Deutsches und Europäisches Strafprozessrecht und Polizeirecht 9

Andreas Grözinger

Die Überwachung von Cloud-Storage

Eine Untersuchung der strafprozessualen Möglichkeiten zur heimlichen Überwachung von Cloud-Storage vor und nach dem Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

Nomos

Deutsches und Europäisches Strafprozessrecht
und Polizeirecht

herausgegeben von

Prof. Dr. Mark A. Zöller, Universität Trier

Band 9

Andreas Grözinger

Die Überwachung von Cloud-Storage

Eine Untersuchung der strafprozessualen Möglichkeiten zur heimlichen Überwachung von Cloud-Storage vor und nach dem Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

Nomos

Die Hohe Rechtswissenschaftliche Fakultät der Universität zu Köln hat diese Arbeit im Wintersemester 2017/2018 als Dissertation angenommen.

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

Zugl.: Köln, Univ., Diss., 2018

ISBN 978-3-8487-5448-9 (Print)

ISBN 978-3-8452-9604-3 (ePDF)

1. Auflage 2018

Meinen Eltern

Die vorliegende Arbeit wurde durch die Rechtswissenschaftliche Fakultät der Universität zu Köln im Wintersemester 2017/2018 als Dissertation angenommen. Inhaltlich befindet sich die Arbeit auf dem Stand von August 2018.

Herzlich bedanken möchte ich mich bei meinem Doktorvater Prof. Dr. Martin Waßmer, der mich bei der Wahl des Themas unterstützte und mir bei der Bearbeitung stets mit zahlreichen wertvollen Anregungen beiseite stand. Dank gebührt auch Herrn Prof. Dr. Dr. h.c. Michael Kubiciel für die zügige Erstellung des Zweitgutachtens und seine hilfreichen Anmerkungen.

Weiterer Dank gilt meinen Kollegen und Kolleginnen der Kanzlei Gercke|Wollschläger, hier insbesondere Prof. Dr. Björn Gercke und Dr. Sebastian Wollschläger, die stets ein offenes Ohr für meine Anliegen hatten.

Ich danke Mani Jaleesi, Dr. Jonas Dereje und Niklas Gräbener für ihre Kritik und ihre Impulse.

Mein besonderer Dank gilt Dr. Anna Eschbach, die mich während der gesamten Zeit der Entstehung vorbehaltlos unterstützte.

Schließlich danke ich meiner Familie. Ohne sie hätte diese Arbeit nicht entstehen können. Besonders danken möchte ich meinen Eltern Beate und Michael Grözinger, die mir zu jedem Zeitpunkt eine Stütze waren. Ihnen ist diese Arbeit gewidmet.

Köln, Herbst 2018 *Andreas Grözinger*

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.A./a.A.	anderer Ansicht/andere Auffassung
a.F.	alte Fassung
Abs.	Absatz
AG	Amtsgericht
Anm.	Anmerkung
AöR	Archiv des öffentlichen Rechts
Art.	Artikel
Az.	Aktenzeichen
Beschl.	Beschluss
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidung in Strafsachen des Bundesgerichtshofes
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidung des Bundesverfassungsgerichts
BVerfGK	Kammerentscheidung des Bundesverfassungsgerichts
CR	Computer und Recht
d.h.	das heißt
ders.	derselbe
dies.	dieselbe
DÖV	Die öffentliche Verwaltung
DRiZ	Deutsche Richter-Zeitung
DuD	Datenschutz und Datensicherheit
DVBl	Deutsches Verwaltungsblatt
f.	folgende
ff.	fortfolgende
Fn.	Fußnote
FS	Festschrift
GA	Goltdammer‘s Archiv für Strafrecht
GG	Grundgesetz
ggf.	gegebenenfalls

