Please quote as: Krcmar, H.; Leimeister, J. M.; Roßnagel, A. & Sunyaev, A. (Hrsg.)
(2016): Cloud-Services aus der Geschäftsperspektive . Erscheinungsjahr/Year: 2016.
Verlag/Publisher: Springer Gabler, Wiesbaden.

Helmut Krcmar · Jan Marco Leimeister
Alexander Roßnagel · Ali Sunyaev *Hrsg.*

Cloud-Services aus der Geschäfts- perspektive

Springer Gabler

Cloud-Services aus der Geschäftsperspektive

Helmut Krcmar • Jan Marco Leimeister
Alexander Roßnagel • Ali Sunyaev
Herausgeber

Cloud-Services aus der Geschäftsperspektive

Springer Gabler

Herausgeber

Prof. Dr. Helmut Krcmar
Technische Universität München
Garching b. München, Deutschland

Prof. Dr. Jan Marco Leimeister
Universität Kassel
Kassel, Deutschland

Prof. Dr. Alexander Roßnagel
Universität Kassel
Kassel, Deutschland

Prof. Dr. Ali Sunyaev
Universität Kassel
Kassel, Deutschland

Das Projekt „Value4Cloud“ wurde als Beitrag zum Technologieprogramm „Trusted Cloud“ vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert – Förderkennzeichen 01MD11043A.

ISBN 978-3-658-08256-7

ISBN 978-3-658-08257-4 (eBook)

DOI 10.1007/978-3-658-08257-4

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

Springer Gabler

© Springer Fachmedien Wiesbaden 2016

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

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

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Gabler ist Teil von Springer Nature

Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH

Vorwort

Cloud-Services leiten einen grundlegenden Wandel in der Bereitstellung und Nutzung von IT ein. Durch die industrialisierte und zunehmend vernetzte Bereitstellung von IT-Services sowie die Nutzung von Effizienzpotenzialen durch Service-Anbieter verändern sich nicht nur angebotene Leistungen am Markt, sondern auch die Industrie- und Dienstleistungsstrukturen insgesamt. IT-Leistungen, die bisher individuell für einzelne Kunden gefertigt wurden, werden von diesen zunehmend in standardisierter Form nachgefragt, um Kostenvorteile zu erzielen. Attraktivere Kostenstrukturen – ermöglicht durch standardisiert angebotene Dienstleistungen zur parallelen Nutzung durch eine Vielzahl von Unternehmen –, sowie die mit dem Servicegedanken einhergehende Zunahme von Flexibilität scheinen dabei insbesondere für Cloud-Anwender kleinerer Unternehmensgrößen attraktiv. Für kleine und mittelständische Unternehmen scheint durch Cloud-Services eine Leistungsqualität erschwinglich, wie sie zuvor nur zu hohen Kosten oder in Großunternehmen unter Nutzung interner Skaleneffekte zu erzielen war. Viele IT-Verantwortliche in Unternehmen, im öffentlichen Sektor wie auch Datenschützer, Verbraucherschützer und die Netzmedienöffentlichkeit stehen dem breiten Einsatz des Cloud-Computing jedoch zum Teil mit großer Skepsis gegenüber.

Hier setzt das Projekt Value4Cloud an. Es wurden innovative Lösungsansätze zur Beseitigung technischer, struktureller, organisatorischer und rechtlicher Hemmnisse für den Einsatz von Cloud-Services skizziert und gemeinsam mit Cloud-Anbietern und Cloud-Anwendern bereits zur Laufzeit des Projekts erprobt und weiterentwickelt. Ziel war es, die rechtskonforme und innovative Weiterentwicklung von Cloud-Services ebenso voranzutreiben, wie die breitenwirksame Nutzung dieser Serviceangebote durch Unternehmen des deutschen Mittelstandes.

