

Internetrecht und Digitale Gesellschaft

Band 22

Cloud Computing

**Strafrechtlicher Schutz privater und
geschäftlicher Nutzerdaten vor Innetäter-Angriffen
de lege lata und de lege ferenda**

Von

Daniel Müller



Duncker & Humblot · Berlin

DANIEL MÜLLER

Cloud Computing

Internetrecht und Digitale Gesellschaft

Herausgegeben von
Dirk Heckmann

Band 22

Cloud Computing

Strafrechtlicher Schutz privater und
geschäftlicher Nutzerdaten vor Innentäter-Angriffen
de lege lata und de lege ferenda

Von

Daniel Müller



Duncker & Humblot · Berlin

Die Juristische Fakultät
der Julius-Maximilians-Universität Würzburg
hat diese Arbeit im Sommersemester 2018
als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

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

Alle Rechte vorbehalten
© 2020 Duncker & Humblot GmbH, Berlin
Satz: 3w+p GmbH, Ochsenfurt-Hohestadt
Druck: CPI buchbücher.de GmbH, Birkach
Printed in Germany

ISSN 2363-5479
ISBN 978-3-428-15747-1 (Print)
ISBN 978-3-428-55747-9 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2018 von der Juristischen Fakultät der Julius-Maximilians-Universität Würzburg als Dissertation angenommen. Gesetzgebung, Literatur und Rechtsprechung konnten bis Oktober 2018 berücksichtigt werden.

Die Ergebnisse dieser Arbeit resultieren aus den Erkenntnissen, die ich im Rahmen der Mitarbeit an dem juristischen Begleitforschungsprojekt „Sicheres Cloud Computing“ (SCC-Jur), das im Rahmen des Forschungsprogramms „IKT 2020 – Forschung für Innovation“ des Bundesministeriums für Wirtschaft und Technologie (BMWi) in dem Zeitraum von April 2015 bis April 2018 gefördert wurde, gewinnen konnte.

Den zahlreichen Personen, die mich während meines Promotionsvorhabens in vielfältiger Art und Weise unterstützt und Rückhalt gegeben haben, möchte ich an dieser Stelle ganz herzlich danken.

Ganz besonderer Dank gebührt zunächst meinem Doktorvater, Herrn Professor Dr. Frank Peter Schuster, Mag. iur., der mir ermöglicht hat, an dem Forschungsprojekt mitzuarbeiten und mir die Anregung zu diesem aktuellen und höchst spannenden Thema gab. Er stand mir jederzeit mit Rat und Tat zur Seite. Die mir von ihm gewährten wissenschaftlichen Freiräume sowie seine wertvollen Ideen und Hinweise haben wesentlich zu dem Gelingen meiner Arbeit beigetragen. Danken möchte ich auch Herrn Professor Dr. Dr. Eric Hilgendorf für die zügige Erstellung des Zweitgutachtens.

Herzlichst bedanken möchte ich mich ferner bei dem gesamten Lehrstuhl-Team für die zahlreiche, konstruktive Unterstützung und die sehr schöne und heitere Zusammenarbeit. Besonders bedanken möchte ich mich bei Tanja Houle für ihren motivierenden Zuspruch und ihre stete Hilfsbereitschaft. Gleiches gilt auch meiner Kollegin, Barbara Krüll, die mich vor allem durch fachliche Diskussionen und Anregungen sowie durch ihr sorgfältiges Korrekturlesen bei der Fertigstellung der Arbeit unterstützte. Für Letzteres gilt ein großer Dank auch an Theresa Barufke und Patrick Staudt.

Für ihre vielfältige Hilfe und ihren Glauben an meinem Erfolg möchte ich mich außerdem bei Johanna Elmrich bedanken.

Mein größter Dank gilt an dieser Stelle meinen Eltern, Petra und Hans-Dieter Müller. Sie haben mir nicht nur meine juristische Ausbildung ermöglicht, sondern mich darüber hinaus auf meinem bisherigen Lebensweg stets vorbehaltlos unterstützt und gefördert. Durch ihren steten Rückhalt, ihren Zuspruch und ihre Liebe

haben sie die Anfertigung dieser Arbeit erst ermöglicht. Ihnen sowie meinem Bruder, Michael Müller, widme ich diese Arbeit.

Würzburg, im November 2019

Daniel Müller

Inhaltsverzeichnis

Einleitung	23
I. Forschungsrahmen	28
II. Gang der Untersuchung	28

1. Kapitel

Technische und organisatorische Grundlagen	33
A. Begriffsbestimmung	33
I. Definition des NIST	34
II. Definition des BSI	37
III. Zusammenfassung	37
B. Erscheinungsformen	38
I. Cloud-Betriebsmodelle	39
1. Public Cloud	39
2. Private Cloud	41
3. Community Cloud	44
4. Hybrid Cloud	45
5. Virtual Private Cloud	47
II. Cloud-Service Modelle	48
1. Infrastructure as a Service (IaaS)	51
a) Charakteristika	51
b) IaaS in der Praxis	53
(1) Amazon Elastic Compute Cloud (Amazon EC2)	54
(2) Amazon Simple Storage Service (Amazon S3)	54
2. Platform as a Service (PaaS)	55
a) Charakteristika	55
b) PaaS in der Praxis	56
3. Software as a Service (SaaS)	57
a) Charakteristika	57
b) SaaS in der Praxis	58
4. Zusammenfassung	60

C. Referenzarchitektur	62
I. Ressourcenschicht	62
II. Virtualisierungsschicht	64
1. Virtuelle Maschinen	65
2. Virtual Machine Monitor	67
III. Serviceschicht	70
IV. Netzwerkschicht	74
V. Managementplattform	76

