

Peter Schneider

# Haftung für Datenverlust im Cloud Computing



# Internet und Recht

Herausgegeben von  
Prof. Dr. Georg Borges  
Universität des Saarlandes

Band 16

Peter Schneider

# Haftung für Datenverlust im Cloud Computing



**Nomos**

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

Zugl.: Bochum, Univ., Diss., 2017

ISBN 978-3-8487-4525-8 (Print)

ISBN 978-3-8452-8767-6 (ePDF)

1. Auflage 2017

© Nomos Verlagsgesellschaft, Baden-Baden 2017. Gedruckt in Deutschland. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

## Vorwort

Daten bestimmen gegenwärtig in großem Umfang unseren Alltag – sei es im digitalen Umgang mit privaten Bekanntschaften oder in der betrieblichen Gewinnmaximierung. Neuartige technologische Ansätze wie das Cloud Computing bieten viel Potential zur Optimierung dieser Abläufe und somit zur Erzielung von besseren Ergebnissen. Komplex wird die Situation immer dann, wenn es innerhalb dieser Abläufe zu Unregelmäßigkeiten kommt.

In der rechtswissenschaftlichen Literatur wurde der Umgang mit Daten in der Cloud bisher primär unter dem Gesichtspunkt der datenschutzrechtlichen Zulässigkeit diskutiert. Gerade moderne Technologien wie das Cloud Computing werfen indes auch zahlreiche neuartige Fragestellungen im besonders praxisrelevanten Bereich der zivilrechtlichen Haftung auf. Die Darstellung, Analyse und Auflösung dieser Problemfelder ist Gegenstand der vorliegenden Arbeit.

Mein Dank gilt zunächst meinem Doktorvater, Herrn Prof. Dr. Georg Borges, der die Anregung zu dem Thema gab und stets ein offenes Ohr für Rückfragen hatte. Erst durch seine konstruktiven Denkanstöße konnte die Bearbeitung des Themenkomplexes in Gänze gelingen. Herrn Jun.-Prof. Dr. Frank Rosenkranz danke ich für die zügige und umfangreiche Zweitbegutachtung dieser Arbeit.

Meiner Lebenspartnerin, Frau Kristin Kramer, gilt besonderer Dank dafür, dass sie die oft nicht einfachen Zeiten der Doppelbelastung mit Dissertation und Beruf mit mir durchgestanden hat. Weiterhin danke ich den ehemaligen Kollegen, hier namentlich den Herren Sascha Adler, Christoph Engling, Alexander Golland, Torben Kriegesmann sowie Dr. Andreas Weitzell, herzlich für die sorgfältige Durchsicht des Manuskripts und die fruchtbaren inhaltlichen Diskussionen. Außerdem möchte ich Herrn Thomas Böttcher danken, der durch seine kontinuierliche persönliche Wertschätzung und Motivation einen erheblichen Anteil an der stringenten Anfertigung dieser Arbeit trägt.

Der größte Dank gilt schließlich meinen Eltern, Ingrid und Heinz Schneider, welche finanziell, aber auch in jeder anderen erdenklichen

*Vorwort*

Art und Weise, meine Ausbildung stets nachdrücklich gefördert haben. Ihnen ist diese Arbeit gewidmet.

Mülheim an der Ruhr

Dr. Peter Schneidereit

# Inhaltsverzeichnis

Abkürzungsverzeichnis	25
1. Kapitel Einführung	29
§ 1 Einleitung	29
I. Cloud Computing: Siegeszug einer innovativen Informationstechnologie	29
II. Praktische Relevanz von Haftungsfragen in der Cloud	30
III. Haftung für Datenverlust: Quo vadis?	31
§ 2 Gegenstand der Untersuchung: Maßgebliche Haftungsszenarien	33
I. Hackerangriff auf die Cloud durch externe Dritte	33
1. Haftungsszenario	33
2. Schadensursachen	34
3. Haftungsadressaten	34
II. Beeinflussung von Datenbeständen durch grundsätzlich berechnigte Cloud-Nutzer	35
1. Haftungsszenario	35
2. Schadensursache	36
3. Haftungsadressat	36
III. Datenverlust bei Betrieb des Cloud-Dienstes durch den Cloud-Anbieter	37
1. Haftungsszenario	37
2. Schadensursachen	37
3. Haftungsadressat	38
§ 3 Gang der Darstellung	38
2. Kapitel Technische und organisatorische Grundlagen des Cloud Computing	41
§ 4 Definition und technische Funktionsweise	41
I. Begriff und Abgrenzung	41
1. Definitionsansätze	41
2. Historische Entwicklung	42

3. Abgrenzung von vergleichbaren Technologien	43
a) IT-Outsourcing	43
b) Application Service Providing	43
c) Grid Computing	44
II. Technische Umsetzung	45
1. Ausgangspunkt: Ubiquitäre Erreichbarkeit für großen potentiellen Nutzerkreis	45
2. Umsetzungsansatz: Virtualisierung	45
3. Vereinheitlichung der Kommunikation	46
4. Flexible und ortsunabhängige Nutzbarkeit von IT-Ressourcen	47
5. Zwischenergebnis	48
III. Technische Ursachen für Datenverlust	48
1. Maßgebliches Haftungsszenario	48
2. Technisch bedingte Verlustursachen	49
§ 5 Leistungen und Nutzerkreis	50
I. Leistungsarten	50
1. Ausgangspunkt	50
2. Software as a Service (SaaS)	51
3. Platform as a Service (PaaS)	51
4. Infrastructure as a Service (IaaS)	52
5. Everything as a Service (XaaS)	53
II. Betroffener Nutzerkreis	53
1. Private und Public Clouds	54
2. Hybrid und Community Clouds	54
§ 6 Zwischenergebnis	55
3. Kapitel Anwendbares Recht	57
§ 7 Anwendbares Vertragsrecht	57
I. Anwendbarkeit der Rom I-VO	57
II. Rechtswahl	58
III. Objektive Anknüpfung	59
1. Grundsätzliche Anknüpfung	60
2. Keine offensichtlich engere Verbindung zu Drittstaat	61
IV. Besonderheiten bei Verbraucherverträgen	62
1. Verbraucherbegriff	62
2. Bezugspunkt zum Heimatstaat des Verbrauchers	63

3. Kein Ausschluss der Anwendbarkeit	65
4. Einschränkung der Rechtswahl	65
§ 8 Anwendbares Deliktsrecht	66
I. Anwendbarkeit der Rom II-VO	66
II. Rechtswahl	67
III. Objektive Anknüpfung	68
1. Ansprüche des Cloud-Nutzers gegen den Cloud-Anbieter	69
2. Ansprüche des Cloud-Nutzers gegen Dritte	69
a) Maßgebliche Haftungsszenarien	69
b) Ort des Schadenseintritts	70
aa) Erfolgsort bei Online-Delikten	70
bb) Problemstellung im Rahmen des Cloud Computing	71
cc) Ausweichklausel: Art. 4 Abs. 3 Rom II-VO	73
(1) Anknüpfung an das Vertragsstatut	73
(2) Kritische Würdigung	73
(3) Lösungsansatz: Differenzierte Anwendung der Ausweichklausel des Art. 4 Abs. 3 Rom II-VO	75
(a) Bedarf für eine kollisionsrechtliche Korrektur	75
(b) Haftung des externen Hackers	76
(c) Haftung des berechtigten Mitnutzers	76
§ 9 Ergebnis	77
4. Kapitel Vertragliche Haftung	79
§ 10 Vertragstypologische Einordnung	79
I. Ausgangspunkt: Vertragstypen	79
II. Die Typologie einzelner Leistungsarten	80
1. Software as a Service (SaaS)	80
a) Streitstand	80
b) Stellungnahme	81
2. Infrastructure as a Service (IaaS)	84
3. Platform as a Service (PaaS)	85
4. Everything as a Service (XaaS)	86
5. Unentgeltliche Erbringung von Cloud-Leistungen	86

6. Zwischenergebnis	88
III. Vereinbarung von Zusatzleistungen	89
1. Grundsatz	89
2. Vertragstypologische Einordnung konkreter Zusatzleistungen	90
a) Schulung und Support	90
b) Softwarepflege und –anpassung	91
aa) Instandhaltungspflicht	91
bb) Softwareverbesserungen	92
c) Datensicherung	93
IV. Ergebnis	94
§ 11 Haftungsszenarien und Rechtsgrundlagen	94
§ 12 Haftung für den Verlust von Daten während des Betriebs des Cloud-Dienstes	96
I. Maßgebliches Haftungsszenario	96
II. Abgrenzung der anwendbaren Haftungsgrundlagen	96
III. Anspruch des Cloud-Nutzers gegen den Cloud-Anbieter aus § 536 a BGB	98
1. Maßgebliche Fallgruppe	98
2. Mangel der Mietsache	98
3. Vertretenmüssen	99
a) Ausgangspunkt	99
b) Anfängliche Mängel der Mietsache	100
c) Nachträglich aufgetretene Mängel der Mietsache	101
aa) Grundsatz	101
bb) Aktiver Verursachungsbeitrag des Cloud- Anbieters zur Mangelbegründung	101
cc) Unterlassung von Instandhaltungsmaßnahmen	102
dd) Unterlassung von allgemeinen Schutzvorkehrungen	103
ee) Einschaltung von Subunternehmern	105
4. Kausalität	106
5. Zwischenergebnis	106
IV. Anspruch des Cloud-Nutzers gegen den Cloud-Anbieter aus § 280 Abs. 1 BGB	106
1. Maßgebliche Fallgruppe	106