h.M.	herrschende Meinung
HRRS	Höchstrichterliche Rechtsprechung im Strafrecht
Hrsg.	Herausgeber
Hs.	Halbsatz
i.d.F.	in der Fassung
i.d.R.	in der Regel
i.E.	im Ergebnis
i.S.d.	im Sinne des
i.V.m.	in Verbindung mit
JA	Juristische Arbeitsblätter
JR	Juristische Rundschau
JURA	Juristische Ausbildung
jurisPR-ITR	juris Praxisreport IT-Recht
JurPC	JurPC
JuS	Juristische Schulung
JZ	JuristenZeitung
K&R	Kommunikations & Recht
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
LG	Landgericht
Lit.	Literatur
m.w.N.	mit weiteren Nachweisen
MMR	MultiMedia und Recht
n.F.	neue Fassung
NJW	Neue Juristische Wochenzeitschrift
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
NStZ-RR	NStZ-Rechtsprechungs-Report Strafrecht
OLG	Oberlandesgericht
Rn.	Randnummer
Rspr.	Rechtsprechung
s.	siehe
sog.	sogenannte/r
st. Rspr.	ständige Rechtssprechung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung

str.	streitig
StraFo	Strafverteidiger Forum
StV	Strafverteidiger
u.	und
u.a.	unter anderem
u.U.	unter Umständen
Urt.	Urteil
v.	von/vom
Var.	Variante
vgl.	vergleiche
WM	Zeitschrift für Wirtschafts- und Bankrecht
z.B.	zum Beispiel
z.T.	zum Teil
ZD	Zeitschrift für Datenschutz
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZUM	Zeitschrift für Urheber- und Medienrecht

§ 1 Einleitung

A. Die Cloud – ein junges Phänomen

Immer neue Phänomene der Informationstechnik schaffen Herausforderungen für das Recht und den Gesetzgeber.

Eines dieser Phänomene ist „die Cloud" (zu deutsch: die Wolke). Zunächst noch als „Hypethema"[1] bezeichnet, kann die wachsende Bedeutung von Cloud-Computing und den damit einhergehenden rechtlichen Fragestellungen heute kaum noch geleugnet werden. So ist sie der Grund dafür, dass der herkömmliche Computer bereits als „Auslaufmodell"[2] bezeichnet und mit Cloud-Computing „die Zukunft"[3] ausgerufen wird. Auch der prophezeite Siegeszug des Cloud-Computing zeichnet sich schon jetzt ab. Immer mehr Bürger*innen[4] und Unternehmen nutzen die Cloud und haben diese in ihren Alltag integriert.[5] Die Vorteile für den Nutzer sind enorm. So bietet der Cloud-Anbieter seinen Nutzern nicht nur die Möglichkeit zur flexiblen Nutzung seiner Speicherkapazitäten und sonstigen Ressourcen wie z.B. Rechenleistung. Darüber hinaus können die Nutzer von nahezu jedem internetfähigen Endgerät auf ihre Cloud zugreifen. Für Unternehmen ergeben sich schließlich erhebliche Kostenersparnisse, weil sie nicht selbst die erforderlichen Infrastrukturen betreiben müssen und beim Cloud-Anbieter entsprechend ihren gegenwärtigen Bedürfnissen Kapazitäten flexibel hinzu- oder abbuchen können.[6]

---

1 *Birk/Wegener*, DuD 2010, 641.

2 *Obenhaus*, NJW 2010, 651.

3 *Obenhaus*, NJW 2010, 651; *Söbbing*, MMR 2008, XII.

4 Soweit im Folgenden Berufs- Gruppen- und/oder Personenbezeichnungen Verwendung finden, beziehen sich diese auch stets auf die jeweils weibliche Form.

5 Allein im Jahr 2015 machten Cloud-Anbieter mit Soft- und Hardware sowie Dienstleistungen einen Umsatz von 183 Milliarden Dollar. Im selben Jahr wuchs der Markt im Vergleich zum Vorjahr damit um 17 Prozent, vgl. http://blog.wiwo.de/look-at-it/2015/03/19/cloud-computing-2015-183-milliarden-dollar-umsatz-agilitat-und-kosten-als-hauptmotive/ (Stand: September 2018). Zu den Vorteilen der Cloud insbesondere für Unternehmen und Behörden *Wicker*, Cloud Computing und staatlicher Strafanspruch, S. 49 ff.