2. Kapitel

Insiderbedrohungen 83

A. Cybercrime-as-a-Service	84
B. Tätertypologische Betrachtung	86
I. Mitarbeiter der Cloud-Anbieter	90
II. Mitarbeiter der Subunternehmer	91
III. Nutzerseite	92
C. Tatmotive	93
D. Exemplarische Angriffsvektoren	94
I. Ressourcenschicht	97
II. Virtualisierungsschicht	99
III. Serviceschicht	110
IV. Netzwerkschicht	112
V. Managementplattform	115

3. Kapitel

Allgemeiner strafrechtlicher Schutz vor Kenntnisnahme und Verschaffung 119

A. Ausspähen von Daten, § 202a StGB	122
I. Geschütztes Rechtsgut	122
II. Tatobjekt	124
III. Nicht für den Täter bestimmt	129
1. Verfügungsberechtigung über die Daten	129
a) Eigentum am Datenträger	130
b) Inhaltliche Betroffenheit	131
c) Geistige Urhebererschaft	132
d) Kenntnis vom Benutzerpasswort	132

e) Geheimhaltungsinteresse	133
f) Skripturakt	133
2. Bestimmung des Verfügungsberechtigten	135
a) Allgemeine Grundsätze	135
b) Spezialfälle	143
(1) Sealed Cloud	143
(2) Split Cloud	145
IV. Gegen unberechtigten Zugang besonders gesichert	146
V. Zugangsverschaffung unter Überwindung der Zugangssicherung	153
1. Erfasste Angriffsmethoden der Inntäter	157
2. Strafbare Fälle der Datenspionage	162
VI. Unbefugt	168
VII. Weitere Voraussetzungen	169
VIII. Zusammenfassung	169
B. Abfangen von Daten, § 202b StGB	170
I. Nichtöffentliche Datenübermittlung, § 202b 1. Alt. StGB	171
1. Datenübermittlung	172
2. Nichtöffentlichkeit	176
II. Seitenkanalangriffe, § 202b 2. Alt. StGB	179
III. Unbefugte Datenverschaffung unter Anwendung technischer Mittel	180
IV. Zusammenfassung	182
C. Vorbereiten des Ausspähens und Abfangens von Daten, § 202c Abs. 1 StGB	184
I. Passwörter und Sicherungscodes, § 202c Abs. 1 Nr. 1 StGB	184
II. Schadprogramme, § 202c Abs. 1 Nr. 2 StGB	189
III. Zusammenfassung	193
D. Verletzung des Fernmeldegeheimnisses, § 206 Abs. 2 Nr. 1 StGB	194
I. Tauglicher Täterkreis	196
1. Telekommunikationsunternehmen	196
2. Beschäftigte der CaaS-Anbieter	200
3. Erweiterung des Täterkreises nach § 206 Abs. 3 StGB	203
II. Verschlüsselte Sendung	203
1. Sendung	204
2. Verschlüsselung	205
III. Zusammenfassung	206

4. Kapitel

Allgemeiner strafrechtlicher Schutz vor Weitergabe und Verwertung	208
A. Datenhehlerei, § 202d StGB	209
I. Tatgegenstand	210
II. Vollendete rechtswidrige Vortat	214
III. Sonstige Voraussetzungen	217
IV. Zusammenfassung	219
B. Verletzung des Fernmeldegeheimnisses, § 206 Abs. 1 StGB	219
I. Fernmelderelevante Tatsachen	220
II. Weitergabe von E-Mails, Text- oder Sprachnachrichten	224
III. Zusammenfassung	228
C. Verletzung und Verwertung von Privatgeheimnissen, §§ 203 Abs. 4, 204 Abs. 1 StGB	229
I. Tauglicher Täterkreis	232
1. § 203 Abs. 3 Satz 1 StGB	232
2. § 203 Abs. 3 Satz 2 StGB	235
II. Fremde Geheimnisse	243
III. Tathandlung	245
1. Offenbaren	245
2. Verwerten	247
IV. Sonstige Voraussetzungen	249
V. Unterlassene Verschwiegenheitserklärung, § 203 Abs. 4 Satz 2 StGB	252
VI. Zusammenfassung	255

5. Kapitel

Nebenstrafrechtlicher Schutz der Datenvertraulichkeit	256
A. Verrat von Geschäfts- und Betriebsgeheimnissen, § 17 UWG	256
I. Geschäfts- und Betriebsgeheimnisse als Tatobjekt	257
II. Geheimnisverrat, § 17 Abs. 1 UWG	261
III. Geheimnisausspähung und -verwertung, § 17 Abs. 2 UWG	263
1. Betriebsspionage, § 17 Abs. 2 Nr. 1 UWG	264
2. Geheimnishehlerei, § 17 Abs. 2 Nr. 2 UWG	266
IV. Weitere Tatbestandsvoraussetzungen	269
V. Zusammenfassung	271
B. Strafbarkeit nach § 148 Abs. 1 Nr. 1 TKG	274
I. Verstoß gegen das Abhörverbot aus § 89 Satz 1 TKG	275
1. Tatgegenstand	275