2. Pflichtverletzung	107
a) Verletzung einer vertraglichen Hauptleistungspflicht	107
b) Verletzung der Verpflichtung zur Abwehr schädlicher natürlicher Einflüsse	108
aa) Maßgebliche Fallgruppe	108
bb) Mietrechtlicher Ausgangspunkt	108
cc) Konkretisierung durch Anforderungen an physische Datensicherheit	110
(1) Grundsatz: Verpflichtung zur Gewährleistung von IT-Sicherheit	110
(2) Physische Schutzmaßnahmen gegen natürliche Einflüsse als Teil der IT-Sicherheit	111
(3) Umfang der erforderlichen Schutzmaßnahmen	112
(a) Ausgangspunkt: Risikoanalyse	112
(b) Grenze: Zumutbarkeit der Sicherheitsvorkehrungen	113
(c) Erforderliche Maßnahmen zur Gewährleistung physischer Datensicherheit	114
(4) Verarbeitung personenbezogener Daten	116
(a) Gesetzliche Konkretisierung vertraglicher Schutzpflichten	116
(b) Grundlegende Anforderungen aus § 9 BDSG	116
(c) Auswirkungen auf erforderliche physische Datensicherheitsmaßnahmen	117
(5) Telemedienrechtliche Anforderungen	118
(a) Anwendungsbereich	119
(b) Auswirkungen im Hinblick auf Schutzvorkehrungen gegen äußere Einflüsse	119
c) Verletzung der Verpflichtung zur Datensicherung	122
aa) Maßgebliche Fallgruppe	122
bb) Meinungsstand	122
(1) Verpflichtung des Cloud-Nutzers	123
(2) Verpflichtung des Cloud-Anbieters	123

cc) Dogmatischer Anknüpfungspunkt	125
dd) Inhalt der Schutzpflicht	127
(1) Maßgebliche Kriterien	127
(2) Interessenverteilung im Cloud-Computing	129
(3) Einflussnahmemöglichkeit des Cloud-Anbieters	130
(4) Zumutbarkeit	131
(a) Schadenspotential	132
(b) Wahrscheinlichkeit der Schadensverwirklichung	133
(c) Korrespondierender Vermeidungsaufwand	134
(d) Abwägung	135
(5) Schutzwürdigkeit des Betroffenen	136
ee) Zwischenergebnis	138
ff) Umfang der Schutzpflicht	138
(1) Meinungsstand	139
(2) Umfang und Frequenz der Datensicherung durch den Cloud-Anbieter	139
(3) Ort der Datensicherung	141
gg) Zwischenergebnis: Pflicht des Cloud-Anbieters zur Datensicherung	141
3. Vertretenmüssen	142
a) Grundsatz	142
b) Vorsätzliche Verletzung von Sicherungspflichten	142
c) Vorliegen eines Organisationsverschuldens	143
4. Kausalität	144
5. Mitverschulden	144
V. Zwischenergebnis: Haftung des Cloud-Anbieters für Datenverlust während des Betriebs des Cloud-Dienstes	146
§ 13 Haftung für den Verlust von Daten aufgrund unbefugten Fremdzugriffs	146
I. Maßgebliches Haftungsszenario	146
II. Anspruch des Cloud-Nutzers gegen den Cloud-Anbieter aus § 280 Abs. 1 BGB	147
1. Pflichtverletzung	147
a) Verpflichtung zur Abwehr von externen Angriffen	147

b) Umfang der erforderlichen Schutzmaßnahmen	149
aa) Grundsatz	149
bb) Grundlegende Maßnahmen bei gewerblicher Datenverarbeitung	150
cc) Spezifische IT-Sicherheitsrisiken in der Cloud	151
dd) Auswirkungen auf das erforderliche IT-Sicherheitsniveau beim Cloud-Anbieter	153
(1) Erhöhte Anforderungen an technische Schutzvorkehrungen	153
(2) Regelmäßige Durchführung einer Datensicherung	154
(3) Implementierung angemessener Authentifizierungsverfahren	155
(4) Schulungs- und Informationspflichten	156
(5) Verarbeitung personenbezogener Daten	157
(6) Telemedienrechtliche Anforderungen	159
2. Vertretenmüssen	160
III. Zwischenergebnis: Haftung des Cloud-Anbieters bei externen Angriffen auf den Datenbestand	161
§ 14 Haftungsbeschränkung durch AGB	161
I. Grenzen der Haftungsbeschränkung in Cloud-AGB	162
1. Einfache Fahrlässigkeit	162
2. Haftungshöchstgrenzen	164
3. Klauselverbote ohne Wertungsmöglichkeit	164
II. Cloud-Lösungen für Privatanwender	165
1. Amazon Cloud Drive	165
2. Microsoft OneDrive	166
3. Google Cloud Drive	166
4. Haftungsrechtliche Analyse	167
a) Haftungsbeschränkung	167
b) Rezeption in der Rechtsprechung	168
5. Zwischenergebnis	168
III. Kommerzielle Cloud-Lösungen	169
1. Oracle Cloud Services	169
2. Dell Cloud Solutions	169
3. Telekom CRM Services Online	170
4. Analyse im Vergleich zu nicht kommerziellen Cloud-Angeboten	170

5. Zwischenergebnis	171
§ 15 Ergebnis: Vertragliche Haftung im Cloud Computing	171
5. Kapitel Deliktische Haftung	173
§ 16 Haftungsszenarien und Verhältnis zur vertraglichen Haftung	173
I. Maßgebliche Haftungsszenarien	173
II. Verhältnis zur vertraglichen Haftung	174
§ 17 Vorliegen einer Rechtsgutsverletzung im Rahmen des § 823 Abs. 1 BGB	175
I. Maßgebliche Haftungsszenarien	175
II. Verletzung des Eigentums	175
1. Anknüpfung an den Datenträger	176
2. Drittschadensliquidation	176
a) Ausgangspunkt	176
b) Anwendung auf Datenverlust in der Cloud	177
aa) Grundsatz	177
bb) Meinungsstand	177
cc) Stellungnahme	178
(1) Fehlen einer vergleichbaren Interessenlage	178
(2) Mangelnde Eignung zur sachgerechten Auflösung von Haftungsdefiziten	179
c) Zwischenergebnis	180
III. Verletzung des Besitzes	180
1. Qualifikation als sonstiges Recht	180
2. Bestehen eines Besitzrechts des Cloud-Nutzers	181
a) Voraussetzungen	181
b) Besitz an den eingesetzten Servern	182
aa) Meinungsstand	182
bb) Stellungnahme	183
IV. Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb	183
1. Maßgebliche Fallgruppen	184
2. Rechtsnatur und Qualifikation als sonstiges Recht	184
3. Schutzbereich	185
4. Potentielle Eingriffe	186
5. Rechtswidrigkeit	186
6. Beeinträchtigung von Datenbeständen in der Cloud	187

7. Zwischenergebnis	188
V. Verletzung des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme	188
1. Maßgebliche Fallgruppe	188
2. Grundrechtlicher Ausgangspunkt	189
3. Qualifikation als sonstiges Recht	189
4. Schutzbereich	190
a) Begriff des informationstechnischen Systems	190
b) Die Cloud als informationstechnisches System	191
aa) Die Entscheidung des BVerfG	191
bb) Stellungnahme	193
5. Potentielle Eingriffe	194
6. Rechtswidrigkeit	195
7. Zwischenergebnis	196
VI. Verletzung des Urheberrechts	196
1. Maßgebliche Fallgruppen	196
2. Qualifikation als sonstiges Recht	197
3. Anwendbarkeit der deliktischen Haftung	197
4. Schutzgut	197
5. Potentielle Verletzungshandlungen	198
6. Zwischenergebnis	199
VII Zwischenergebnis	199
.	199
§ 18 Verletzung von Verkehrspflichten	200
I. Maßgebliche Fallgruppe	200
II. Dogmatische Grundlage	201
III. Bestehen einer Verkehrspflicht	202
1. Ausgangspunkt	202
2. Verkehrspflicht des Cloud-Anbieters	203
IV. Ausgestaltung der Verkehrspflicht	203
V. Zwischenergebnis	205
§ 19 Verletzung eines Schutzgesetzes i.S.d. § 823 Abs. 2 BGB	205
I. Dogmatische Grundlage	206
II. Verstoß gegen § 202 a StGB	207
1. Maßgebliche Fallgruppe	207
2. Qualifizierung als Schutzgesetz	208
3. Tatbestand	208
a) Betroffene Datensätze	208

b) Personelle Zuweisung	209
c) Tathandlung	211
d) Subjektiver Tatbestand	211
e) Zugriff auf Daten in der Cloud	212
f) Verhältnis zu § 202 b StGB	212
4. Vorliegen eines Schadens	213
a) Ausgangspunkt	213
b) Rechtsverfolgungskosten	214
c) Schadensermittlungskosten	214
d) Imageschaden	215
5. Zwischenergebnis	216
III. Verstoß gegen § 303 a StGB	216
1. Maßgebliche Fallgruppen	216
2. Qualifizierung als Schutzgesetz	217
3. Tatbestand	217
a) Datenbegriff	217
b) Tathandlung	218
c) Subjektiver Tatbestand	219
d) Verhältnis zu § 303 b StGB	220
aa) Anwendungsbereich und Voraussetzungen	220
bb) Bedeutung im Cloud Computing	221
4. Verschulden	222
a) Grundsatz	222
b) Haftung des externen Hackers	222
c) Haftung des grundsätzlich berechtigten Cloud-Nutzers	223
5. Kausalität	223
6. Zwischenergebnis	225
IV. Verstoß gegen § 263 a StGB	225
1. Maßgebliche Fallgruppe	225
2. Qualifizierung als Schutzgesetz	226
3. Tatbestand	226
a) Tathandlung	226
aa) Bedrohungsszenario	226
bb) Unrichtige Gestaltung eines Programms	227
cc) Sonstige unbefugte Einflussnahme	228
b) Erfordernis eines Vermögensschadens	230
aa) Auseinanderfallen von Angriffsziel und Geschädigtem	230

