literatur jedoch vertreten, dass die E-Mail bereits mit Eingang auf dem Server des Providers als zugegangen gilt.
<i>Transportrisiko beim Absender</i>	Solange sich die E-Mail auf dem Weg zum Empfänger befindet, trägt allein der Absender das Transportrisiko. Es spielt dabei keine Rolle, aus welchen Gründen die E-Mail vom Empfänger nicht abgerufen werden kann. Dies kann eine Insolvenz des Providers genauso sein, wie technische Störungen oder Zahlungsrückstände des Empfängers. Nähme man den Zugang einer E-Mail bereits mit Eingang beim Provider an, so ergäbe sich ein ungerechtfertigter Wertungswiderspruch zu den in jahrzehntelanger Rechtsprechung entwickelten Grundsätzen beim Zugang postalischer Briefe.
<i>Niederlegung bei der Post</i>	So erachtet der BGH die Niederlegung eines postalischen Schreibens bei der Post noch nicht als ausreichend für den Zugang, selbst wenn dem Empfänger eine entsprechende Benachrichtigung in den Briefkasten gelegt wurde (BGHZ 67, 275). Dem gegenüber erhält der Adressat einer E-Mail von seinem Provider nicht einmal eine Eingangsbestätigung, die ihn zum Abruf seiner E-Mails auffordert. Mit Eingang beim Provider ist die E-Mail dem Empfänger daher noch nicht zugegangen.
<i>Zugang beim Empfänger</i>	Vielmehr erfolgt der Zugang erst durch den Eingang auf seinem eigenen Server bzw. wenn er seine E-Mails abgeholt hat. Nur so ist die Gleichstellung der klassischen und der neuen Kommunikationsmedien im Rahmen der BGH-Rechtsprechung gewahrt.
<i>Eigener Mailserver</i>	Die rechtlichen Zuordnungsprobleme sind geringer, wenn der Empfänger einen eigenen E-Mail-Server betreibt. Die E-Mail gelangt bereits mit Passieren der internen Schnittstelle – nicht erst mit Abspeichern – in den Machtbereich des Empfängers und geht zu. Damit unterfallen auch zentrale Filtermaßnahmen auf dem Gateway bereits dem Organisationsrisiko des Empfängers.

*Organisations-
risiko beim
Empfänger*

Die Fragen von Machtbereich und Risikoverteilung werden vor allem bedeutsam, wenn E-Mails unterwegs verloren gehen oder fehlgeleitet werden. Der Absender trägt hierbei das Transportrisiko. Dagegen geht es zu Lasten des Empfängers, wenn eine Erklärung, wieder verloren geht, über die er bereits die Verfügungsgewalt besitzt, z. B. durch eine Filtermaßnahme. Das Organisationsrisiko vor Ort liegt also beim Empfänger, da nur er selbst den notwendigen Einfluss in seinem Machtbereich hat.

Filtermaßnahmen

Diese Grundsätze werden beispielsweise beim Einsatz von Spamfiltern bedeutsam, wo Fehlleitungen vorkommen können (vgl. hierzu unten, Kapitel 7.2.5).

1.1.3.3

Objektive Möglichkeit der Kenntnisnahme, Zugangsfiktion

*Objektive
Möglichkeit*

Für den Zugang genügt die *objektive* Möglichkeit der Kenntnisnahme, sofern eine Kenntnisnahme objektiv zu erwarten ist. Ob der Empfänger von dieser Möglichkeit tatsächlich Gebrauch macht, geht dagegen zu seinen Lasten. Holt er beispielsweise die E-Mails bei seinem Provider **mutwillig nicht ab**, so gelten sie gleichwohl als zugegangen (Zugangsfiktion).

*Faxrecht-
sprechung des
BGH*

Für die Beantwortung der Frage, wann die Kenntnisnahme **objektiv zu erwarten** ist, kann die Faxrechtsprechung des BGH entsprechend herangezogen werden. Demnach gilt ein noch während der **Geschäftszeiten** an das Empfangsgerät eines Kaufmannes übermitteltes Faxschreiben spätestens mit Geschäftsschluss des Kaufmannes als zugegangen. Es ist also anerkannt, dass mit der Kenntnisnahme eines per Fax übermittelten Schreibens noch während der Geschäftsstunden eines Unternehmens gerechnet werden darf, den Faxempfänger also eine entsprechende Überprüfungspflicht hinsichtlich der Faxeingänge trifft (BGHZ 67, 271, 278).