6 Vgl. https://www.heise.de/download/blog/Die-Vorteile-und-Nachteile-des-Cloud-Computing-3713041 (Stand: September 2018).

Doch Wolken werfen bekanntlich auch Schatten.[7] Längst haben Kriminelle die Vorteile der Cloud für sich entdeckt und sich in einen Wettlauf[8] mit den Strafverfolgungsbehörden begeben. Um in diesem Wettlauf mithalten zu können, sind die Strafverfolgungsbehörden ihrerseits nicht nur auf die notwendigen informationstechnischen Werkzeuge zur Aufklärung des Sachverhalts angewiesen. Sie müssen sich zudem auf einem sicheren rechtlichen Fundament bewegen können. Schließlich ist zu berücksichtigen, dass es „kein Grundsatz der StPO [ist], daß [sic] die Wahrheit um jeden Preis erforscht werden müßte [sic]"[9].

B. Untersuchungsgegenstand

Dieser Befund führt unweigerlich zu der Frage, ob die Strafverfolgungsbehörden Kriminellen im Wettlauf der Informationstechnik auf Augenhöhe begegnen können oder ob der Rechtsstaat mangels hinreichender rechtlicher „Ausstattung" nicht bereits „hinterherhinkt"[10].

Die jährlich steigende Zahl von Anordnungen der Telekommunikationsüberwachungen[11] und der vermehrte Einsatz des Internets als Fahndungsmittel[12] zeigen jedenfalls den Willen der Strafverfolgungsbehörden, den Blickkontakt zu Kriminellen im Internet nicht zu verlieren.

Dieser Ehrgeiz bringt aus der Perspektive der Bürger aber auch Gefahren mit sich.[13] Die Anordnung von Telekommunikationsüberwachungen

---

7 *Jotzo*, Der Schutz personenbezogener Daten in der Cloud, S. 17; *Valerius*, in: Cybercrime und Cyberinvestigations, S. 67.

8 Vgl. *Bäcker*, Kriminalpräventionsrecht, S. 68.

9 BGH, NJW 1960, 1580, 1582.

10 *Paeffgen*, in: FS-Roxin, 1299, 1318; vgl. zur verstärkten Einbindung Privater bei der Rechtsdurchsetzung im Internet und zur Frage der Verwertbarkeit der so gewonnenen Informationen *Kubiciel*, GA 2013, 226.

11 Allein im Jahr 2013 betrug die Anzahl der Anordnungsbeschlüsse 19.398 und die der Verlängerungsbeschlüsse 3.519. Hält man sich nunmehr vor Augen, dass sich die Anzahl an Anordnungsbeschlüssen im Jahr 2010 noch auf 12.239 und an Verlängerungsanordnungen auf 337 belief, wird das inflationäre Ausmaß der Anordnung von Telekommunikationsüberwachung nach § 100a der StPO deutlich, vgl. https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2013.pdf?__blob=publicationFile (Stand: September 2018).

12 Vgl. hierzu *Pätzel*, NJW 1997, 3131; *Soiné*, NStZ 1997, 166 ff. und 321 ff.

13 Vgl. auch *Zöller*, ZStW 124 (2012), 411, 416.

ist heute bereits zum Massenphänomen geworden.[14] Der Umstand, dass weite Teile der Bevölkerung das Internet und die Cloud mit der Attitüde benutzen, man habe nichts zu verbergen, kann vor dem Hintergrund umfassender Möglichkeiten zur Datenauswertung und -verarbeitung bis hin zur Erstellung von Persönlichkeitsprofilen nur als leichtfertig bezeichnet werden.[15]

Fehlen gegenwärtig erforderliche Rechtsgrundlagen zur heimlichen Überwachung der Cloud und versäumt der Staat durch die Schaffung notwendiger Rechtsgrundlagen „nachzurüsten", ist zu befürchten, dass das rechtsstaatliche Fundament staatlichen Handelns Risse bekommt. Umso wichtiger ist es, dass staatlichem Handeln klare rechtliche Grenzen gesetzt und dadurch die verfassungsmäßigen Rechte der Bürger geschützt werden.