2. Tathandlung	277
II. Verstoß gegen das Mitteilungsverbot aus § 89 Satz 2 TKG	278
III. Zusammenfassung	278
C. Bußgeldnorm nach Art. 83 DSGVO	279
I. Anwendungsbereich	280
1. Sachlicher Anwendungsbereich	280
2. Räumlicher Anwendungsbereich	282
a) Niederlassungsprinzip, Art. 3 Abs. 1 DSGVO	283
b) Marktortprinzip, Art. 3 Abs. 2 lit. a DSGVO	287
c) Résumé	289
II. Ordnungswidrigkeit nach Art. 83 Abs. 4 lit. a, Abs. 5 lit. a DSGVO	289
1. Adressat der Bußgeldtatbestände	290
2. Bußgeldbewehrte Datenschutzverstöße nach Art. 83 Abs. 4 lit. a DSGVO ..	293
3. Bußgeldbewehrte Datenschutzverstöße nach Art. 83 Abs. 5 lit. a DSGVO ..	296
4. Verschuldenserfordernis	298
5. Rechtsfolge	301
III. Zusammenfassung	303
D. Strafvorschrift gem. § 42 BDSG	305
I. Anwendungsbereich	306
II. Tatgegenstand	307
III. Tauglicher Täter	310
IV. Tathandlungen des § 42 Abs. 1 BDSG	310
V. Tathandlungen des § 42 Abs. 2 BDSG	312
VI. Sonstige Voraussetzungen	313
VII. Zusammenfassung	314

6. Kapitel

Strafrechtlicher Schutz der Datenintegrität und -verfügbarkeit	317
A. Datenveränderung, § 303a StGB	317
I. Fremde Daten	318
II. Tathandlungen	324
1. Datenlöschung	325
2. Datenunterdrückung	327
3. Unbrauchbarmachen von Daten	330
4. Datenveränderung	331
III. Rechtswidrigkeit der Tathandlung	333
IV. Zusammenfassung	337

B. Computersabotage, § 303b StGB	337
I. Cloud als Datenverarbeitung von wesentlicher Bedeutung	339
II. Tathandlungen	344
1. Datenveränderung nach § 303a Abs. 1 StGB	344
2. Eingeben oder Übermitteln von Daten	345
3. Sabotagehandlungen am Cloud-System oder an Datenträgern	348
III. Erhebliche Störung der Datenverarbeitung als Taterfolg	352
IV. Qualifikation nach § 303b Abs. 2 StGB	354
V. Besonders schwere Fälle nach § 303b Abs. 4 StGB	355
VI. Zusammenfassung	357
C. Urkundenunterdrückung, § 274 Abs. 1 Nr. 2 StGB	357
I. Tatbestandsvoraussetzungen	357
II. Zusammenfassung	361
D. Verletzung des Fernmeldegeheimnisses, § 206 Abs. 2 Nr. 2 StGB	361
I. Anvertraute Sendung	362
II. Unterdrücken	365
III. Unbefugt	366
IV. Zusammenfassung	367

7. Kapitel

Anwendbarkeit des deutschen Strafrechts 369

A. Innentäter-Angriffe aus Deutschland	372
B. Innentäter-Angriffe aus dem Ausland	373
I. Betriebs- und Geschäftsgeheimnisse, § 5 Nr. 7 StGB	374
II. Geltung für Auslandstaten in anderen Fällen, § 7 StGB	375
III. Ubiquitätsprinzip, §§ 3, 9 StGB	381
1. Erfolgsdelikte	381
2. Abstrakte Gefährdungsdelikte	383
a) Ausdehnung des Handlungsorts	383
b) Erweiterung des Erfolgsorts	384
c) Fazit	387
C. Ausländische Angriffshandlung auf eine international verteilte Cloud-Infrastruktur	388
D. Innentäter-Angriff aus dem Ausland mittels inländischer Cloud-Server	391
E. Schutzbereich der verwirklichten Straftatbestände	393
I. Schutzbereich der §§ 202a ff. StGB	395

II. Schutzbereich der §§ 203, 204 StGB; § 206 StGB und § 17 UWG 395
 III. Schutzbereich des § 42 BDSG 396
 IV. Ergebnis zum Schutzbereich der deutschen Straf- und Bußgeldtatbestände 396
 F. Zusammenfassung 397

8. Kapitel

Strafrechtlicher Schutz de lege ferenda 398

A. Schutz der Datenvertraulichkeit 398
 I. Ergänzung der Tätergruppe des § 203 Abs. 1 StGB um „IT-Dienstleister“ 400
 II. Schaffung eines Straftatbestands der Datenuntreue, § 202d StGB-E 401
 III. Änderungsbedarf des § 202a StGB 408
 IV. Änderungsbedarf des § 202b StGB 410
 V. Änderungsbedarf des § 202c StGB 411
 VI. Änderungsbedarf des § 202d StGB 412
 VII. Änderungsbedarf des § 205 StGB 412
 B. Schutz der Integrität und Verfügbarkeit der Nutzerdaten 413
 I. Änderungsbedarf des § 303a StGB 414
 II. Änderungsbedarf des § 303b StGB 415
 C. Strafanwendungsrecht 416
 D. Internationale Strafverfolgung 420
Literaturverzeichnis 424
Sachverzeichnis 471