*Zugang am
selben Tag*

Entsprechendes gilt für den **E-Mailverkehr**, sofern ein Unternehmen durch Angabe einer E-Mail-Adresse auf Webseite, Briefbogen oder sonstigen Werbeträgern dem Geschäftsverkehr signalisiert, dass es die E-Mail-Kommunikation bereithält. Damit trifft das Unternehmen auch die Pflicht, seine E-Mails regelmäßig abzurufen, da der Absender mit einer zeitnahen Kenntnisnahme rechnen darf.

*Zugang beim
Kaufmann*

Ist der Empfänger Kaufmann, kann auch hier eine Zugangsfiktion der versendeten E-Mail **zum Geschäftsschluss** des Empfängers angenommen werden. Die im Laufe des Tages abgesendete E-Mail geht also noch während der Bürozeiten am selben Tage

zu. Innerhalb der üblichen Geschäftszeiten kann mit der Kenntnisnahme gerechnet werden. Sofern die Erklärung außerhalb der Geschäftszeiten versendet wird, geht sie erst am darauf folgenden Geschäftstag zu. Betreibt der Anbieter einen **24-Stunden-Service**, so ist sogar jederzeit mit der Kenntnisnahme zu rechnen. Wer am elektronischen Rechts- und Geschäftsverkehr teilnimmt, muss also seine Mailbox ständig im Auge behalten.

Zugang beim Privatmann

Dagegen sind die Erwartungen an den Privatmann geringer. Ihm kann lediglich die tägliche Einsichtnahme in seine Mailbox zugemutet werden, so dass der Zugang einer versendeten E-Mail erst mit dem darauf **folgenden Tag** angenommen wird.

1.1.3.4

Zugangsvereitelung

Abholpflicht

Der Empfänger kann den Zugang der E-Mail nicht hinauszögern, indem er seine Nachrichten beim Provider nicht abholt. Denn wie gesehen muss jeder, der mit einer E-Mail-Adresse am Rechtsverkehr teilnimmt, sicherstellen, dass ihn die E-Mail-Nachrichten erreichen. Für den Kaufmann besteht sogar eine besonders zeitnahe Pflicht, seine E-Mails abzurufen. Ruft der Empfänger seine E-Mails pflichtwidrig über einen längeren Zeitraum nicht ab oder löscht er sie ohne Kenntnisnahme, so erfolgt die beschriebene Zugangsfiktion.

Zugangsfiktion

In den Fällen der Zugangsvereitelung muss sich der Empfänger im Wege einer Annahme so behandeln lassen, als sei ihm die E-Mail in seinem Machtbereich zugegangen (BGHZ 67, 271, 278). Dabei wird der Zugang zu dem Zeitpunkt unterstellt, zu dem unter **gewöhnlichen Umständen** mit einer Kenntnisnahme gerechnet werden kann. Dies ist wie beschrieben bei Geschäftsleuten noch am selben Tag, sofern die E-Mail nicht zur Unzeit versendet wurde. Bei Privatpersonen wird der Zugang dagegen erst am nächsten Tag angenommen.

Störungsbeseitigung

Sofern der Empfänger erkennen konnte, dass die Weiterleitung oder sein Zugriff auf die E-Mails gestört ist, muss er **zumutbare Möglichkeiten** ausschöpfen, um das Hindernis zu beseitigen. Bleibt es dennoch bestehen, so ist der Zugang nicht erfolgt, vielmehr verwirklicht sich das **Transportrisiko** beim Absender. In diesem Fall kann im Rahmen der technischen Möglichkeiten von einer vertraglichen Hinweispflicht des Empfängers auf die Störung ausgegangen werden.

1.1.3.5

Zugangsbeweis

Beweislast

Den Zugangsbeweis kann der **Anspruchsteller** nur unter Schwierigkeiten führen. Übermittlungsfehler sind beim E-Mail-Verkehr genausowenig ausgeschlossen wie beim postalischen Brief. Der Schuldner (Besteller) kann deshalb immer behaupten, er habe die Annahmeerklärung des Anbieters nicht erhalten, weshalb kein Vertrag zustande gekommen sei. Denn sofern aufgrund eines Übermittlungsfehlers die E-Mail oder sonstige Nachricht nicht in den Machtbereich des Empfängers gelangt, fehlt es wie gesehen am Zugang und damit am Vertragsschluss.

Digitale Signatur

Fraglich ist, wie der Zugangsbeweis in der Praxis sicher geführt werden kann. Auch hier ist an erster Stelle wiederum die digitale Signatur zu nennen, die auch den Zugang verlässlich belegen kann.