bb) Vorliegen eines Vermögensschadens	232
(1) Grundsatz	232
(2) Unbefugte Inanspruchnahme von (IT-)Leistungen	232
(3) Datenbeschädigung und Datenverlust	233
(4) Vermögensgefährdung als Schaden	234
c) Subjektiver Tatbestand	236
4. Zwischenergebnis	236
V. Zwischenergebnis	237
§ 20 Eigenständige deliktische Haftungsgrundlagen	238
I. Sittenwidrige Schädigung i.S.d. § 826 BGB	238
1. Maßgebliche Fallgruppe	238
2. Haftungsvoraussetzungen	238
3. Vernichtung von Datenbeständen in der Cloud	239
4. Zwischenergebnis	240
II. Wettbewerbsrechtliche Haftung aus § 9 S. 1 UWG	240
1. Maßgebliche Fallgruppen	241
2. Sachlicher und personeller Anwendungsbereich	242
3. Vorliegen einer gezielten Behinderung	243
a) Grundsatz	243
b) Beeinträchtigung von Datenbeständen in der Cloud	244
4. Zwischenergebnis	244
III. Haftung aus § 1 Abs. 1 S. 1 ProdHaftG	245
1. Maßgebliche Fallgruppe	245
2. Haftungsadressat	246
3. Taugliches Haftungsobjekt	247
a) Streitstand	247
b) Stellungnahme	248
aa) Gänzliche Verneinung der Produkteigenschaft	248
bb) Begrenzung auf Individualsoftware	249
cc) Differenzierung anhand der Übermittlungsart	250
dd) Differenzierung anhand eines Übermittlungserfordernisses	251
(1) Meinungsstand	251
(2) Stellungnahme	252
(a) Wortlaut der Norm	252
(b) Rechtsprechung des EuGH	252
(3) Risikoentscheidung des Herstellers	253

c) Zwischenergebnis	254
4. Fehlerhaftigkeit des Produkts	254
5. Haftungsausschluss aufgrund mangelnder Vorhersehbarkeit	256
6. Subjektives Element	258
7. Erfasste Schadenspositionen	258
8. Zwischenergebnis	259
IV. Zwischenergebnis	259
§ 21 Zwischenergebnis: Rechtsschutzlücken im deliktischen Schutz von Datenbeständen	259
§ 22 Lösungsansätze: Absolute Rechtspositionen am Datenbestand	261
I. Bedürfnis nach einer Haftungserweiterung	261
1. Lückenhafter deliktischer Schutz von Datenbeständen	261
2. Gesteigerte Bedeutung digitaler Inhalte in der Cloud	262
3. Erweiterungstendenzen in Rechtsprechung und Literatur	263
4. Zwischenergebnis	264
II. Eigentum am Datenbestand	265
1. Problemstellung	265
2. Meinungsstand	266
3. Rechtsprechung des BGH	267
4. Stellungnahme	268
III. Besitz am Datenbestand	272
1. Meinungsstand	272
2. Stellungnahme	273
IV. Zwischenergebnis	274
V. Recht am generierten Datenbestand	275
1. Bisherige Lösungsansätze in der Literatur	275
a) Meinungsstand	275
b) Stellungnahme	277
c) Vorzüge gegenüber der Anerkennung von sonstigen absoluten Rechten am Datenbestand	278
2. Dogmatische Herleitung	279
a) Anknüpfungspunkt	279
b) Grundlegende Voraussetzungen	280
aa) Zuweisungsfunktion	281
bb) Ausschlussfunktion	281
c) Schutzwürdigkeit	284

3. Personelle Zuordnung	285
a) Problemstellung bei der Zuweisung von Rechtspositionen an Daten	285
b) Potentielle Anknüpfungspunkte	286
aa) Anknüpfung an die inhaltliche Betroffenheit	286
bb) Anknüpfung an faktische Ausschlussmöglichkeiten	287
cc) Anknüpfung an den Datenträger	287
dd) Anknüpfung an die Urheberschaft	289
(1) Ausgangspunkt	289
(2) Kritik	289
(3) Stellungnahme	290
ee) Anknüpfung an den Skripturakt	291
(1) Ausgangspunkt	291
(2) Eignung als Zuordnungskriterium	292
(3) Datenscriptur in Weisungsverhältnissen	293
(a) Meinungsstand	293
(b) Stellungnahme	293
c) Zwischenergebnis	294
4. Terminologische Abgrenzung	295
5. Schutzzumfang und Grenzen	297
a) Geschütztes Rechtsgut	297
aa) Betriebsrelevante Daten	297
bb) Ausschließlich personenbezogene Daten	298
cc) Lokal gespeicherte Daten	298
b) Verletzungshandlungen	299
aa) Ausgangspunkt	299
bb) Ausspähung von Daten	299
cc) Datenmanipulation	301
dd) Datenvernichtung	302
c) Anwendung einschränkender Kriterien	302
6. Verschulden	303
7. Zwischenergebnis	304
§ 23 Ergebnis: Deliktische Haftung im Cloud Computing	305
6. Kapitel Ersatzfähiger Schaden	306
§ 24 Grundlagen der Schadensquantifizierung	306
I. Maßgebliche Haftungsszenarien	306

II. Grundlegende Berechnung der Schadenshöhe	306
§ 25 Konkrete Schadenspositionen im Zusammenhang mit dem Verlust von Daten	307
I. Datenwiederherstellung	307
1. Haftung des externen Hackers	308
2. Haftung des berechtigten Mitnutzers	309
3. Haftung des Cloud-Anbieters	310
II. Datenneuerfassung	310
1. Haftung des externen Hackers	311
2. Haftung des berechtigten Mitnutzers	311
3. Haftungs des Cloud-Anbieters	312
III. Entgangener Gewinn	312
1. Maßgebliche Haftungsszenarien	312
2. Beweismaßstab	313
3. Praxisrelevanz	313
§ 26 Der Verlust von Daten als selbstständige Schädigungsfolge	313
I. Ausgangspunkt	314
II. Am Markt handelbare Daten	314
III. Sonstige private Daten	316
IV. Unternehmensdaten mit betrieblicher Relevanz	319
V. Zwischenergebnis: Der materielle Wert von Daten	321
§ 27 Ergebnis	322
7. Kapitel Rechtfertigungsgründe für die Löschung von Daten	323
§ 28 Rechtfertigung einer Datenlöschung durch den Cloud-Anbieter	323
I. Rechtfertigung der Datenlöschung im Rahmen einer Vertragsbeziehung	323
1. Maßgebliches Haftungsszenario	323
2. Rechtfertigende Wirkung der Löschungsverpflichtung	324
a) Dogmatische Einordnung	324
b) Bestehen einer vertraglichen Löschungsbefugnis	325
aa) Grundsatz	325
bb) Ausgestaltung der Klausel	326
c) Fehlen einer vertraglichen Regelung: Ergänzende Vertragsauslegung	326
aa) Vorliegen einer vertraglichen Regelungslücke	327
bb) Ausfüllung der vertraglichen Regelungslücke	328

II. Rechtfertigung der Datenlöschung bei Fehlen einer Vertragsbeziehung	329
1. Maßgebliches Haftungsszenario	329
2. Rechtfertigender Notstand gemäß § 34 StGB	330
a) Systematik	330
b) Notstandslage	331
aa) Maßstab der Gefahrenermittlung	331
bb) Take-down bei vollständiger und zutreffender Sachverhaltskenntnis	332
cc) Take-down bei unvollständiger Sachverhaltskenntnis	332
c) Notstandshandlung	333
3. Geschäftsführung ohne Auftrag	334
a) Anwendbarkeit	335
b) Fremdheit des Geschäfts	335
c) Berechtigung der Geschäftsführung	336
4. Virtuelles Hausrecht	336
a) Meinungsstand	337
b) Stellungnahme	338
5. Rechtfertigende Pflichtenkollision	339
a) Dogmatische Einordnung	340
b) Voraussetzungen	341
III. Zwischenergebnis	342
§ 29 Rechtfertigung einer Datenlöschung durch den Cloud-Nutzer	343
I. Maßgebliches Haftungsszenario	343
II. Ausgangspunkt: § 859 BGB	344
III. Geschäftsführung ohne Auftrag	345
§ 30 Ergebnis	346
8. Kapitel Beweisrechtliche Aspekte	347
§ 31 Grundlegende Nachweisschwierigkeiten im Cloud Computing	347
§ 32 Der Nachweis haftungsbegründender Merkmale durch den Cloud-Nutzer	348
I. Grundlegende Verteilung der Beweislast	348
II. Anspruch gegen den Cloud-Anbieter aus § 536 a BGB	349
1. Maßgebliches Haftungsszenario	349