Abkürzungsverzeichnis

a.A.	andere(r) Ansicht
a.F.	alte Fassung
a.M.	am Main
Abb.	Abbildung
Abl.	Amtsblatt der Europäischen Union
Abs.	Absatz
ACL	Access Control List (Zugriffskontrollliste)
ACM	Association for Computer Machinery
AES	Advanced Encryption Standard
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft; Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AiB	Arbeitsrecht im Betrieb (Zeitschrift)
AktG	Aktiengesetz
Alt.	Alternative
Anm.	Anmerkung
AnwBl.	Anwaltsblatt (Zeitschrift)
AnwK	Anwaltskommentar
API	Application Programming Interface (Webbrowser oder Programmierschnittstelle)
App	Applikation (Anwendung)
ArbEG	Gesetz über Arbeitnehmererfindungen (Arbeitnehmererfindungsgesetz)
ArbRB	Der Arbeits-Rechtsberater (Zeitschrift)
ARP	Address Resolution Protocol
Art.	Artikel
ASP	Application Service Providing
AT	Allgemeiner Teil
AWS	Amazon Web Services
Az.	Aktenzeichen
BayObLG	Bayerisches Oberstes Landgericht
BB	Betriebs-Berater (Zeitschrift)
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck'scher Online Kommentar
BeckRS	Beck-Rechtsprechung
Begr.	Begründer
Beschl.	Beschluss
BGB	Bürgerliches Gesetzbuch
BGBI.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen

BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BKA	Bundeskriminalamt
BKartA	Bundeskartellamt
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMWi	Bundesministerium für Wirtschaft und Energie
BNotO	Bundesnotarordnung
BPaaS	Business Process as a Service
BPatG	Bundespatentgericht
BRAO	Bundesrechtsanwaltsordnung
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-Gesetz	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BT	Besonderer Teil
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfGK	Kammerentscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
bvitg	Bundesverband Gesundheits-IT e.V.
BvR	Aktenzeichen einer Verfassungsbeschwerde zum Bundesverfassungsgericht
bzw.	beziehungsweise
C ³	Compliant Community Cloud (Monographie der Bayerischen Innovationsstiftung)
ca.	circa
CaaS	Communication as a Service
CCPE	Concurrency and Computation: Practice and Experience (Zeitschrift)
CCS	Conference on Computer and Communications Security
CCZ	Corporate Compliance (Zeitschrift zur Haftungsvermeidung im Unternehmen)
CD	Compact Disc
CD-ROM	Compact Disc Read-Only Memory
CERT	Computer Emergency Response Team
CLOUD	3rd International Conference on Cloud Computing
CompaaS	Compute as a Service, Rechnen-als-Dienst
COMPSAC	Computer Software and Applications Conference
CPU	Central Processing Unit (Hauptprozessor eines Computers)
CR	Computer und Recht (Zeitschrift)
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CSRD	Computer Science Research + Development (Zeitschrift)
CSRF	Cross-Site-Request-Forgery
CSUR	ACM Computing Surveys (Zeitschrift)
d.h.	das heißt
DaaS	Desktop as a Service

D-A-CH	Deutschland-Österreich-Schweiz
DB	Der Betrieb (Zeitschrift)
DBaaS	Database as a Service
(D)DoS	(Distributed) Denial of Service
ders.	derselbe
DGRI	Deutsche Gesellschaft für Recht und Informatik e.V.
DHCP	Dynamic Host Configuration Protocol
dies.	dieselbe(n)
DIN	Deutsches Institut für Normung e.V.
DKA	Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
DNS	Domain Name System
DPI	Deep Packet Inspection
DRDoS	Distributed Reflected Denial of Service
DRiZ	Deutsche Richterzeitung
DSaaS	Data Storage as a Service
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSB	Datenschutz-Berater (Zeitschrift)
DSGVO	Datenschutzgrundverordnung
DSN-W	International Conference on Dependable Systems and Networks Workshops
DS-RL	Datenschutzrichtlinie
DSRITB	Tagungsband der Deutschen Stiftung für Recht und Informatik
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVD	Digital Versatile Disc
e.g.	exempli gratia
e.V.	eingetragener Verein
EC2	Amazon Elastic Compute Cloud
eco	Verband der deutschen Internetwirtschaft e.V.
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaften
EL	Ergänzungslieferung
E-Mail	electronic mail
ENISA	European Network and Information Security Agency (Europäische Agentur für Netz- und Informationssicherheit)
EP-VO	E-Privacy-Verordnung
ERP	Enterprise Ressource Planning
ERS-Verfahren	Evidence Record Syntax-Verfahren
etc.	et cetera (und so weiter)
ETS	Europe Treaty Series (Sammlung der Europäischen Verträge)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuR	Europarecht (Zeitschrift)
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum
f.	folgende
FAZ	Frankfurter Allgemeine Zeitung
ff.	fortfolgende
Fn.	Fußnote