Zur Erreichung dieser Ziele entwickelte Value4Cloud marktunterstützende Mehrwertdienste, die auch in bestehende Marktplätze für Cloud-Dienste und Informationsportale eingebunden werden könnten. Die entwickelten Ergebnisse unterstützen Cloud-Anwender, aber auch Cloud-Anbieter:

Erstens benötigen Anwender für ihre Entscheidung strukturierte Informationen über einen Cloud-Dienst. Dazu entwickelt das Projekt Empfehlungen für eine Servicebeschreibung, mit der die Dienste leichter vergleichbar werden. Eine Kategorisierung der Dienste und Fallstudien erleichtern zusätzlich den Überblick. Zweitens entwickelt das Projekt ein auf der Servicebeschreibung aufbauendes Benchmarking von Cloud-Services nach einheitlichen Kriterien, in dem wichtige Diensteigenschaften wie Leistungsumfang, Rechtskonformität und Servicequalität vergleichbar werden. Drittens will Value4Cloud die Anwender bei der Qualitätsbewertung unterstützen. Dazu entwickelt das Projekt Möglichkeiten der Bewertung von Cloud-Diensten durch andere Anwender und erarbeitet ein Rahmenwerk zur Zertifizierung der Dienste durch unabhängige Dritte. Viertens entwickelt das Projekt vertrauensunterstützende Mehrwertdienste für mehr Transparenz in der Beschaffung, Auswahl und Nutzung.

Mit der so geschaffenen Transparenz und Vergleichbarkeit wird es im Gegenzug für die Cloud-Anbieter noch wichtiger, marktgerechte Angebote zu schaffen, die den Anforderungen der Kunden an Qualität, Vertrauenswürdigkeit und Verlässlichkeit genügen. Cloud-Anwender erwarten von ihren Cloud-Anbietern einerseits eine kostengünstige und effiziente Bereitstellung. Andererseits fordern sie kundenspezifische Innovationen. Value4Cloud unterstützt Cloud-Anbieter dabei, diesen Zielkonflikt zu meistern, und zwar in den Bereichen der rechtsverträglichen Gestaltung und innovativen Weiterentwicklung (Open-Innovation) von Cloud-Diensten. Die Rechtsverträglichkeit neuer Angebote wird durch Leitfäden zur rechtskonformen Servicegestaltung adressiert. Diese beziehen sich auf Fragen des Datenschutzes, des IT-Strafrechts und der Haftung.

Die Ergebnisse des Projekts – wie etwa der erarbeitete Vorschlag zur strukturierten und umfassenden Beschreibung von Cloud-Diensten sowie der zugehörige Leitfaden zur Unterstützung bei der Analyse von Cloud-Angeboten – stehen auf der Webseite des Projekts (www.value4cloud.de) zum Download bereit. Außerdem wurden die Ergebnisse an Fachverbände weitergegeben und Schulungskonzepte zum Einsatz der Projektergebnisse in der

Unternehmenspraxis entwickelt. Aktuelle Termine von Workshops oder aktualisierte Dokumente sind auf der Webseite ebenso abrufbar. Im wissenschaftlichen Bereich wurden die Ergebnisse in hochrangigen wissenschaftlichen Fachzeitschriften und auf Konferenzen vorgestellt.

Unser Dank gilt dem Bundesministerium für Wirtschaft und Energie (BMWi) und seinem Projektträger DLR, Arbeitsbereich Technische Innovationen in der Wirtschaft für die Finanzierung und Betreuung des Vorhabens. Unser persönlicher Dank gebührt Frau Jennifer Welp (BMWi) und Herrn Dr. Patrick Lay (DLR) für die Unterstützung und Begleitung des Projekts, sowie allen beteiligten Projektpartnern und Mitarbeitern für den unermüdlichen und engagierten Einsatz, ohne den dieses Vorhaben nicht möglich gewesen wäre. Dies sind insbesondere Jan Wollersheim, Patrick Hoberg, Andreas Reidt, Lysann Gebauer, Michael Kunz, Dr. Silke Jandt, Magda Wicker, Steffen Kroschwald, Stephan Schneider, Dr. Franz Glatz, Anette Keller, Robert Eberlein, Andreas Eberl, Friedrich Haarmann, Sabine Teufl, Dr. Matthias Söllner, Dr. Christoph Peters, Jens Lansing, Sebastian Lins und einige weitere.