Empfangs- und Lesebestätigung

Einen **Anscheinsbeweis** dürfte die Empfangs- und insbesondere die Lesebestätigungsmail vom Empfänger liefern, die den Eingang bzw. den Aufruf der Mail beim Empfänger dokumentieren. Bei Rücksendung einer solchen Bestätigungsmail wird in aller Regel der Zugang technisch erfolgt sein. Hier muss der Empfänger also durch Darlegung und Beweis außergewöhnlicher Umstände die Anscheinssituation entkräften. Hinreichende Sicherheit bietet die Lese- oder Empfangsbestätigungsmail aber schon deshalb nicht, weil ihre Rücksendung von der ausdrücklichen Zustimmung des Empfängers, die stets auch verweigert werden kann, abhängig ist. Überdies kann der Empfänger in seinem Mailprogramm die gesamte Funktion einfach **abschalten**.

Sendebestätigung

Nicht ausreichend für einen Anscheinsbeweis ist – entsprechend den Grundsätzen des BGH zum Faxprotokoll – die Vorlage einer Sendebestätigung. Diese kann lediglich belegen, dass die E-Mail den Mailserver des Absenders verlassen hat, nicht jedoch, dass sie auch in die Mailbox des Empfängers gelangt ist.

Unterstützende Zeugenaussagen

Allerdings wird man zur Beweisführung mit unterstützenden Zeugenaussagen arbeiten können, zumal im gewerblichen Bereich, wo zumeist **Mitarbeiter** als Zeugen zur Verfügung stehen. Sofern ein Zeuge aussagt, dass die E-Mail entsprechend der Sendebestätigung den Mailserver des Absenders verlassen hat, und ein weiterer Zeuge den Eingang auf Empfängerseite bestätigt, wird ein ausreichender Beweis für den Zugang geführt sein. Auch für die Empfangs- und Lesebestätigungs-Mails können unterstützende Zeugenaussagen wichtig werden.

*Gefälligkeits-
aussagen*

In diesem Zusammenhang muss natürlich auch mit Gefälligkeitsaussagen aufgrund falsch verstandener Loyalität von Mitarbeitern gerechnet werden. Regelmäßig wird es sich ein Zeuge aber gut überlegen müssen, die Unwahrheit zu sagen, da bei der E-Mail stets mit der Kenntnisnahme mehrerer Personen gerechnet werden muss. Man denke nur an die **CC-Benachrichtigung** oder Mailboxen mit mehreren Zugangsberechtigten, die zu einer Nachprüfbarkeit von Zeugenangaben führen.

1.1.4**Fazit***Hilfestellung*

Der Anbieter von E-Commerce-Dienstleistungen hat bei der Durchsetzung seiner Zahlungsansprüche besondere Schwierigkeiten, da er die Anspruchsvoraussetzungen, für die er grundsätzlich die Beweislast trägt, regelmäßig nicht beweisen kann. Als kleine Hilfestellung ist ihm deshalb zu raten, seine Leistungen über einen **passwortgeschützten Account** anzubieten. Dann kommt ihm zumindest ein Anscheinsbeweis (Beweisvermutung) für die Zahlungsverpflichtung des Passwortinhabers zu Hilfe. Jedoch ist dieser Schutz begrenzt, da auch bei der Passwortvergabe jederzeit Missbräuche möglich sind. Sicherheit für den Anbieter geben nur die digitale Signatur oder ein fälschungssicheres **Identifikationssystem**.

1.2**Online-AGB***Schuldrechts-
reform*

Für die Wirksamkeit des sogenannten Kleingedruckten (**Allgemeine Geschäftsbedingungen**, AGB) gibt es eine ganze Reihe von gesetzlichen Vorschriften, die seit der Schuldrechtsreform nicht mehr in einem eigenständigen AGB-Gesetz (AGBG), sondern in den §§ 305 ff. BGB verankert sind.

*Vertragliche
Bestimmungen*

AGB sind also nur wirksam, wenn sie den gesetzlichen Vorgaben entsprechen. Trotzdem gelten die AGB nicht auf Grund des Gesetzes, sondern sind vertragliche Bestimmungen, die wie alle anderen Vertragsbestandteile auch rechtswirksam in den **Vertrag miteinbezogen** werden müssen. Es handelt sich um willentliche Vereinbarungen zwischen den beteiligten Vertragsparteien. In der Folge wird deshalb erläutert, unter welchen Voraussetzungen AGB Vertragsbestandteil werden.