Originäres Ziel dieser Untersuchung ist es, das Speichern von Daten in der Cloud einem grundrechtlichen Schutzbereich zuzuordnen und – daran anknüpfend – die Frage zu beantworten, ob in der StPO eine Rechtsgrundlage für die heimliche Überwachung der Cloud existiert. Insoweit wird zunächst der Fokus auf die Rechtslage *vor* Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.08.2017 (BGBl. I S. 3202) am 24.08.2017[16] (im Folgenden: StPO-Reform) gelegt, bevor insbesondere die Verfassungsmäßigkeit der im Zuge dieser Reform neu eingeführten §§ 100a Abs. 1 S. 2 und 3, 100b StPO n.F.[17] untersucht und deren Auswirkungen auf die Möglichkeiten zur heimlichen Überwachung der Cloud beleuchtet werden.

---

14 *Wolter*, in: SK-StPO, § 100a, Rn. 6.

15 *Sandfuchs*, Privatheit wider Willen?, S. 21.

16 BT-Drs. 18/12785.

17 Als „§ 100a StPO" bzw. „100b StPO" werden zur besseren Gewährleistung der Übersichtlichkeit die Vorschriften der §§ 100a, 100b StPO a.F., namentlich in ihrer Fassung bis zum Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.08.2017 (BGBl. I S. 3202) (StPO-Reform), am 24.08.2017, bezeichnet. Die im Zuge der StPO-Reform geänderten bzw. eingeführten §§ 100a, 100b StPO werden trotz ihres zwischenzeitlichen Inkrafttretens als „§ 100a StPO n.F." bzw. „§ 100b StPO n.F." bezeichnet. § 100a Abs. 1 S. 1 StPO n.F. entspricht dem bisherigen § 100a Abs. 1 StPO.

C. Gang der Untersuchung

Die Analyse gliedert sich insgesamt in sieben Kapitel (§§ 1 – 7). Nachdem zunächst der Realbereich dargestellt und insbesondere die Begriffe Cloud, Cloud-Computing und Cloud-Storage erläutert werden (§ 2), widmet sich die Arbeit dem verfassungsrechtlichen (§ 3) Normbereich. Anschließend werden der einfach-gesetzlichen Normbereich *vor* Inkrafttrefen der StPO-Reform (§ 4) untersucht und die prozessualen Rechtsfolgen im Falle der unzulässigen Überwachung von Cloud-Storage erläutert (§ 5). Schließlich befasst sich das sechste Kapitel mit den im Zuge der StPO-Reform eingeführten Eingriffsbefugnissen, die als denkbare Rechtsgrundlagen für die Überwachung von Cloud-Storage in Betracht kommen (§ 6).

Das zweite Kapitel legt zunächst die wesentlichen tatsächlichen und begrifflichen Grundlagen für die weitere Untersuchung. So erläutert es den Begriff der Cloud, ihre Ausprägungen und Erscheinungsformen und beleuchtet die technischen Grundlagen der Cloud und der Datenübertragung im Internet. Anschließend beschreibt es die unterschiedlichen Arten von Daten, die aus einer Überwachung gewonnen werden können und skizziert die technischen Möglichkeiten der Durchführung einer solchen. Sodann stellt es den eigentlichen Untersuchungsgegenstand dar. Schließlich zeigt es die Bedeutung auf, die die Möglichkeit zur heimlichen Überwachung der Cloud für die Strafverfolgungsbehörden vor dem Hintergrund der weltweiten Vernetzung des Internets hat und nimmt die Vorteile der heimlichen Überwachung gegenüber anderen Ermittlungsmaßnahmen in den Blick.

Das dritte Kapitel stellt die Frage nach der Regelungsbedürftigkeit einer entsprechenden Maßnahme in der StPO und bespricht den verfassungsrechtlichen Schutz des Cloud-Nutzers. Als betroffene Grundrechte behandelt dieses Kapitel insbesondere das Telekommunikationsgeheimnis sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Am Ende beantwortet § 3 die Frage, wann und unter welchen Voraussetzungen der Nutzer sich auf den Schutz welchen Grundrechts berufen kann.