Danken möchten wir auch unseren Unterstützern außerhalb des geförderten Projektkonsortiums, die mit ihrem Engagement und Expertenrat maßgeblich zum Erfolg des Vorhabens beigetragen haben. Dies sind insbesondere Christoph Hecker und Patrick Quellmalz (VOICE), Dr. Mathias Weber und Dr. Axel Garbers (BITKOM), Rolf Chung (BITMi), Dr. Jan Geert Meents (DLA Piper), Werner Schwarz (Gerolsteiner Brunnen), Detlev Mages (Konrad Kleiner), Dr. Michael Kranz (ThyssenKrupp), Eric Schmeling (NORMA Lebensmittelfilialbetrieb), Dr. Frank Simon (SQS Software Quality Systems), Werner Merkl (S-Y Systems Technologies Europe), Dr. Thomas Mannmeusel (Webasto), Dr. Jürgen Sturm (ZF Friedrichshafen) und Nils Burmester (BSH Bosch und Siemens Hausgeräte), Alexander Eichler (salesforce.com), Marius Würzner und Koba Metreveli (Sedo), sowie einige weitere.

Wir hoffen, dem Leser eine spannende und Nutzen stiftende Lektüre an die Hand geben zu können und wünschen dem Abschlussbericht die ihm gebührende weite Verbreitung.

Prof. Dr.
Helmut Krcmar

Prof. Dr.
Jan Marco Leimeister

Prof. Dr.
Alexander Roßnagel

Prof. Dr.
Ali Sunyaev

Inhaltsüberblick

Vorwort V

Inhaltsverzeichnis XIII

Teil A: Einleitung 1

- 1 Motivation, Bausteine und Vorgehensweise 3
J. Wollersheim, P. Hoberg, A. Reidt, H. Krcmar

Teil B: Der Markt für Cloud-Computing-Services 15

- 2 Ausgangslage und Definitorisches 17
*L. Gebauer, M. Kunz, P. Hoberg, S. Kroschwald, A. Reidt,
J. Schneider, M. Wicker, J. Wollersheim*
- 3 Service-Typen und Wertschöpfungsnetzwerke 31
P. Hoberg, H. Krcmar

Teil C: Unterstützungsbedarf aus Sicht Cloud-nutzender Unternehmen 39

- 4 Qualitätsanalyse und -bewertung von Cloud-Services 41
J. Wollersheim, H. Krcmar
- 5 Cloud-Service-Zertifizierung 53
A. Sunyaev, S. Schneider
- 6 Vertrauensproblematiken im Cloud-Computing-Umfeld 59
L. Gebauer, M. Söllner, J.M. Leimeister

Teil D: Unterstützungsbedarf aus Sicht Cloud-anbietender Unternehmen 71

- 7 Anforderungserhebung für eine Online-Community für Open
Service Innovation im Cloud-Computing-Umfeld 73
M. Kunz, P. Ebel, J.M. Leimeister
- 8 Relevante Rechtsfragen des Cloud-Computing 87
S. Jandt, S. Kroschwald, A. Roßnagel, M. Wicker

Teil E: Die Value4Cloud-Mehrwertdienste 91

- 9 Service-Auswahl – Entwicklung von Merkmalskatalog und Klassifizierungssystem 93
P. Hoberg, H. Krcmar
- 10 Servicebeschreibung – Entwicklung eines domänenspezifischen Vokabulars (eUSDL) 121
J. Wollersheim, H. Krcmar
- 11 Entwicklung und Implementierung eines Softwareprototyps zur Informationsunterstützung und Qualitätsbewertung 143
A. Reidt, H. Krcmar
- 12 Empfehlungen zur Gestaltung von Cloud-Service-Zertifizierungen ... 159
S. Schneider, J. Lansing, A. Sunyaev
- 13 Vertrauensunterstützende Mehrwertdienste – Ein systematisches Vorgehen zur Förderung von Vertrauen im Cloud-Computing-Umfeld 171
L. Gebauer, M. Söllner, J.M. Leimeister
- 14 Open Service Innovation Online-Community für Cloud-Service-Ökosysteme 187
M. Kunz, P. Ebel, J.M. Leimeister
- 15 Datenschutzkonformes Cloud-Computing 207
S. Jandt, S. Kroschwald, A. Roßnagel, M. Wicker
- 16 Vertragliche Aspekte des Cloud-Computing 267
S. Jandt, S. Kroschwald, A. Roßnagel, M. Wicker
- 17 Strafrechtliche Risiken beim Cloud-Computing 279
S. Kroschwald, A. Roßnagel, M. Wicker
- 18 Staatliche Zugriffe auf Daten in der Cloud 301
S. Kroschwald, A. Roßnagel, M. Wicker