2. Nachweis der Mangelhaftigkeit der Mietsache	349
a) Ausgangspunkt der Rechtsprechung	349
b) Kritik und Stellungnahme	350
c) Abgrenzung nach Risikosphären	352
d) Beweisantritt im Prozess	353
3. Nachweis des Vertretenmüssens	354
4. Nachweis des Schadenseintritts	355
a) Problemstellung	355
b) Beweiserleichterung aus § 287 ZPO	356
aa) Grundsatz	356
bb) Quantifizierung des Verlustschadens	357
cc) Eintritt eines Schadens	358
c) Beweisantritt im Prozess	359
5. Nachweis der Kausalität	360
6. Zwischenergebnis	360
III. Anspruch gegen den Cloud-Anbieter aus § 280	
Abs. 1 BGB	360
1. Maßgebliches Haftungsszenario	360
2. Nachweis der Pflichtverletzung	361
3. Nachweis des Vertretenmüssens	361
4. Nachweis der Kausalität	362
a) Grundsatz	362
b) Verletzung der Verpflichtung zur Abwehr schädlicher natürlicher Einflüsse und externer Angriffe	363
aa) Sachverständigenbeweis	363
(1) Grundsätzliche Relevanz im IT-Prozess	363
(2) Besonderheiten im Cloud-Bereich	364
(a) Zugriffsverweigerung durch den Cloud-Anbieter	365
(aa) Zumutbarkeit	365
(bb) Ermessensentscheidung	365
(b) Beweissicherung	367
(aa) Ausgangspunkt	367
(bb) Besorgnis der Beweiserschwerung	368
(cc) Beweissicherungsbeschluss für Cloud-Daten	369
(c) Auslandsbezug	369

(aa) Einbeziehung des Zielstaats	370
(bb) Fehlende Durchsetzbarkeit vor nationalen Gerichten	370
bb) Zeugenbeweis	371
cc) Inaugenscheinnahme	371
dd) Anordnung der Vorlegung durch die Gegenpartei	372
ee) Zwischenergebnis	373
c) Verletzung der Verpflichtung zur Datensicherung	373
aa) Beweislastumkehr durch die Rechtsprechung	373
bb) Datensicherung durch den Cloud-Anbieter	374
IV. Schadensersatzanspruch gegen den externen Hacker	375
1. Maßgebliches Haftungsszenario	375
2. Nachweis einer Verletzungshandlung	375
3. Nachweis des Verschuldens	376
4. Nachweis der Kausalität	376
5. Nachweis der Belegenheit der Daten im Schädigungszeitpunkt	376
a) Problemstellung	376
b) Dem Cloud-Anbieter bekannter Belegenheitsort	377
c) Unaufklärbarkeit des Belegenheitsorts	377
V. Schadensersatzanspruch gegen den berechtigten Mitnutzer	378
1. Maßgebliches Haftungsszenario	378
2. Nachweis einer Verletzungshandlung	379
3. Nachweis des Verschuldens	379
4. Zwischenergebnis	379
§ 33 Zwischenergebnis: Unbefriedigende Beweissituation	380
§ 34 Lösungsansätze: Modifizierung der Darlegungs- und Beweislast	381
I. Grundlagen	381
1. Beweislastumkehr	381
a) Dogmatische Einordnung	381
b) Voraussetzungen und Fallgruppen	383
c) Rechtsfolge	384
2. Sonstige Beweiserleichterungen	385
a) Anscheinsbeweis	385
b) Reduzierung des Beweismaßes	386
c) Sekundäre Darlegungslast	387

II. Anspruch gegen den Cloud-Anbieter aus § 536 a BGB	388
1. Nachweis der Mangelhaftigkeit der Mietsache	388
2. Nachweis des Vertretenmüssens	389
3. Nachweis des Schadenseintritts	389
4. Nachweis der Kausalität	390
5. Zwischenergebnis	390
III. Anspruch gegen den Cloud-Anbieter aus § 280 Abs. 1 BGB	390
1. Nachweis der Pflichtverletzung	390
2. Nachweis des Verschuldens	391
3. Nachweis der Kausalität	392
a) Verletzung der Verpflichtung zur Abwehr schädlicher natürlicher Einflüsse und externer Angriffe	392
b) Verletzung der Verpflichtung zur Datensicherung	393
4. Zwischenergebnis	394
IV. Schadensersatzanspruch gegen den externen Hacker	394
1. Nachweis der Verletzungshandlung	394
2. Nachweis des Verschuldens	395
3. Nachweis der Kausalität	395
V. Schadensersatzanspruch gegen den berechtigten Mitnutzer	395
§ 35 Ergebnis: Beweisführung im Cloud Computing	396
9. Kapitel Zusammenfassung der Ergebnisse	398
§ 36 Anwendbares Recht	398
§ 37 Vertragliche Haftung	399
§ 38 Deliktische Haftung	401
§ 39 Ersatzfähiger Schaden	402
§ 40 Beweisrechtliche Aspekte	403
§ 41 Gesamtergebnis	404
Literaturverzeichnis	407

## Abkürzungsverzeichnis

a.A.	anderer Ansicht
a.a.O.	am angegebenen Ort
Abs.	Absatz/Absätze
ADSp	Allgemeine Deutsche Spediteurbedingungen
a.F.	alte Fassung
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
Alt.	Alternative
Amtsbl.	Amtsblatt
Anm.	Anmerkung
ArbG	Arbeitsgericht
Art.	Artikel
ASP	Application Service Providing
Aufl.	Auflage
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
Begr.	Begründer/Begründung
BGB	Bürgerliches Gesetzbuch
BGBL.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BKA	Bundeskriminalamt
BPaaS	Business Process as a Service
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise

## *Abkürzungsverzeichnis*

CaaS	Communication as a Service
CPU	Central Processing Unit
CRM	Customer Relationship Management
DaaS	Data Storage as a Service
ders./dies .	Derselbe/Dieselbe(n)
d.h.	das heißt
ebd.	ebenda
EC-Karte	Electronic Cash-Karte
EDV	Elektronische Datenverarbeitung
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche
et al.	et alii
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGVÜ	Übereinkommen über die gerichtliche Zuständigkeit und die Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen
EuGVVO	Verordnung über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen
EWR	Europäischer Wirtschaftsraum
f./ff.	folgende
Fn	Fußnote
gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
HGB	Handelsgesetzbuch
h.M.	herrschende Meinung
Hrsg.	Herausgeber
Hs.	Halbsatz
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPR	Internationales Privatrecht

i.S.d.	im Sinne des/der
ISO	International Organization for Standardization
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria
i.V.m.	in Verbindung mit
Kap.	Kapitel
KFZ	Kraftfahrzeug
krit.	kritisch
LAG	Landesarbeitsgericht
LG	Landgericht
lit.	litera
M&A	Mergers and Acquisitions
MarkenG	Markengesetz
n.F.	neue Fassung
NIST	National Institute of Standards and Technology
Nr.	Nummer
NSA	National Security Agency
o.ä.	oder ähnlich/es
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PaaS	Platform as a Service
ProdHaftG	Produkthaftungsgesetz
Rn	Randnummer
Rom I-VO	Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht („Rom I“)
Rom II-VO	Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates vom 11. Juli 2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht („Rom II“)
S.	Satz/Seite
SaaS	Software as a Service
SecaaS	Security as a Service
SLA	Service Level Agreements

## *Abkürzungsverzeichnis*

sog.	sogenannte/r/n
StGB	Strafgesetzbuch
TCDP	Trusted Cloud Datenschutzprofil
TMG	Telemediengesetz
u.a.	unter anderem
Uabs.	Unterabsatz
UrhG	Urheberrechtsgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	von/vom
v.a.	vor allem
Var.	Variante
VG	Verwaltungsgericht
vgl.	vergleiche
WLAN	Wireless Local Area Network
XaaS	Everything as a Service
z.B.	zum Beispiel
ZPO	Zivilprozessordnung
z.T.	zum Teil

# 1. Kapitel Einführung

## § 1 Einleitung

### I. Cloud Computing: Siegeszug einer innovativen Informationstechnologie

Eine Studie der EMC Corporation geht davon aus, dass im Jahr 2020 weltweit 44 Milliarden Terabyte an Daten produziert werden.<sup>1</sup> Dieser immense Datenbestand führt zu einem ebenso ausgeprägten Bedürfnis nach Rechen- und Speicherkapazitäten. Viele Unternehmen sehen sich außerstande oder halten es zumindest für wirtschaftlich wenig sinnvoll, selbst die hierfür erforderlichen IT-Ressourcen vorzuhalten.

Die Auslagerung von IT-Leistungen im Wege des Cloud Computing wird deshalb als eines der zentralen zukünftigen Gestaltungsmodelle der Informationsverwaltung gehandelt.<sup>2</sup> Gleichzeitig wirft diese IT-Lösung zahlreiche rechtliche Probleme auf, deren Auflösung durch die Rechtswissenschaft aktuell noch nicht mit der rasant fortschreitenden wirtschaftlichen Entwicklung des Cloud Computing Schritt halten kann.

Der zweite die aktuelle IT-Landschaft prägende Trend wird unter dem Schlagwort Big Data zusammengefasst, womit der Einsatz großer Datenmengen aus vielfältigen Quellen mit hoher Verarbeitungsgeschwindigkeit zur Erzeugung wirtschaftlichen Nutzens bezeichnet wird.<sup>3</sup> Wie bereits dargelegt steigt die Masse der weltweit generierten Daten kontinuierlich an, was nicht zuletzt auf die stärkere Vernetzung mobiler Endgeräte und das immer mehr in den Fokus rückende Interesse von Konzernen an möglichst umfassenden Datenbanken zurückzuführen ist.

Eine effiziente Ansammlung, Verwaltung und Analyse dieser uneinheitlichen, aus gänzlich unterschiedlichen Quellen stammenden Datenmassen

---

1 EMC Digital Universe Study, Executive Summary; vgl. hierzu auch *Roth-Neuschild*, ITRB 2013, 213.

2 *Friederichs*, IT-Trends für das Jahr 2016; so zuvor bereits *Spender*, Top 10 Strategic Technology Trends for 2015.