FS	Festschrift
FTEG	Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen
GA	Goldammer's Archiv für Strafrecht (Zeitschrift)
GB	Gigabyte
GCE	Grid Computing Environments Workshop
GDD	Gesellschaft für Datenschutz und Datensicherheit e.V.
gem.	gemäß
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GMail	Google Mail
GmbH	Gesellschaft mit beschränkter Haftung
GMX	Global Message eXchange
GRCh	Charta der Grundrechte der Europäischen Union (Grundrechte-Charta)
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GWR	Gesellschafts- und Wirtschaftsrecht (Zeitschrift)
HaaS	Hardware as a Service
HansOLG	Hanseatisches Oberlandesgericht
HASE 2016	International Symposium on High Assurance Systems Engineering
HBVR	Hardware Based Virtualization Rootkits
HD-Video	High Definition-Video
HGB	Handelsgesetzbuch
HICSS	Hawaii International Conference on System Sciences
HiFi	High Fidelity
HMD	Handbuch der modernen Datenverarbeitung (Zeitschrift)
HPCaaS	High Performance Computing as a Service
HRRS	Online-Zeitschrift für Höchststrichterliche Rechtsprechung im Strafrecht
Hrsg.	Herausgeber
Hs.	Halbsatz
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transport Protocol Secure
HuaaS	Human as a Service
i.d.R.	in der Regel
i.S.d.	im Sinne der/des
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
IC2E	International Conference on Cloud Engineering
ICAC	International Conference on Automation and Computing
ICACCI	Conference on Advances in Computing, Communications and Informatics
ICCPCT	International Conference on Circuit, Power and Computing Technologies
ICECS	International Conference on Electronics and Communication Systems
ICSE	International Conference on Software Engineering
ICWS	International Conference on Web Services
IDS	Intrusion Detection System(e)
IDW	Institut für Wirtschaftsprüfer e.V.
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers (Berufsverband von Ingenieuren hauptsächlich aus den Bereichen Elektrotechnik und Informationstechnik)
IFIP	International Federation for Information Processing
iiWAS	International Conference on Information Integration and Web-based Applications & Services
IJACSA	International Journal of Advanced Computer Science and Applications (Zeitschrift)
IJARCE	International Journal of Advent Research in Computer and Electronics (Zeitschrift)
IJARCS	International Journal of Advanced Research in Computer Science & Technology (Zeitschrift)
IJCA	International Journal of Computer Applications (Zeitschrift)
IJCSIT	International Journal of Computer Science & Information Technology (Zeitschrift)
IJDSN	International Journal of Distributed Sensor Networks (Zeitschrift)
IJEIT	International Journal of Engineering and Innovative Technology (Zeitschrift)
IJERGS	International Journal of Engineering Research and General Science (Zeitschrift)
IJHPCA	International Journal of High Performance Computing Applications (Zeitschrift)
IJIET	International Journal of Information and Education Technology (Zeitschrift)
IJIS	International Journal of Information Security (Zeitschrift)
IJSR	International Journal of Science and Research (Zeitschrift)
IJSTR	International Journal of Scientific & Technology Research (Zeitschrift)
IKT	Informations- und Kommunikationstechnologien
IM+io	Information Management und Consulting (Zeitschrift)
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System(e)
ISO	International Organization for Standardization
ISRN	International Scholarly Research Notices
ISSE	Information Security Solutions Europe 2015 Conference der EEMA (European Association for e-Identity and Security)
IT Pro	IT Professional (Zeitschrift)
it	Information Technology (Zeitschrift)
IT	Informationstechnologie
ITRB	Der IT-Rechtsberater (Zeitschrift)
ITU	International Telecommunication Union
iur	Informatik und Recht (Zeitschrift)
JA	Juristische Arbeitsblätter (Zeitschrift)
jM	Die Monatszeitschrift
JoCCASA	Journal of Cloud Computing: Advances, Systems and Applications (Zeitschrift)
JoNaCA	Journal of Network and Computer Applications (Zeitschrift)
JoWUA	Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (Zeitschrift)
JR	Juristische Rundschau (Zeitschrift)

JSON	JavaScript Object Notation
JURA	Juristische Ausbildung (Zeitschrift)
jurisPR-Compl	juris PraxisReport Compliance & Investigations (Zeitschrift)
jurisPR-ITR	Juris PraxisReport IT-Recht (Zeitschrift)
JuS	Juristische Schulung (Zeitschrift)
JZ	Juristenzeitung
K&R	Kommunikation und Recht (Zeitschrift)
Kap.	Kapitel
KG	Kammergericht
KMS	Key Management Service (Dienst im Rahmen der Amazon Web Services zur Verwahrung der Datenverschlüsselung)
KMU	Kleine und mittlere (mittelständische) Unternehmen
KPMG	Firmennetzwerk von Wirtschaftsprüfungs- und Beratungsunternehmen
KriPoZ	Kriminalpolitische Zeitschrift
KWG	Gesetz über das Kreditwesen
LaaS	Landscape as a Service; Law as a Service
LAG	Landesarbeitsgericht
LAN	Local Area Network
LG	Landgericht
lit.	litera
LK	Leipziger Kommentar
LUN Masking	Logical Unit Number Masking
m.w.N.	mit weiteren Nachweisen
MAC-Adresse	Media-Access-Control-Adresse
MDR	Monatsschrift für Deutsches Recht (Zeitschrift)
medstra	Zeitschrift für Medizinstrafrecht
MK	Münchener Kommentar
MMR	MultiMedia und Recht (Zeitschrift)
n.F.	neue Fassung
NaaS	Network as a Service, Netzwerk-als-Dienst
NATO	North Atlantic Treaty Organization
NGCERT	Next Generation Certification
NIA	DIN-Normausschuss Informationstechnik und Anwendungen
NIST	National Institute of Standards and Technology
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJW-RR	NJW-Rechtsprechungs-Report (Zeitschrift)
NK	Nomos Kommentar
Nr.	Nummer(n)
NSA	National Security Agency
NStZ	Neue Zeitschrift für Strafrecht
NStZ-RR	NStZ-Rechtsprechungs-Report (Zeitschrift)
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NVwZ-RR	Neue Zeitschrift für Verwaltungsrecht Rechtsprechungs-Report
NZA	Neue Zeitschrift für Arbeitsrecht
NZA-RR	NZA-Rechtsprechungs-Report (Zeitschrift)
NZG	Neue Zeitschrift für Gesellschaftsrecht
NZWSt	Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht
OLG	Oberlandesgericht