Das vierte Kapitel konzentriert sich auf die Frage, welche einfach-gesetzlichen Eingriffsermächtigungen innerhalb der StPO vor Inkrafttreten der StPO-Reform für die heimliche Überwachung von Cloud-Storage herangezogen werden konnten. Den Fokus legt § 4 auf die Telekommunikationsüberwachung gemäß § 100a StPO und fragt zunächst danach, was unter dem Begriff der Telekommunikation in diesem Sinne zu verstehen ist.

Nachdem insoweit ein Ergebnis gefunden worden ist, widmet sich § 4 dem Überwachungsbegriff und untersucht die Frage, welche (Begleit-) Maßnahmen vor der StPO-Reform konkret auf Grundlage von § 100a StPO durchgeführt werden durften. Schließlich wird die Anwendbarkeit weiterer strafprozessualer Eingriffermächtigungen in Bezug auf die heimliche Überwachung von Cloud-Storage geprüft sowie die Frage beantwortet, ob entsprechende Vorschriften aus der StPO analog als Rechtsgrundlage für entsprechende Überwachungsmaßnahmen herangezogen werden dürfen. Am Ende des Kapitels wird der gesetzgeberische Handlungsbedarf aufgezeigt, der vor Inkrafttreten der StPO-Reform bestand.

Das fünfte Kapitel widmet sich den prozessualen Rechtsfolgen einer unzulässigen Überwachung der Cloud und beantwortet die Fragen nach dem Vorliegen eines Beweisverwertungsverbotes sowie der Möglichkeit der Heilung etwaiger Beweisverwertungsverbote durch die nachträgliche Schaffung einer bis dahin nicht vorhandenen aber erforderlichen gesetzlichen Regelung.

§ 6 untersucht schließlich die Rechtslage nach der StPO-Reform. Das Augenmerkt der Untersuchung legt § 6 auf die neu eingeführten §§ 100a, 100b StPO n.F., die die sog. Quellen-Telekommunikationsüberwachung und die sog. Online-Durchsuchung regeln. Neben der Darstellung der Auswirkungen der §§ 100a, 100b StPO n.F. im Hinblick auf die Möglichkeiten zur heimlichen Überwachung von Cloud-Storage beantwortet § 6 die Fragen nach der Verfassungsmäßigkeit dieser Vorschriften und etwaig verbleibendem gesetzgeberischen Handlungsbedarf.

Das siebte und letzte Kapitel enthält eine Zusammenfassung der wesentlichen Ergebnisse der Untersuchung.

§ 2 Grundlagen

Der Markt von Cloud-Angeboten wächst rasant.[18] Neben Unternehmen haben längst immer mehr Privatpersonen den Nutzen der Cloud erkannt. Das Speichern in der Cloud ist im Alltag angekommen. Der Begriff der Cloud ist inzwischen im allgemeinen Sprachgebrauch angelangt. Doch was bedeutet eigentlich Cloud? Wodurch charakterisiert sich die Cloud und wie funktioniert sie? Diese Fragen werden in der Folge näher beleuchtet. Nach Herausarbeitung des dieser Arbeit zugrundeliegenden Untersuchungsgegenstands werden sodann die verfassungsrechtlichen Grundlagen für die Überwachung der Cloud sowie die Vorteile der heimlichen Überwachung gegenüber anderen – insbesondere offenen – Ermittlungsmaßnahmen aufgezeigt.

A. Begriffliche Grundlagen

Da es eine Vielzahl von Definitionen und Verwendungen der Begriffe Cloud-Computing und Cloud-Storage gibt, sollen im Folgenden die dieser Arbeit zugrunde gelegten Begrifflichkeiten erläutert werden.

I. Cloud, Cloud-Computing und Cloud-Storage

Um Cloud-Storage zu verstehen ist es wichtig, zunächst eine Definition des Cloud-Computing herauszuarbeiten, das als Oberbegriff Cloud-Storage umfasst. Ferner werden die verschiedenen Bereitstellungs- und Service-Modelle des Cloud-Computing in der gebotenen Kürze erläutert.

