Internet und Recht 16

Peter Schneidereit

Haftung für Datenverlust im Cloud Computing

Nomos

Internet und Recht

Herausgegeben von

Prof. Dr. Georg Borges
Universität des Saarlandes

Band 16

Peter Schneidereit

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

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 Schneidereit, welche finanziell, aber auch in jeder anderen erdenklichen

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

Mülheim an der Ruhr Dr. Peter Schneidereit

Inhaltsverzeichnis

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

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 Institue 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

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.[1] 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.[2] 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.[3] 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.[4]

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.[5]

Insbesondere die Haftung des außenstehenden Hackers, der sich unbefugt Datenzugriff verschafft,[6] 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.[7] 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; *Roßnagel,* 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.[8] 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.[9]

Doch auch die Verantwortlichkeit des Cloud-Anbieters, der hinreichende Sicherheitsvorkehrungen gegen derartige unbefugte Zugriffe treffen muss, ist von praktischer Relevanz.[10] 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[11] 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.[12] 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.[13]

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

Dies überrascht zunächst, da die technische Ausgestaltung dieser Technologie in vielerlei Hinsicht Anlass gibt, die korrespondierenden haftungsrechtlichen Fragestellungen zu ergründen.[18] 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.[19]

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; *Rammos/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 *Bisges,* 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.[20] 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.[21] 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 Beispielsfall 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.[22]

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.

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

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.[25]

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.[26] 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.[27]

---

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 berechtigte Cloud-Nutzer

1. Haftungsszenario

Weiterhin ist als potentielles Haftungsszenario denkbar, dass im Rahmen einer Cloud-Lösung mit mehreren nutzungsberechtigten Anwendern Datensätze beeinträchtigt oder entfernt werden, die einem anderen Cloud-Nutzer zugeordnet waren. Zu denken wäre etwa an eine Private Cloud[28]-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:[29] 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.[30] 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 berechtigten 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:[31] 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.

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:[32] 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.[33]

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[34] zum Datenverlust. So war etwa im oben dargestellten Beispiel Amazon EC2 der Datenverlust durch einen Routingfehler im Rahmen eines Netzwerkupgrades ausgelöst worden.[35] Es stellt sich dann die Frage, ob bzw. unter welchen Voraussetzungen der Cloud-Anbieter für die entstandenen Schäden haftet.[36]

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.[37]

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.[38]

§ 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.[39]

Sodann ist auf die Frage einzugehen, welches nationale Recht auf Haftungsfälle im Cloud Computing Anwendung findet.[40] 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.[41] Zunächst wird die vertragstypologische Einordnung der Cloud Computing-Vereinbarung erörtert,[42] 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[43] und in demjenigen eines externen Hackerangriffs[44] vertragliche Schadensersatzansprüche gegen den Cloud-Anbieter zustehen.[45] Schließlich wird in diesem Abschnitt die gängige Regelungspraxis der großen Cloud-Anbieter hinsichtlich ihrer Konformität mit den zuvor erarbeiteten Grundsätzen überprüft.[46]

Der zweite Schwerpunkt der Untersuchung befasst sich hiernach mit den Rechtsgrundlagen der deliktischen Haftung.[47] 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[48] oder bei Datenlöschung durch grundsätzlich mitberechtigte Cloud-Nutzer[49]. Es kann jedoch auch das Bestehen von Verkehrspflichten des Cloud-Anbieters relevant werden, sofern nicht zu jedem Cloud-Nutzer ein Vertragsverhältnis besteht.[50]

Im Hinblick auf die deliktische Haftung gestaltet sich bereits die Suche nach einer geeigneten Anspruchsgrundlage diffizil. § 823 Abs. 1 BGB[51] 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.[52] Auch eigenständige Anspruchsgrundlagen wie § 826 BGB oder § 1 ProdHaftG werden in diesem Rahmen erörtert.[53] 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.[54]

---

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.[55]

Abschließend wird die in der Praxis bedeutsame prozessuale Nachweissituation untersucht.[56] 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.[57] 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.[58]

Die Arbeit schließt mit einer Zusammenfassung der Ergebnisse.[59]

---

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.[60]

Besondere Bekanntheit hat die technische Definiton des NIST erlangt:[61]

"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/Döpkens,* 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,[62] deren Differenzierungen im Detail für die rechtliche Beurteilung nicht entscheidend sind.[63] 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.[64]

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.[65] Im Rahmen der weiteren technologischen Entwicklung konnte in der Folge eine Umstellung auf netzwerkbasierte Ressourcenteilung erreicht werden.[66] Auch dieser Trend wurde früh erkannt: Bereits etwa[67] 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.[68] 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/Döpkens,* 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-Zrakic/Milutinovic/Belic,* Handbook of Research, S. 2.

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

3. Abgrenzung von vergleichbaren Technologien

a) IT-Outsourcing

Abzugrenzen ist das Cloud Computing insbesondere vom konventionellen IT-Outsourcing,[72] 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[73] durch den Cloud-Nutzer steht hier nicht im Fokus.[74] 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[75] weist hingegen das sog. Application Service Providing (ASP) auf, das insbesondere aufgrund der einschlägigen Rechtsprechung des BGH[76] 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-Zrakic/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.[77] 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[78] handelt es sich mithin im Ergebnis nicht.

c) Grid Computing

Schließlich ist begrifflich zu einem weiteren Vorläufer[79] moderner Cloud-Strukturen abzugrenzen; dem sog. Grid Computing. Dieses bezeichnet den netzwerkseitigen Zusammenschluss mehrerer Rechner, um mit erhöhter Leistungsfähigkeit bestimmte Aufgaben erledigen zu können.[80] 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.[81]

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.[82] 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.