OS	Operating System
OWiG	Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeitengesetz)
PaaS	Platform as a Service
PAO	Patentanwaltsordnung
PC	Personal Computer
PDA	Personal Digital Assistant
PDP-Verfahren	Provable Data Possession-Verfahren
PIK	Praxis der Informationsverarbeitung und Kommunikation (Zeitschrift)
PIN	Persönliche Identifikationsnummer
PinG	Privacy in Germany (Zeitschrift)
POP3	Post Office Protocol Version 3
PWC	PricewaterhouseCoopers GmbH
RAM	Random Access Memory (Arbeitsspeicher eines Rechners)
RDV	Recht der Datenverarbeitung (Zeitschrift)
REST	Representational State Transfer
RGSt	Entscheidungen des Reichsgerichts in Strafsachen
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RL	Richtlinie
Rn.	Randnummer(n)
RStGB	Reichsstrafgesetzbuch
RStV	Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag)
S&P	Symposium on Security and Privacy
S.	Satz; Seite(n)
S3	Amazon Simple Storage Service
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SCC-Jur	Juristisches Begleitforschungsprojekt „Sicheres Cloud Computing“
Session-ID	Session Identifier (Sitzungsnummer bzw. Sitzungskennung)
SFC	Securing the Financial Cloud
SIGCOMM	Special Interest Group on Data Communication
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz)
SK	Systematischer Kommentar
SMS	Short Message Service (Kurznachrichtendienst)
SMTP	Simple Mail Transfer Protocol
SOA	Serviceorientierte Architekturen
SOAP	Simple Object Access Protocol
SOCC	Symposium on Cloud Computing
sog.	so genannte(r/n/s)
SPOF	Single Point of Failure
SQL	Structured Query Language
SSL	Secure Socket Layer
SSYM	USENIX Security Symposium
StAG	Staatsangehörigkeitsgesetz
StÄG	Strafrechtsänderungsgesetz
StBerG	Steuerberatungsgesetz
StGB	Strafgesetzbuch

StGB-E	Entwurf zum Strafgesetzbuch
StIGH	Ständiger Internationaler Gerichtshof
StPO	Strafprozessordnung
StraFo	Strafverteidiger Forum (Zeitschrift)
StRR	StrafRechtsReport (Zeitschrift)
StV	Strafverteidiger (Zeitschrift)
StVG	Straßenverkehrsgesetz
SWD	Staff Working Document (Dokument der Europäischen Kommission)
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOR	The Onion Router
TrustCom	Conference on Trust, Security and Privacy in Computing and Communications
u.a.	unter anderem
U.S.C.	United States Code
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte (Urhebergesetz)
URL	Uniform Resource Locator
US/U.S.	United States
USA	United States of America (Vereinigte Staaten von Amerika)
USB	Universal Serial Bus
usw.	und so weiter
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	von; vom
VA	Virtual Appliances
Var.	Variante
VBIBW	Verwaltungsblatt für Baden-Württemberg (Zeitschrift)
VersR	Versicherungsrecht (Zeitschrift)
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
vgl.	vergleiche
VLAN	Virtual Local Area Network
VM	Virtuelle Maschine(n)
VMBR	Virtual-Machine Based Rootkit
VMM	Virtual Machine Monitor, Hypervisor
VoIP	Voice over Internet Protocol
Vorb.	Vorbemerkungen
VPN	Virtual Private Network
WI	Wirtschaftsinformatik (Zeitschrift)
WiKG	Gesetz zur Bekämpfung der Wirtschaftskriminalität
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WP	Working Paper (Arbeitspapier der Artikel-29-Datenschutzgruppe)
WPHG	Gesetz über den Wertpapierhandel (Wertpapierhandelsgesetz)
WPO	Gesetz über eine Berufsordnung der Wirtschaftsprüfer (Wirtschaftsprüferordnung)
WRP	Wettbewerb in Recht und Praxis (Zeitschrift)
XaaS	Everything as a Service bzw. Anything as a Service
XML	Extensible Markup Language
XSS	Cross-Site-Scripting

z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZEuS	Zeitschrift für Europarechtliche Studien
ZIP	Zeitschrift für Wirtschaftsrecht
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZÖR	Zeitschrift für öffentliches Recht
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZUM	Zeitschrift für Urheber und Medienrecht
zust.	zustimmend(er)
ZWH	Zeitschrift für Wirtschaftsstrafrecht und Haftung im Unternehmen

Einleitung

Die Informationstechnologie erfährt einen immer rascheren Wandel und beeinflusst inzwischen alle Lebensbereiche. Was noch vor Jahren eine Zukunftsvision war, gehört bereits heute zum Alltag einer digital vernetzten Welt. Jeder kann an nahezu jedem Ort mithilfe eines internetfähigen Geräts mit anderen Personen elektronisch kommunizieren, auf seine Daten, Bilder und Arbeitspapiere zugreifen, diese mit Freunden oder Arbeitskollegen teilen oder gemeinsam bearbeiten sowie Anwendungen jeglicher Art aus dem Internet beziehen. Diese globale Vernetzung und Kommunikation bei einer gleichzeitigen Erwartung an einer hohen Flexibilität, Kollaboration und Mobilität erfordern aber die Erreichbarkeit von hochverfügbaren IT-Dienstleistungen. Grundlage hierfür bildet das innovative Geschäftsmodell des Cloud Computing. Dessen Einsatzbereich ist dabei äußerst vielfältig und entwickelt sich von Speicherdiensten, Kommunikations- und Officeanwendungen hin zu neuen Geschäftsmodellen wie Big Data, Internet der Dinge, Industrie 4.0 oder dem autonomen Fahren, permanent weiter.¹