3 BITKOM, Big-Data-Technologien, S. 12; *Peschel/Rockstroh*, MMR 2014, 571; *Ziegler/Smirra*, MMR 2013, 418; vgl. auch *Dorner*, CR 2014, 617; *F. Koch*, ITRB 2015, 13.

wirkt auf Unternehmen besonders attraktiv, da sich so das eigene Geschäftsmodell passgenauer als jemals zuvor auf die Bedürfnisse der (potentiellen) Kundschaft ausrichten lässt. Die massenhafte Ansammlung und Auswertung von Daten ist mit konventioneller, rein standortgebundener Datenverarbeitung kaum zu leisten. Erforderlich ist vielmehr, dass unabhängig vom Serverstandort Einfluss auf den Datenbestand genommen werden kann, um eine effiziente Verwaltung von großen Datenmengen sicherzustellen. Dies kann insbesondere durch den Einsatz von Cloud-Technologie geleistet werden.<sup>4</sup>

## II. Praktische Relevanz von Haftungsfragen in der Cloud

Das Cloud Computing verfügt wie eingangs dargestellt über ein erhebliches Wachstumspotential, so dass diese Verarbeitungsform zukünftig noch deutlich weitflächiger auftreten dürfte. Hierdurch werden auch anknüpfende Rechtsfragen wie die Verantwortlichkeiten im Haftungsfall besonders virulent. Zudem geht mit dem Verlust von Daten bzw. deren Integrität für Unternehmen typischerweise ein besonders signifikanter Vertrauensverlust einher, der das Firmenimage nachhaltig beschädigen kann.<sup>5</sup>

Insbesondere die Haftung des außenstehenden Hackers, der sich unbefugt Datenzugriff verschafft,<sup>6</sup> weist große praktische Relevanz auf. Dies zeigen die bisher publik gewordenen Angriffe auf große Cloud-Anbieter, die insbesondere zur unbefugten Kenntnisnahme von Nutzerdaten, aber auch zur unkontrollierten Verbreitung privater Inhalte geführt haben.<sup>7</sup> Schließlich hat dieser Aspekt nicht zuletzt durch die Aufdeckung massiver Überwachung durch den amerikanischen Auslandsgeheimdienst NSA er-

---

4 Vgl. zur Bedeutung des Cloud Computing für Big Data BITKOM, Big-Data-Technologien, S. 15; Fraunhofer ISI, Projektbeschreibung Big Data in der Cloud; *F. Koch*, ITRB 2015, 13, 14; *Rofsnagel*, ZD 2013, 562.

5 Vgl. hierzu *Mommers*, Datenverlust im Unternehmen; Angst vor Image-Schaden, PC Welt vom 12.06.2008.

6 Vgl. hierzu unten § 2 I.

7 So etwa bei Angriffen auf Evernote, vgl. Hackerangriff auf Evernote, Spiegel Online vom 02.03.2013; Dropbox, vgl. *Bott*, Dropbox gets hacked sowie zuletzt besonders medienwirksam auf die Apple iCloud mit Zielrichtung auf prominente Privatfotos, vgl. Apple weist Mitschuld an Hackerangriff zurück, Spiegel Online vom 03.09.2014.

heblich an Brisanz gewonnen.<sup>8</sup> Die Ursache für derartige Vorkommnisse ist maßgeblich in der Vervielfältigung der potentiellen Angriffswege für externe Angreifer zu sehen, die aus der technologischen Ausgestaltung des Cloud Computing folgt.<sup>9</sup>

Doch auch die Verantwortlichkeit des Cloud-Anbieters, der hinreichende Sicherheitsvorkehrungen gegen derartige unbefugte Zugriffe treffen muss, ist von praktischer Relevanz.<sup>10</sup> Sowohl für private Nutzer, die ggf. bedeutsame persönliche Dateien einbüßen; als auch für Unternehmen, deren wirtschaftliche Existenz unter Umständen an den Zugriff auf einen konkreten Datenbestand gekoppelt ist, ist die Frage nach angemessener Kompensation von großer Bedeutung. Zudem ist der Cloud-Anbieter in diesem Haftungsszenario<sup>11</sup> als Gegner etwaiger Schadensersatzansprüche – anders als der externe Angreifer – zumindest dem Grunde nach greifbar.

Schließlich eröffnet die fortschreitende Verbreitung des Cloud Computing auch neue Anwendungsfelder für vertiefte Kooperationen im unternehmerischen Kontext.<sup>12</sup> Doch auch hierbei ergeben sich haftungsrechtliche Besonderheiten. Dies gilt namentlich für den Fall, in dem es zu einer versehentlichen Löschung von Daten durch andere Nutzer einer solchen Cloud-Lösung kommt.<sup>13</sup>

### III. Haftung für Datenverlust: Quo vadis?

Sofern Cloud Computing bisher Gegenstand der juristischen Diskussion war, lag der Schwerpunkt üblicherweise auf datenschutzrechtlichen As-

---

8 Vgl. hierzu Geheimdienst analysiert umfassend soziale Beziehungen, heise online vom 30.09.2013.

9 Vgl. hierzu unten § 13 II. 1. b) cc).

10 Vgl. hierzu unten § 13.

11 Vgl. hierzu unten § 2 I. 3.

12 Vgl. hierzu unten § 2 II. 1.

13 Vgl. hierzu unten § 21.

pekten.<sup>14</sup> Auch Randgebiete wie das Straf-<sup>15</sup> oder Urheberrecht<sup>16</sup> wurden bereits erörtert. Die haftungsrechtliche Perspektive des Cloud Computing war dagegen bisher nur vereinzelt Gegenstand der wissenschaftlichen Diskussion.<sup>17</sup>

Dies überrascht zunächst, da die technische Ausgestaltung dieser Technologie in vielerlei Hinsicht Anlass gibt, die korrespondierenden haftungsrechtlichen Fragestellungen zu ergründen.<sup>18</sup> Insbesondere im Bereich der deliktischen Haftung ist zu hinterfragen, ob konventionelle Anknüpfungspunkte im Rahmen der Haftung für Datenverlust diese Besonderheiten des Cloud Computing angemessen berücksichtigen.<sup>19</sup>

Der fortschreitenden technologischen Entwicklung soll im Folgenden mit einer umfassenden Untersuchung der zivilrechtlichen Haftungsgrundlagen zugunsten des vom Datenverlust betroffenen Cloud-Nutzers und der Entwicklung von Lösungsansätzen für den Fall etwaiger Rechtsschutzlücken Rechnung getragen werden.

- 
- 14 Vgl. etwa *Borges/Brennscheidt*, in: *Borges/Schwenk*, S. 43 ff.; *Brennscheidt*, *Cloud Computing und Datenschutz*; *Gaul/Koehler*, BB 2011, 2229, 2230 ff.; *Haag*, in: *Leupold/Glossner*, Teil 4 C. III. Rn 37 ff.; *Heidrich/Wegener*, MMR 2010, 803; *Jotzo*, *Der Schutz personenbezogener Daten in der Cloud*; *Kühling/Biendl*, CR 2014, 150; *Meents*, in: *Lehmann/Meents*, Kapitel 7 F. Rn 177 ff.; *Nägele/Jacobs*, ZUM 2010, 281, 289 f.; *Rath/Rothe*, K&R 2013, 623; *Schulz*, MMR 2010, 75, 78 f.; *Splittgerber/Rockstroh*, BB 2011, 2179, 2180 ff.; *Thüsing/Pötters*, in: *Thüsing, Beschäftigendatenschutz und Compliance*, § 15 III. Rn 13 ff.
- 15 *Gercke*, CR 2010, 345; *MüKo-StGB/Graf*, § 202 a Rn 87; *Härting*, ITRB 2011, 242, 243; *Kroschwald/Wicker*, CR 2012, 758; *Niemann/Paul*, K&R 2009, 444, 451; *Ramos/Vonhoff*, CR 2013, 265, 269 ff.; *Redeker*, ITRB 2014, 232; *Wicker*, *Cloud Computing und staatlicher Strafanspruch*, S. 99 ff.; strafprozessuale Aspekte hervorhebend *Mahn*, in: *Böttger, Wirtschaftsstrafrecht*, Kapitel 10 D. II. 2. Rn 229; *Obenaus*, NJW 2010, 651, 652 ff.
- 16 *Bises*, MMR 2012, 574; *Hilber/Reintzsch*, CR 2014, 697; *Klett*, ZUM 2014, 18; *Lehmann/Giedke*, CR 2013, 681; *Meents*, in: *Lehmann/Meents*, Kapitel 7 i. IV. 5. Rn 271 ff.; *Nägele/Jacobs*, ZUM 2010, 281, 284 ff.; *Niemann/Paul*, K&R 2009, 444, 448; *Schuster/Reichl*, CR 2010, 38, 40 f.; *Splittgerber/Rockstroh*, BB 2011, 2179, 2179 ff.
- 17 Vgl. etwa *Borges*, in: *Borges/Meents*, § 12 I. Rn 1 ff.; *Intveen/Hilber/Rabus*, in: *Hilber*, Teil 2 IV. 5.; *Kompetenzzentrum Trusted Cloud, Leitfaden Vertragsgestaltung*, S. 24 ff.; *Wicker*, MMR 2014, 715; *dies.*, MMR 2012, 783.
- 18 Vgl. hierzu unten § 4 II.
- 19 Vgl. hierzu unten § 17.