---

18 Vgl. http://blog.wiwo.de/look-at-it/2015/03/19/cloud-computing-2015-183-milliarden-dollar-umsatz-agilitat-und-kosten-als-hauptmotive/ (Stand: September 2018).

1. Begriff und Definition

Der Begriff „Cloud" bedeutet ins Deutsche übersetzt „Wolke" und beschreibt metaphorisch die undurchsichtige, in ständiger Bewegung befindliche und komplexe Infrastruktur, auf die netzbasierte Anwendungen zugreifen, ohne dass die Nutzer sie näher kennen oder gar kontrollieren können.[19]

Eine einheitliche Definition von Cloud-Computing und Cloud-Storage existiert nicht. Dennoch nähern sich die unterschiedlichen Definitionsversuche einander immer mehr an, sodass der Begriff der Cloud nicht mehr nur eine „diffuse Marketingworthülse"[20] ist.

Zum Teil wird Cloud-Computing als eine große Ansammlung von Ressourcen (z.B. Hardware, Dienste oder Entwicklungsplattformen) verstanden, die leicht nutzbar sind und auf die einfach zugegriffen werden kann.[21] Kennzeichnend ist demnach, dass diese Ressourcen flexibel an die jeweiligen Bedürfnisse angepasst werden können, sodass eine optimale Auslastung der Ressourcen möglich ist.[22]

Andere definieren Cloud-Computing als einen IT-Betrieb, bei dem erheblich skalierbare Ressourcen für externe Kunden über das Internet als Dienst zur Verfügung gestellt werden.[23]

Das Bundesamt für Sicherheit in der Informationstechnik definiert Cloud-Computing wie folgt:

> „Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem

19 Vgl. *Federrath*, ZUM 2014, 1; *Hoffmann-Riem*, JZ 2008, 1009, 1011.
20 *Krcmar*, in: Borges/Meents (Hrsg.), Cloud Computing, § 1, Rn. 27.
21 *Vaquero et al.*, A Break in the Clouds, S. 51.
22 Vaquero/Rodero-Merino/Caceres/Lindner, a.a.O.
23 *Cearley*, Gartner, Cloud computing: Key Initiative Overview, S. 2.

> Infrastruktur (z.B. Rechenleistung, Speicherplatz),[24] Plattformen und Software.“[25]

Die Definition mit der wohl größten Akzeptanz in Fachkreisen[26] ist die Definition der US-amerikanischen Standardisierungsstelle National Institute of Standards and Technology (NIST). Cloud-Computing ist danach ein Modell, das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Server-Provider-Interaktion zur Verfügung gestellt werden können.[27]

Darüber hinaus legt die NIST fünf Charakteristika fest, die einen Cloud-Service beschreiben, nämlich On-Demand-Self-Service, Broad Network Access, Resource Pooling, Rapid Elasticity und Measured Services.[28]

Unter On-Demand-Self-Service versteht man die automatische Bereitstellung der Ressourcen. Eine Interaktion mit dem Service Provider findet nicht statt.[29]

Broad Network Access bedeutet, dass die Dienste nicht an einen bestimmten Client[30] gebunden, sondern mit Standard-Mechanismen über das Netz verfügbar sind.[31]

Resource Pooling beschreibt die Bündelung von Ressourcen, die in einem Pool zusammengetragen werden, aus dem sich viele Nutzer gleichzeitig bedienen können. Wo sich die Ressourcen befinden, ist den Nutzern grundsätzlich nicht bekannt. Etwas anderes gilt allenfalls dann, wenn vertraglich ein bestimmter Speicherort festgelegt worden ist.[32]

---

24 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html;jsessionid=BD3E-FE636495D9C054CBC43ACF75D3C2.2_cid368 (Stand: September 2018).

25 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html;jsessionid=BD3E-FE636495D9C054CBC43ACF75D3C2.2_cid368 (Stand: September 2018).

26 *Süptitz/Utz/Eymann*, DuD 2013, 307.

27 NIST, Special Publication 800-145, S. 2.

28 Vgl. auch Darstellung in *Niemann/Paul*, Cloud Computing, S. 18.

29 NIST, Special Publication 800-145, S. 2.

30 Als Client wird ein Rechner innerhalb eines Netzwerks bezeichnet, der vom Server Dienste abruft, vgl. Duden, Deutsches Universalwörterbuch.