Inzwischen sind diese nahezu grenzenlos erscheinenden IT-Dienstleistungen aus der „Wolke des Internets“ aus dem Alltag von Privatpersonen und Unternehmen nicht mehr wegzudenken. So nutzten allein schon 2014 drei Viertel der Privatanutzer die Cloud vorwiegend als Speicherplatz, um persönliche Daten zu archivieren und mit Dritten zu teilen.² Auch im geschäftlichen Bereich wächst die Cloud-Nutzung stetig weiter. So haben bereits im Jahr 2016 mehr als die Hälfte der Unternehmen in Deutschland Geschäftsanwendungen aus der Cloud in Anspruch genommen.³ Nach einer Prognose des Verbands der deutschen Internetwirtschaft e.V. (eco) werden noch vor dem Jahr 2020 über 80 Prozent des weltweiten Datenverkehrs aus der Cloud kommen.⁴ Auf die Bedeutung des Cloud Computing als Wirtschaftsmotor in Deutschland verweist auch die Studie „Cloud Vendor Benchmark 2016“ der Experton Group, wonach 2015 der Gesamtumsatz des Cloud-Marktes 9,2 Milliarden Euro betrug und bis zum Jahr 2018 mit einer prognostizierten Wachstumsrate von

¹ *Johanning/Mildner*, Car IT, S. 19 f.; *Harter*, ERP Management (1) 2016, 57 (57); *Langmann/Stiller*, HMD (52) 2015, 647 (647 f.); *Eckert*, IM+io (29) 2014, 40 (42 ff.). Zu weiteren Einsatzbereichen siehe *BITKOM*, Geschäftsmodelle, S. 12 ff.

² *BITKOM*, Pressemitteilung vom 28.08.2014 „Cloud-Speicher verdrängen die Festplatte“; abrufbar unter <https://www.bitkom.org/Presse/Presseinformation/Cloud-Speicher-verdraengen-die-Festplatte.html> (zuletzt aufgerufen am 01.02.2018).

³ *KPMG AG/Bitkom Research GmbH*, Cloud Monitor 2016, S. 7, 15.

⁴ *Eco*, Pressemitteilung vom 24.05.2016 „Cloud wächst und wächst und wächst und wächst“; abrufbar unter <http://euromarcom.de/2016/05/cloud-waechst-und-waechst-und-waechst-und-waechst/> (zuletzt aufgerufen am 01.02.2018).

durchschnittlich 35 % auf rund 19,8 Milliarden Euro ansteigen soll.⁵ Um die Einsatzpotentiale weiter zu fördern, hat die Europäische Kommission die Strategie „Freisetzung des Cloud-Computing-Potentials in Europa“ beschlossen.⁶ Diese sieht Maßnahmen vor, die bis 2020 eine jährliche Steigerung des Bruttoinlandprodukts der Europäischen Union in Höhe von 160 Milliarden Euro bewirken sollen. Damit das Wachstum des Cloud Computing auch für die digitale Wirtschaft in Deutschland lanciert wird, steht es zudem im Zentrum der Digitalpolitik der Bundesregierung⁷ und im Fokus der „Digitalen Strategie 2025“ des Bundesministeriums für Wirtschaft und Energie (BMWi).⁸

Das ungebrochene Marktwachstum des Cloud Computing liegt vor allem an seinen vielfältigen wirtschaftlichen Vorteilen und Innovationspotentialen.⁹ Im Gegensatz zu klassischen Bezugsmodellen fallen für die Nutzung von IT-Ressourcen und Applikationen aus der Cloud keine Investitions- und Betriebskosten (Wartungs-, Energie-, Personalkosten, Lizenzgebühren etc.) an.¹⁰ Abgerechnet wird zudem nach dem tatsächlichen Verbrauch, was einen kosteneffizienten Einsatz der finanziellen Ressourcen ermöglicht.¹¹ Die Leistungen aus der Cloud sind außerdem in jede Richtung skalierbar, so dass auf schwankende Anforderungen dynamisch und flexibel reagiert werden kann.¹² Die sofortige Anpassung benötigter Ressourcen führt zu einer optimalen Auslastung des eigenen IT-Systems und macht eine langfristige Beschaffungsplanung überflüssig, da in Nebenzeiten nicht genauso viele Kapazi-

⁵ Der Cloud Vendor Benchmark ist abrufbar unter <http://www.experton-group.de/research/studien/cloud-vendor-benchmark-2016/overview.html> (zuletzt aufgerufen am 01.02.2018).

⁶ European Cloud Strategy 2012; abrufbar unter <https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy> (zuletzt aufgerufen am 01.02.2018).

⁷ Siehe hierzu die Grundsätze der Digitalpolitik der Bundesregierung, abrufbar unter https://www.digitale-agenda.de/Webs/DA/DE/Grundsaeetze/Grundsaeetze_Digitalpolitik/grundsaeetze-digitalpolitik_node.html (zuletzt aufgerufen am 01.02.2018); siehe auch *Bundesregierung*, Digitale Agenda 2014–2017, S. 5 ff.

⁸ BMWi, Digitale Strategie 2015, S. 47.

⁹ Ausführlich zu den Vorteilen Innovationsstiftung Bayerische Kommune, C³, S. 24; *Vossen/Haselmann/Hoeren*, Cloud Computing, S. 23 ff.; *Meir-Huber*, Cloud Computing, S. 64 ff.; *Metzger/Reitz/Villar*, Cloud Computing, S. 27 ff.; *Tetzner*, Sicherheitsanforderungen, S. 18 ff.; *Giebichenstein*, BB 2011, 2218 (2219 f.); speziell zu den Vorteilen für kleine und mittlere Unternehmen (KMU) auch *Wicker*, Cloud Computing, S. 49 ff.