§ 2 Gegenstand der Untersuchung: Maßgebliche Haftungsszenarien

Die Haftung im Bereich des Cloud Computing eröffnet neuartige rechtliche Problemstellungen, die im Kontext vielfältiger Fallgestaltungen auftreten und auf unterschiedlichsten Ursachen basieren.<sup>20</sup> Zur sachgerechten Analyse dieser Problemfelder ist es daher unerlässlich, zunächst überblicksartig darzustellen, welche Haftungsszenarien in der nachfolgenden Abhandlung untersucht werden, woraus diese resultieren und welches Rechtsverhältnis hierbei maßgeblich sein soll.

Die nachfolgend dargestellten Szenarien unterscheiden maßgeblich danach, durch wen auf welche Art und Weise Zugriff auf Datenbestände in der Cloud genommen wurde. Gegenstand der Untersuchung sind jeweils ausschließlich Schadensersatzansprüche zugunsten des vom Datenverlust betroffenen Cloud-Nutzers. Nicht erörtert werden dagegen Ersatzansprüche des Cloud-Anbieters etwa gegen den externen Angreifer, den Hersteller von Hardware oder den Cloud-Nutzer.

I. Hackerangriff auf die Cloud durch externe Dritte

1. Haftungsszenario

Zunächst kann ein Schaden dadurch entstehen, dass sich ein externer Angreifer Zugang zu in der Cloud hinterlegten Daten verschafft und diese verändert bzw. endgültig löscht.<sup>21</sup> Zu denken ist insbesondere an das klassische Szenario eines Hacker-Angriffs, wobei Ziel des Angriffs hier nicht der lokale Datenbestand eines Endnutzers, sondern dessen in der Cloud hinterlegten Daten sind. Ein populärer Beispielfall ist die vollständige Vernichtung des digitalen Informationsbestands des Journalisten *Mat Honan*, der durch einen Hacker-Angriff den Großteil seiner in der Cloud hinterlegten Daten verlor.<sup>22</sup>

Denkbar ist auch, dass ein derartiger Angriff ausschließlich den Verlust unternehmensbezogener Daten nach sich zieht, die gleichfalls ein attraktives Ziel für Angreifer darstellen – etwa um potente Mitbewerber nachhal-

---

20 Vgl. *Borges*, in: *Borges/Meents*, § 12 I. Rn 1.

21 Vgl. *Borges*, in: *Borges/Meents*, § 12 I. Rn 2.

22 *Honan*, How Apple and Amazon security flaws led to my epic hacking.

## 1. Kapitel Einführung

tig zu schädigen.<sup>23</sup> Die Geltendmachung von Ersatzansprüchen für den Verlust derartiger Datensätze unterfällt anderen Maßstäben als bei ausschließlicher Betroffenheit privater Daten.<sup>24</sup>

## 2. Schadensursachen

Die Ursache für den Schadenseintritt liegt zunächst darin begründet, dass sich der außenstehende Dritte in rechtswidriger Art und Weise Zugriff auf den Datenbestand verschafft und diesen eigenmächtig beeinflusst. Ursächlich ist also primär das Verhalten des unmittelbaren Schädigers.

Für die hier maßgebliche Haftung des Cloud-Anbieters kommt nur ein mittelbarer Verursachungsbeitrag in Betracht: So muss der externe Angreifer zunächst zwingend diejenigen Sicherungsmechanismen überwunden haben, die der Cloud-Anbieter zur Verhinderung derartiger Fremdzugriffe etabliert hat. Dementsprechend drängt sich in diesem Szenario die Untersuchung der Frage auf, ob diese Vorkehrungen als nicht hinreichend eingestuft werden müssen.<sup>25</sup>

## 3. Haftungsadressaten

Da dieses Haftungsszenario maßgeblich durch das schädigende Verhalten des externen Angreifers geprägt ist, stehen zunächst Schadensersatzansprüche des Cloud-Nutzers gegen diesen im Fokus der Betrachtung.<sup>26</sup> Jedoch ist wie gesehen durchaus vorstellbar, dass der Zugriff durch den Dritten erst dadurch möglich geworden ist, dass der Cloud-Anbieter keine hinreichenden Sicherheitsvorkehrungen hiergegen getroffen hat. Dementsprechend sind in diesem Haftungsszenario auch Ersatzansprüche gegen den Cloud-Anbieter zu untersuchen.<sup>27</sup>

---

23 Vgl. zur wettbewerbsrechtlichen Haftung unten § 20 II.

24 Vgl. hierzu unten § 26.

25 Vgl. hierzu unten § 13 II. 1.

26 Vgl. hierzu unten 5. Kapitel.

27 Vgl. hierzu unten § 13 II.

## II. Beeinflussung von Datenbeständen durch grundsätzlich berechnigte Cloud-Nutzer

### 1. Haftungsszenario

Weiterhin ist als potentielles Haftungsszenario denkbar, dass im Rahmen einer Cloud-Lösung mit mehreren nutzungsberechnigten Anwendern Datensätze beeinträchtigt oder entfernt werden, die einem anderen Cloud-Nutzer zugeordnet waren. Zu denken wäre etwa an eine Private Cloud<sup>28</sup>-Lösung, auf die sämtliche Mitarbeiter eines Unternehmens Zugriff haben.

Ein weiteres Anwendungsbeispiel in größerem Kontext ist die Kooperation von Unternehmen bei Projekten im Rahmen der sog. Industrie 4.0:<sup>29</sup> Zur Optimierung von Fertigungs- und Vertriebsprozessen müssen mehrere beteiligte Unternehmen ständig auf einen umfangreichen Datensatz zugreifen können, der sinnvoll nur im Wege einer Cloud-Lösung bereitgestellt werden kann. Bedeutsam für die haftungsrechtliche Analyse ist hierbei, dass im Rahmen der sog. sternförmigen Kooperation nur Vertragsbeziehungen zu dem koordinierenden Zentralunternehmen, nicht aber zu den sonstigen Vertragspartnern bestehen, die an der Leistungserbringung beteiligt sind.<sup>30</sup> Auch ein Vertragsverhältnis zum Cloud-Anbieter wird in dieser Fallgruppe häufig nur das leitende Unternehmen unterhalten.

Ein anderes Praxisbeispiel für den Zugriff auf eine Cloud-Lösung, bei der weder zwischen den einzelnen berechnigten Cloud-Nutzern noch im Verhältnis zum Cloud-Anbieter ein Vertragsverhältnis besteht, ist schließlich die Nutzung eines sog. Virtual Data Rooms im Rahmen von M&A-Transaktionen:<sup>31</sup> Auch hier erhalten alle Beteiligte (Mitarbeiter, Wirtschaftsprüfer, Rechtsanwälte) Zugriff auf das Portal, um die eingestellten Inhalte einsehen und prüfen zu können, ohne dass entsprechende Vertragsverhältnisse bestünden. Die Einschaltung des Cloud-Anbieters erfolgt hier typischerweise durch die zu erwerbende Gesellschaft. Rechtsanwälte und Wirtschaftsprüfer sind dagegen im Regelfall jeweils von der potentiell erwerbenden Gesellschaft eingeschaltet, sodass diese kein Vertragsverhältnis zum Cloud-Anbieter oder gar untereinander unterhalten.

---

28 Vgl. hierzu unten § 5 II.1.

29 Vgl. hierzu BMWi, Umsetzungsstrategie Industrie 4.0, S. 10.

30 Vgl. hierzu BMWi, IT-Sicherheit für die Industrie 4.0, S. 92; *Rohe*, Netzverträge, S. 389.

31 Vgl. zu diesem Verfahren *Gole/Hilger*, Corporate Divestitures, S. 135.

## 1. Kapitel Einführung

### 2. Schadensursache

Auch hier war zunächst das Verhalten des Cloud-Nutzers als unmittelbarer Schädiger ursächlich, welches den Datenbestand eines berechtigten Mitbenutzers beeinträchtigt hat. Im Übrigen soll davon ausgegangen werden, dass es gerade dem Modell der kooperativen Cloud-Lösung entspricht, dass alle Nutzungsberechtigten grundsätzlich auf sämtliche Daten zugreifen können – ein Verursachungsbeitrag des Cloud-Anbieters, etwa in Form des Unterlassens weiter gehender Zugriffsbeschränkungen, kann daher insofern ausgeschlossen werden.

In diesem Haftungsszenario liegt es - anders als in demjenigen des externen Hackerangriffs - durchaus nahe, dass die Löschung von Datenbeständen nicht vorsätzlich erfolgt ist.<sup>32</sup> Während der Hacker stets bewusst einen Angriff auf fremde Daten initiiert, steht dem berechtigten Nutzer der Zutritt zur Plattform grundsätzlich offen und es ist nicht auszuschließen, dass etwa im Rahmen komplexer Projekte versehentlich fremde Dateien überschrieben oder gelöscht werden. Es ist folglich in diesem Haftungsszenario zumindest denkbar, dass fahrlässiges Verhalten für den Datenverlust ursächlich geworden ist.

### 3. Haftungsadressat

Anders als im obigen Haftungsszenario des Zugriffs eines externen Dritten auf den Datenbestand kommt hier wie dargestellt ein Verursachungsbeitrag des Cloud-Anbieters nicht in Betracht. Schadensersatzansprüche des geschädigten Cloud-Nutzers können sich daher allenfalls gegen den handelnden Nutzer selbst richten.