31 NIST, Special Publication 800-145, S. 2.

32 NIST, Special Publication 800-145, S. 2.

Rapid Elasticity bedeutet, dass die unterschiedlichen Dienste schnell, elastisch und in manchen Fällen auch automatisch bereitgestellt werden. Aus der Sicht des Nutzers scheinen die Ressourcen unendlich zu sein.[33]

Schließlich versteht man unter Measured Services, dass die Ressourcennutzung gemessen, überwacht und entsprechend bemessen den Nutzern zur Verfügung gestellt werden kann.[34]

Aufgrund der hohen Akzeptanz der NIST-Definition und weil weitere hier besprochene Differenzierungen (Public Cloud und Private Cloud, Servicemodelle) von der NIST entwickelt worden sind, wird dieser Arbeit die NIST-Definition zugrunde gelegt.

2. Von der Public Cloud über die Private Cloud zur Internal Cloud

Das NIST teilt Cloud-Computing in vier Bereitstellungsmodelle ein, nämlich Public Cloud, Private Cloud, Community Cloud und Hybrid Cloud.

Für eine Private Cloud ist kennzeichnend, dass die Cloud-Infrastruktur exklusiv für eine Institution, also einen festgelegten Nutzerkreis, betrieben wird. Die Cloud kann von einem Dritten oder der Institution selbst organisiert und betrieben werden. Entsprechend kann die Cloud-Infrastruktur bei einem Dritten oder innerhalb der eigenen Institution stehen.[35] Steht die gesamte Cloud-Infrastruktur im Eigentum z.B. eines Unternehmens, spricht man von einer Internal Cloud, die einen Unterfall der Private Cloud darstellt. Die Internal Cloud kann als Unternehmensintranet in Cloud-Form bezeichnet werden.[36]

In einer Public Cloud können die von einem Anbieter zur Verfügung gestellten Dienste von der Allgemeinheit oder einer großen Gruppe (z.B. einer ganzen Industriebranche) genutzt werden.

Von einer Community Cloud spricht man, wenn die Infrastruktur von mehreren Institutionen geteilt wird, die typischerweise ähnliche Interessen haben. Der Betreiber der Cloud kann ein Dritter oder die Institution selbst sein.[37] Treffend vergleicht *Krcmar* die Community Cloud mit einer Einkaufsgemeinschaft, die sich von einer Private Cloud insbesondere dadurch

---

33 NIST, Special Publication 800-145, S. 2.
34 NIST, Special Publication 800-145, S. 2.
35 NIST, Special Publication 800-145, S. 3.
36 *Bedner*, Cloud Computing, S. 33.
37 NIST, Special Publication 800-145, S. 3.

unterscheidet, dass sich der Benutzerkreis aus unterschiedlichen, rechtlich sowie wirtschaftlich unabhängigen Unternehmen zusammensetzt.[38]

Eine Hybrid Cloud kennzeichnet sich schließlich dadurch aus, dass mehrere für sich eigenständige Cloud Infrastrukturen über standardisierte Schnittstellen gemeinsam genutzt werden können.[39] Insoweit kombiniert eine Hybrid Cloud die Modelle der Private Cloud und der Public Cloud. Eine Hybrid Cloud hat damit den Vorteil, dass ein Unternehmen es in der Hand hat, ob es sensible Daten und Anwendungen im eigenen Kontrollbereich belässt (Private Cloud) oder in die Public Cloud verschiebt, wenn mit einem erhöhten Ressourcenbedarf zu rechnen ist.[40]

Auch wenn die vorgenannten Definitionen einen Großteil der Cloudmodelle erfassen, sind sie nicht abschließend.[41]

3. Servicemodelle – IaaS, PaaS, SaaS

Cloud-Computing lässt sich in drei wesentliche Servicemodelle unterteilen, nämlich Infrastructure-as-a-Service, Platform-as-a-Service und Software-as-a-Service.[42]