¹⁰ *BITKOM*, Entscheider, S. 13, 21 f.; *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises*, Orientierungshilfe, S. 4; *Heckmann*, in: juris-Praxis-Kommentar, Kap. 9, Rn. 580, 605; *Barnitzke*, Rechtliche Rahmenbedingungen, S. 56 f.; *Kühling/Biendl*, CR 2014, 150 (150); *Pohle/Ammann*, CR 2009, 273 (274); ausführlich *Höllwarth*, Cloud Migration, S. 51 f.

¹¹ *Barnitzke*, Rechtliche Rahmenbedingungen, S. 57; *Brennscheidt*, Cloud Computing, S. 22; *Niemann/Paul*, K&R 2009, 444 (444); ausführlich zu den Abrechnungsmodellen *Meir-Huber*, Cloud Computing, S. 61 ff.; *Vossen/Haselmann/Hoeren*, Cloud Computing, S. 36 ff.

¹² *BSI*, Sicherheitsempfehlungen, S. 19; *Baun/Kunze/Nimis/Tai*, Cloud Computing, S. 2; *Kühling/Biendl*, CR 2014, 150 (150); *Sujecki*, K&R 2012, 312 (312); *Heidrich/Wegener*, MMR 2010, 803 (803); *Pohle/Ammann*, CR 2009, 273 (273 f.).

täten bereitgehalten werden müssen wie in Spitzenzeiten notwendig ist.¹³ Besonders kleinen und mittelständischen Unternehmen bietet das Cloud Computing die Chance, neue, ressourcenintensive und ubiquitäre Anwendungen verwenden zu können, die sie aufgrund der erforderlichen hohen Investitionen in die eigenen IT-Systeme oder fehlenden Know-hows sonst nicht in der Lage wären selbst zu betreiben.¹⁴ Dadurch bietet sich ihnen die Möglichkeit, neue Geschäftsfelder zu erschließen oder bestehende Prozesse und Arbeitsabläufe zu optimieren.¹⁵ Für Privatanwender liegen dagegen die Vorteile der Cloud-Dienste besonders in ihrer flexiblen und ortsungebundenen Erreichbarkeit.¹⁶ Zudem können sie auf dem eigenen Endgerät Rechenleistung und Speicherplatz einsparen, so dass sie selbst mit leistungsschwachen IT-Systemen rechenintensive Verarbeitungsprogramme nutzen können.¹⁷ Schließlich brauchen sie sich auch nicht um die Sicherheit der genutzten Software zu sorgen, da das Einspielen von Updates und Patches allein den Cloud-Anbietern obliegt.¹⁸

Diesen Vorteilen stehen aber auch zahlreiche neuartige Risiken gegenüber.¹⁹ Herausforderungen stellen sich bei der „Datenverarbeitung in der Wolke“²⁰ vor allem im Hinblick auf die Gewährleistung der klassischen Schutzziele der Daten- und Informationssicherheit,²¹ namentlich die Integrität (Schutz vor Datenmanipulationen und Informationsveränderungen),²² Verfügbarkeit (Gewährleistung der permanenten

¹³ *Vossen/Haselmann/Hoeren*, Cloud Computing, S. 33 f.; *Böhm/Leimeister/Riedl/Krcmar*, IM+io (24) 2009, 6 (6); *Nägele/Jacobs*, ZUM 2010, 281 (282); *Niemann/Paul*, K&R 2009, 444 (444); *Schulz/Rosenkranz*, ITRB 2009, 232 (233).

¹⁴ *Artikel-29-Datenschutzgruppe*, Stellungnahme 05/2012, S. 5; *Hennrich*, Cloud Computing, S. 40; *Barnitzke*, Rechtliche Rahmenbedingungen, S. 57.

¹⁵ *BITKOM*, Geschäftsmodelle, S. 9 ff.; *Vossen/Haselmann/Hoeren*, Cloud Computing, S. 34; *Hennrich*, Cloud Computing, S. 40; *Barnitzke*, Rechtliche Rahmenbedingungen, S. 57; *Giebichenstein*, BB 2011, 2218 (2219); *Gaul/Koehler*, BB 2011, 2229 (2229); *Münch/Doubrava/Essoh*, DuD 2011, 322 (322).

¹⁶ *Brennscheidt*, Cloud Computing, S. 21; *Heier/Abt/Maistry/Schewski*, in: Köhler-Schulte, Cloud Computing, S. 47.

¹⁷ *Mester*, DuD 2010, 675.

¹⁸ *Mester*, DuD 2010, 675; siehe auch *Wicker*, Cloud Computing, S. 25.

¹⁹ Ausführlich zu den Risiken beim Cloud Computing *ENISA*, Benefits, Risks 2009, S. 9 ff.; *International Working Group on Data Protection in Telecommunications*, Arbeitspapier, S. 2 ff.; *Vossen/Haselmann/Hoeren*, Cloud Computing, S. 121 ff., 175 ff.; *Giebichenstein*, BB 2011, 2218 (2220).

²⁰ Den Begriff verwenden u.a. *Wicker*, Cloud Computing, S. 23; *Wagner/Groß*, BB 2011, I (Beilage).

²¹ *International Working Group on Data Protection in Telecommunications*, Arbeitspapier, S. 2; *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises*, Orientierungshilfe, S. 2; *Vossen/Haselmann/Hoeren*, Cloud Computing, S. 176.

²² *Hennrich*, Cloud Computing, S. 208; *Vossen/Haselmann/Hoeren*, Cloud Computing, S. 181; *Terplan/Voigt*, Cloud Computing, S. 79; *Hennrich*, CR 2011, 546 (549); *Schultze-*