---

32 Vgl. hierzu ausführlich unten § 19 III. 4. c).

### III. Datenverlust bei Betrieb des Cloud-Dienstes durch den Cloud-Anbieter

#### 1. Haftungsszenario

Schließlich kann der Verlust von Daten auch ausschließlich auf einem Beitrag aus der Sphäre des Cloud-Anbieters beruhen, ohne dass hierbei Dritte involviert wären. Gemeint ist zunächst insbesondere diejenige Fallkonstellation, in der Fehlfunktionen im Betrieb des Cloud-Dienstes dazu führen, dass Daten des Cloud-Nutzers verloren gehen oder verändert werden. Ein großes Medienecho löste etwa der systembedingte Datenverlust im Rahmen des Cloud-Dienstes EC2 von Amazon aus.<sup>33</sup>

In dieses Haftungsszenario fällt auch die Fallgruppe, in der zufällige natürliche Ereignisse wie Blitzschlag, Feuer oder Überflutung durch physische Einflussnahme dazu führen, dass die Cloud-Infrastruktur Schaden nimmt und hierdurch Daten des Cloud-Nutzers verloren gehen. Dies kann etwa der Fall sein, wenn es aufgrund eines Brandes zur Vernichtung der für die Speicherung der Daten des Cloud-Nutzers eingesetzten Server kommt.

#### 2. Schadensursachen

In diesem Haftungsszenario führen fehlerhafte technische Rahmenbedingungen in der Infrastruktur des Cloud-Anbieters<sup>34</sup> zum Datenverlust. So war etwa im oben dargestellten Beispiel Amazon EC2 der Datenverlust durch einen Routingfehler im Rahmen eines Netzwerkupgrades ausgelöst worden.<sup>35</sup> Es stellt sich dann die Frage, ob bzw. unter welchen Voraussetzungen der Cloud-Anbieter für die entstandenen Schäden haftet.<sup>36</sup>

Im Falle unvorhersehbarer natürlicher Ereignisse wie Brand, Blitzschlag o.ä. ist auch insofern maßgeblich, ob entsprechende Schutzvorkehrungen hiergegen hätten getroffen werden können und müssen. Vor diesem

---

33 Vgl. hierzu *Ihlenfeld*, Amazon erklärt Ausfall seiner Cloud-Server.

34 Vgl. zu technischen Verlustursachen unten § 4 III.

35 *Ihlenfeld*, Amazon erklärt Ausfall seiner Cloud-Server.

36 Vgl. hierzu unten § 12 III.

Hintergrund ist insbesondere fraglich, ob und in welchem Ausmaß der Cloud-Anbieter entsprechende Sicherheitsvorkehrungen treffen muss.<sup>37</sup>

### 3. Haftungsadressat

In diesem Haftungsszenario kann sich die Haftung wiederum ausschließlich gegen den Cloud-Anbieter richten, der ggf. dafür Sorge tragen müsste, dass die von ihm verwendete Infrastruktur (sicherheits-)technisch dazu geeignet ist, den Cloud-Dienst ohne Datenverlust bereitzustellen.<sup>38</sup>

### § 3 Gang der Darstellung

Zur Beantwortung der maßgeblichen Rechtsfragen ist es unerlässlich, zunächst die technischen Grundlagen des Cloud Computing und die auftretenden Leistungsarten grundlegend zu erläutern.<sup>39</sup>

Sodann ist auf die Frage einzugehen, welches nationale Recht auf Haftungsfälle im Cloud Computing Anwendung findet.<sup>40</sup> Diese Frage gestaltet sich insbesondere im Bereich der deliktischen Haftung komplex, da die grundsätzlich vorgesehene Anknüpfung an den Ort des Schadenseintritts im Cloud Computing nur schwierig umzusetzen ist. Insofern wird die Möglichkeit einer alternativen Anknüpfungslösung zu untersuchen sein.

Der erste Schwerpunkt der Arbeit liegt sodann in der Betrachtung der vertraglichen Haftung im Bereich des Cloud Computing.<sup>41</sup> Zunächst wird die vertragstypologische Einordnung der Cloud Computing-Vereinbarung erörtert,<sup>42</sup> da diese rechtliche Qualifizierung von unmittelbarer Relevanz für das anwendbare vertragliche Haftungsregime ist. Maßgeblich für den Gang der Darstellung ist sodann die Unterscheidung der einzelnen Haftungsszenarien: Es wird untersucht, ob und unter welchen Voraussetzungen dem Cloud-Nutzer im Haftungsszenario des Datenverlusts während

---

37 Vgl. hierzu unten § 12 IV. 2. b).

38 Vgl. hierzu unten § 12.

39 Vgl. hierzu sogleich 2. Kapitel.

40 Vgl. hierzu unten 3. Kapitel.

41 Vgl. hierzu unten 4. Kapitel.

42 Vgl. hierzu unten § 10.

des Betriebs des Cloud-Dienstes<sup>43</sup> und in demjenigen eines externen Hackerangriffs<sup>44</sup> vertragliche Schadensersatzansprüche gegen den Cloud-Anbieter zustehen.<sup>45</sup> Schließlich wird in diesem Abschnitt die gängige Regelungspraxis der großen Cloud-Anbieter hinsichtlich ihrer Konformität mit den zuvor erarbeiteten Grundsätzen überprüft.<sup>46</sup>

Der zweite Schwerpunkt der Untersuchung befasst sich hiernach mit den Rechtsgrundlagen der deliktischen Haftung.<sup>47</sup> Auch hier wird anhand der zuvor herausgearbeiteten Haftungsszenarien differenziert: Maßgeblich sind hier insbesondere diejenigen Haftungsszenarien, in denen ein Vertragsverhältnis zum Schädiger fehlt wie etwa im Falle eines externen Hackerangriffs<sup>48</sup> oder bei Datenlöschung durch grundsätzlich mitberechtigte Cloud-Nutzer<sup>49</sup>. Es kann jedoch auch das Bestehen von Verkehrspflichten des Cloud-Anbieters relevant werden, sofern nicht zu jedem Cloud-Nutzer ein Vertragsverhältnis besteht.<sup>50</sup>

Im Hinblick auf die deliktische Haftung gestaltet sich bereits die Suche nach einer geeigneten Anspruchsgrundlage diffizil. § 823 Abs. 1 BGB<sup>51</sup> als zentrale deliktische Haftungsnorm bietet mehrere potentielle Anknüpfungspunkte für eine Haftung für Datenverlust, die zu untersuchen sind; gleiches gilt für Abs. 2 der Norm i.V.m. spezifischen Schutzgesetzen.<sup>52</sup> Auch eigenständige Anspruchsgrundlagen wie § 826 BGB oder § 1 ProdHaftG werden in diesem Rahmen erörtert.<sup>53</sup> Nur nach umfassender Prüfung sämtlicher potentiellen deliktischen Haftungsgrundlagen lässt sich beurteilen, ob bzw. in welchem Umfang Rechtsschutzlücken bestehen. Weiterhin soll aufgezeigt werden, ob und in welchem Umfang die Anerkennung ergänzender Rechtspositionen in diesem Bereich geboten ist.<sup>54</sup>

---

43 Vgl. hierzu oben § 2 III.

44 Vgl. hierzu oben § 2 I.

45 Vgl. unten §§ 11 ff.

46 Vgl. hierzu unten § 14.

47 Vgl. hierzu unten 5. Kapitel.

48 Vgl. hierzu oben § 2 I.

49 Vgl. hierzu oben § 2 II.

50 Vgl. hierzu unten § 18.

51 Vgl. hierzu unten § 17.

52 Vgl. hierzu unten § 19.

53 Vgl. hierzu unten § 20.

54 Vgl. hierzu unten § 22.

Schließlich wird in diesem Kontext auf potentielle Rechtfertigungsgründe für die Löschung von Daten eingegangen.<sup>55</sup>

Abschließend wird die in der Praxis bedeutsame prozessuale Nachweis-situation untersucht.<sup>56</sup> Ohne eine effiziente Möglichkeit zur Rechtsdurchsetzung ist dem Geschädigten mit dem Bestehen materiell-rechtlicher Ersatzansprüche wenig gedient. Auch in diesem Rahmen ist nach den eingangs dargestellten Haftungsszenarien zu differenzieren.<sup>57</sup> Fraglich ist, inwieweit haftungsbegründende Merkmale im Streitfall vom Cloud-Nutzer nachgewiesen werden müssen und können. Hierbei ist insbesondere die Verteilung der Beweislast kritisch zu hinterfragen, da diese gravierende Hindernisse für die Rechtsdurchsetzung des vom Datenverlust betroffenen Cloud-Nutzers implizieren kann.<sup>58</sup>

Die Arbeit schließt mit einer Zusammenfassung der Ergebnisse.<sup>59</sup>

---

55 Vgl. hierzu unten 7. Kapitel.

56 Vgl. hierzu unten 8. Kapitel.

57 Vgl. hierzu unten § 32 II ff.

58 Vgl. hierzu unten §§ 33 f.

59 Vgl. hierzu unten 9. Kapitel.

## 2. Kapitel Technische und organisatorische Grundlagen des Cloud Computing

Vor der Erörterung der wesentlichen rechtlichen Besonderheiten in der zivilrechtlichen Haftung sollen zunächst das dieser Arbeit zugrunde liegende Begriffsverständnis sowie die wesentliche technische Ausgestaltung der Cloud-Infrastruktur dargestellt werden. Diese Aspekte sind von entscheidender Bedeutung für die nachfolgende Untersuchung der zentralen haftungsrechtlichen Gesichtspunkte. Gleiches gilt für die wesentlichen organisatorischen Rahmenbedingungen wie insbesondere die zentralen über die Cloud bezogenen Leistungsarten und die hiervon jeweils betroffenen Nutzergruppen.