Zu Recht wird jedoch eingewandt, dass die Grenzen zwischen den einzelnen Servicemodellen teilweise fließend sind, sodass sich nicht jeder angebotene Dienst ausschließlich einem Servicemodell zuordnen lässt.[43]

Unter Infrastructure-as-a-Service (IaaS) versteht man ein Angebot zur Bereitstellung von physischen IT-Basisressourcen wie z.B. Datenspeicher, Rechenleistung oder Netze. Durch die Inanspruchnahme von IaaS erhält ein Nutzer die Möglichkeit, fremde Hardware-Kapazitäten für die eigenen Bedürfnisse zu nutzen. So kann er beispielsweise Rechenleistung, Arbeitsspeicher und Festplattenspeicher anmieten und über diese Cloud-Ressourcen ein Betriebssystem mit Anwendungen seiner Wahl ablaufen lassen.

Bei dem Servicemodell Platform-as-a-Service (PaaS) wird dem Kunden eine komplette Anwendungs-Infrastruktur bereitgestellt. Über standardi-

---

38 *Krcmar*, in: Borges/Meents (Hrsg.), Cloud Computing, § 1, Rn. 49.
39 NIST, Special Publication 800-145, S. 3.
40 *Krcmar*, in: Borges/Meents (Hrsg.), Cloud Computing, § 1, Rn. 50.
41 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html;jsessionid=BD3E-FE636495D9C054CBC43ACF75D3C2.2_cid368 (Stand: September 2018).
42 NIST, Special Publication 800-145, S. 2 f.
43 *Armbrust et al.*, Communications of the ACM, S. 50.

sierte Schnittstellen, die dem Nutzer zur Verfügung gestellt werden, kann dieser nunmehr auf der Plattform eigene Anwendungen laufen lassen. Allerdings hat er keinen Zugriff auf die darunterliegenden Schichten (Hardware, Betriebssystem).

Software-as-a-Service (SaaS) stellt dem Nutzer die Funktionalität einer vollwertigen Anwendung zur Verfügung.[44] Wartung und Betrieb der Software erfolgen bei diesem Servicemodell allein durch den jeweiligen Dienstleister und liegen außerhalb des Verantwortungsbereichs des Nutzers.[45]

II. Akteure

Beim Cloud-Computing spielen verschiedene Akteure eine Rolle. Im Wesentlichen kann zwischen Cloud-Nutzern (Kunden), Cloud-Anbietern (alt.: Cloud-Providern), und Ressourcenanbietern unterschieden werden.[46] Daneben spielen die Telekommunikationsdiensteanbieter eine Rolle.

Cloud-Anbieter vermarkten ihre Ressourcen. Namhafte Cloud-Anbieter sind Amazon, Google, Microsoft oder Salesforce. Im Fall von Cloud-Storage wird insbesondere Speicherkapazität zur Verfügung gestellt. Cloud-Nutzer, die diesen Service in Anspruch nehmen, können Speicherkapazitäten beim Cloud-Anbieter nach Bedarf mieten.[47]

Nicht immer verfügt ein Cloud-Anbieter über genug Kapazitäten, um die Nachfrage der Kunden zu befriedigen. Übersteigt die Kundennachfrage die vorhandenen Kapazitäten, kann ein Cloud-Provider seinerseits Speicher bei unabhängigen Ressourcenanbietern anmieten, um die Kundennachfrage befriedigen zu können. Der Kunde bekommt von diesem Vorgang grundsätzlich nichts mit. Ressourcenanbieter sind damit Subunternehmer der Cloud-Provider.[48]

---

44 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html;jsessionid=BD3E-FE636495D9C054CBC43ACF75D3C2.2_cid368 (Stand: September 2018).

45 *Krcmar*, in: Borges/Meents (Hrsg.), Cloud Computing, § 1, Rn. 32.

46 *Weichert*, DuD 2010, 679, 680.

47 Vgl. zur zivilrechtlichen Einordnung des Cloud Computing ausführlich *Wicker*, Cloud Computing und staatlicher Strafanspruch, S. 65 ff.

48 *Eckhardt*, DuD 2015, 176, 179.