### § 4 Definition und technische Funktionsweise

#### I. Begriff und Abgrenzung

##### 1. Definitionsansätze

Der Begriff Cloud Computing umschreibt im Wesentlichen eine moderne Erscheinungsform in der Informationstechnologie, bei der Datenverarbeitung nicht auf dem lokalen System des Endnutzers, sondern auf der beim Cloud-Anbieter befindlichen IT-Infrastruktur erfolgt, welcher dem Cloud-Nutzer hierdurch Hardware oder sonstige Leistungen zur Verfügung stellt.<sup>60</sup>

Besondere Bekanntheit hat die technische Definition des NIST erlangt:<sup>61</sup>

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing re-

---

60 *Borges/Brennscheidt*, in: *Borges/Schwenk*, S. 46; *Brennscheidt*, *Cloud Computing und Datenschutz*, S. 20; *Engels*, K&R 2011, 548; *Lehmann/Giedke*, CR 2013, 608; vgl. auch *Bisges*, MMR 2012, 574; *Grünwald/Döpfkens*, MMR 2011, 287; *Heidrich/Wegener*, MMR 2010, 803; *Jotzo*, *Der Schutz personenbezogener Daten in der Cloud*, S. 19; *Stögmüller*, in: *Leupold/Glossner*, Teil 4 A. I. Rn 1.

61 *Mell/Grance*, *The NIST Definition of Cloud Computing*, S. 2.

sources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.”

Es existieren darüber hinaus weitere technische Definitionsansätze,<sup>62</sup> deren Differenzierungen im Detail für die rechtliche Beurteilung nicht entscheidend sind.<sup>63</sup> In rechtlicher Hinsicht ist maßgeblich, dass eine ortsunabhängige Abrufbarkeit von IT-Ressourcen ermöglicht wird, die von einem Anbieter bedarfsabhängig einer Vielzahl potentieller Nutzer zur Verfügung gestellt werden.<sup>64</sup>

## 2. Historische Entwicklung

Die gemeinsame Nutzung von Ressourcen ist nicht erst seit Verbreitung des Cloud Computing ein Entwicklungsziel der IT-Branche: Bereits in den 60er Jahren des vergangenen Jahrhunderts wurden im Rahmen des sog. time sharing CPU-Kapazitäten lokal an unterschiedliche Nutzer verteilt.<sup>65</sup> Im Rahmen der weiteren technologischen Entwicklung konnte in der Folge eine Umstellung auf netzwerkbasierte Ressourcenteilung erreicht werden.<sup>66</sup> Auch dieser Trend wurde früh erkannt: Bereits etwa<sup>67</sup> im Jahre 1990 postulierte *John Gage* von Sun Microsystems: „The Network is the Computer“.

Der Begriff des „Cloud Computing“ wurde im wissenschaftlichen Kontext erstmals 1997 vom Informatikprofessor *Ramnath Chellappa* während eines Vortrags in Dallas verwendet.<sup>68</sup> Populäre Dienste, die dem heute

---

62 Vgl. hierzu überblicksartig *Krcmar*, in: *Borges/Meents*, § 1 II. Rn 27 ff.

63 So auch *Borges/Brennscheidt*, in: *Borges/Schwenk*, S. 46.

64 *Brennscheidt*, *Cloud Computing und Datenschutz*, S. 20; *Giedke*, *Cloud Computing*, S. 5; *Grünwald/Döpfkens*, *MMR* 2011, 287; *Nägele/Jacobs*, *ZUM* 2010, 281; *Jotzo*, *Der Schutz personenbezogener Daten in der Cloud*, S. 19; vgl. zur technischen Umsetzung sogleich unten § 4 II.

65 Vgl. hierzu *Krcmar*, in: *Borges/Meents*, § 1 II. Rn 24.

66 *Krcmar*, in: *Borges/Meents*, § 1 II. Rn 25.

67 *Schuster/Reichl*, *CR* 2010, 38 sprechen von „vor 20 Jahren“, dem ohne zusätzliche Quellenangabe folgend *Bedner*, *Cloud Computing*, S. 53. Das IT-Fachmagazin *wired* beschreibt im Jahre 1996 einen Zeitpunkt „vor einigen Jahren“, vgl. *Reiss*, *Power to the People*.

68 *Despotovic-Zratic/Milutinovic/Belic*, *Handbook of Research*, S. 2.

vorherrschenden Verständnis von Cloud-Leistungen entsprachen, kamen erstmals 2006 in Form von Amazon EC2<sup>69</sup> sowie kurz darauf Google Docs<sup>70</sup> (2007) auf den Markt. Seitdem hat sich das Cloud Computing in verschiedensten Nutzungssegmenten etabliert und sieht sich weiterhin sehr positiven Wachstumsprognosen ausgesetzt.<sup>71</sup>

### 3. Abgrenzung von vergleichbaren Technologien

#### a) IT-Outsourcing

Abzugrenzen ist das Cloud Computing insbesondere vom konventionellen IT-Outsourcing,<sup>72</sup> bei dem es primär um die Auslagerung der Erbringung von IT-Leistungen auf ein selbstständiges Unternehmen geht. Der netzwerkbasierte Abruf von einer Vielzahl von Nutzern bereitgestellten Einzelleistungen<sup>73</sup> durch den Cloud-Nutzer steht hier nicht im Fokus.<sup>74</sup> Regelmäßig wird insofern eine eher individuelle Auslagerungslösung entworfen, die noch dazu keineswegs zwingend einen ortsunabhängigen Abruf von Diensten beinhalten muss. Die Schnittmenge zum Bereich des Cloud Computing kann daher äußerst gering ausfallen.

#### b) Application Service Providing

Erhebliche Parallelen zu SaaS-Angeboten<sup>75</sup> weist hingegen das sog. Application Service Providing (ASP) auf, das insbesondere aufgrund der einschlägigen Rechtsprechung des BGH<sup>76</sup> erheblichen Einfluss auf die juristische Diskussion zum Cloud Computing genommen hat. Dieses stellt letztlich eine weiterentwickelte Form des konventionellen IT-Outsourcings

---

69 Vgl. hierzu *Bedner*, Cloud Computing, S. 44.

70 Vgl. hierzu *Despotovic-Zratic/Milutinovic/Belic*, Handbook of Research, S. 2.

71 Vgl. hierzu oben § 1 I.

72 Vgl. hierzu *Krcmar*; in: Borges/Meents, § 1 I. Rn 6 ff.

73 Vgl. hierzu unten § 4 II. 4.

74 Vgl. zu dieser Abgrenzung auch *Brennscheidt*, Cloud Computing und Datenschutz, S. 44 ff.

75 Vgl. hierzu unten § 5 I. 2.

76 Vgl. hierzu unten § 10 II. 1. a).

dar, bei dem die Bereitstellung von Software online erfolgt. Dieses Merkmal weist auch eine klassische SaaS-Lösung auf.

Allerdings verbleibt es letztlich beim individuellen Zuschnitt der Lösung: Im Wege des ASP wird der Betrieb einer individuellen Softwarelösung ausgelagert und sodann ortsunabhängig abgerufen. Eine Verknüpfung von Ressourcen zur effizienten Leistungserbringung an eine Vielzahl von Nutzern findet dagegen grundsätzlich auch hier nicht statt.<sup>77</sup> Somit rückt das ASP zwar dichter an Cloud-Lösungen nach modernem Verständnis heran – letztlich bleibt es jedoch bei einer Outsourcing-Lösung, die ortsunabhängig zur Verfügung gestellt werden kann. Um eine Fallgruppe des Cloud Computing nach hier vertretenem Begriffsverständnis<sup>78</sup> handelt es sich mithin im Ergebnis nicht.

### c) Grid Computing

Schließlich ist begrifflich zu einem weiteren Vorläufer<sup>79</sup> moderner Cloud-Strukturen abzugrenzen; dem sog. Grid Computing. Dieses bezeichnet den netzwerkseitigen Zusammenschluss mehrerer Rechner, um mit erhöhter Leistungsfähigkeit bestimmte Aufgaben erledigen zu können.<sup>80</sup> Auch beim Cloud Computing nach heute vorherrschendem Verständnis kommt es zur Verknüpfung von IT-Ressourcen. Dies stellt wie dargelegt jedoch kein Novum in der Informationstechnologie dar.<sup>81</sup>

Die Bündelung von Ressourcen bei einem Anbieter zur Bereitstellung von Leistungen an einen breiten Nutzerkreis ist jedoch auch im Bereich des Grid Computing nicht vorgesehen.<sup>82</sup> Die bloße Vernetzung von Rechnern zur gemeinsamen Aufgabenerfüllung genügt gleichfalls nicht, um

---

77 *Bedner*, Cloud Computing, S. 62; *Brennscheidt*, Cloud Computing und Datenschutz, S. 43; *Nägele/Jacobs*, ZUM 2010, 281; vgl. zur abweichenden Struktur im Cloud Computing sogleich unten.

78 Vgl. hierzu oben § 4 I. 1.

79 So ausdrücklich *Kremer/Völkel*, CR 2015, 501, 503; Cloud Computing ähnlich als „Weiterentwicklung“ bezeichnend *Jotzo*, Der Schutz personenbezogener Daten in der Cloud, S. 19.

80 *Grützmacher*, CR 2011, 697, 702; *Hoeren/Spittka*, MMR 2009, 583, 589; *Söbbing*, MMR 2008, XII; vgl. auch *Kremer/Völkel*, CR 2015, 501, 503.

81 Vgl. zur historischen Entwicklung oben § 4 I. 2.

82 Vgl. *Hoeren/Spittka*, MMR 2009, 583, 589; *Weiss*, in: *Niemann/Paul*, Kapitel 3 B. Rn 7.