Teil F: Marktunterstützung durch Einsatz der Value4Cloud-Mehrwertdienste 325

- 19 Marktunterstützung in den Bereichen Bedarfsanalyse, Service-Auswahl und Service-Management 327
J. Wollersheim, H. Krcmar

20	Entwicklung eines Kriterienkatalogs zur Zertifizierung von Cloud-Services.....	337
	<i>S. Schneider, J. Lansing, F. Gao, A. Sunyaev</i>	
21	Marktunterstützung durch vertrauensunterstützende Dienste.....	351
	<i>L. Gebauer, M. Söllner, J.M. Leimeister</i>	
22	Marktunterstützung durch Open Service Innovation.....	359
	<i>M. Kunz, P. Ebel, J.M. Leimeister</i>	
23	Marktunterstützung durch rechtskonforme Gestaltung von Cloud-Services.....	369
	<i>S. Kroschwald, M. Wicker, A. Roßnagel</i>	
24	Fallstudie: Werkzeug-unterstützte Analyse und Bewertung von Cloud Services aus Anwendersicht.....	379
	<i>J. Wollersheim, A. Keller, F. Glatz</i>	
25	Fallstudie: Open Innovation	399
	<i>R. Eberlein, A. Eberl</i>	
Teil G: Geschäftsmodelle.....		409
26	Geschäftsmodelle für marktunterstützende Mehrwertdienste im Cloud-Computing-Ökosystem.....	411
	<i>P. Hoberg, J. Wollersheim, H. Krcmar</i>	
Teil H: Anhang.....		423
27	Veröffentlichungen.....	425
	Die Autoren.....	433

Inhaltsverzeichnis

Vorwort	V
---------------	---

Inhaltsüberblick	IX
------------------------	----

Teil A: Einleitung 1

1 Motivation, Bausteine und Vorgehensweise.....	3
<i>J. Wollersheim, P. Hoberg, A. Reidt, H. Krcmar</i>	
1.1 Motivation und Ziele des Projekts	3
1.2 Die Value4Cloud-Projektbausteine.....	5
1.2.1 Bedarfspezifikation und Servicebeschreibung.....	7
1.2.2 Qualitätsbewertung und Benchmarking	7
1.2.3 Vertrauensentwicklung in Cloud-Services und Serviceanbieter	8
1.2.4 Kundenorientierte Weiterentwicklung – Open Innovation.....	8
1.2.5 Rechtskonforme Bereitstellung und Nutzung	9
1.2.6 Zertifizierung von Cloud-Services	9
1.3 Vorgehen und Partner für den nachhaltigen Transfer der Ergebnisse	10
1.3.1 Das Vorgehen.....	11
1.3.2 Die Projektpartner	12
1.4 Aufbau dieses Abschlussbandes	13
1.5 Literaturverzeichnis	14

Teil B: Der Markt für Cloud-Computing-Services 15

2 Ausgangslage und Definitorisches.....	17
<i>L. Gebauer, M. Kunz, P. Hoberg, S. Kroschwald, A. Reidt, S. Schneider, M. Wicker, J. Wollersheim</i>	
2.1 Cloud-Computing.....	17
2.2 Cloud-Services und ihre Bereitstellungsmodelle	20
2.3 Herausforderungen für Cloud-Anwender und Cloud-Anbieter.....	22
2.3.1 Spezifikation des Service-Bedarfs	24
2.3.2 Bewertung der Service-Qualität.....	24
2.3.3 Vertrauen in der Wirtschaftsinformatik	25

2.3.4	Rechtskonforme Bereitstellung und Nutzung von Services	26
2.3.5	Innovative Weiterentwicklung von Cloud-Services	27
2.3.6	Unterstützung von Anbietern bei der Zertifizierung von Services	28
2.4	Literaturverzeichnis	29
3	Service-Typen und Wertschöpfungsnetzwerke	31
	<i>P. Hoberg, H. Krcmar</i>	
3.1	Vom traditionellen IT-Outsourcing zum Cloud-Computing.....	31
3.2	Veränderte Wertschöpfungsstrukturen im Cloud-Computing	33
3.3	Standardisierungsproblem im Cloud-Markt.....	36
3.4	Literaturverzeichnis	37
 Teil C: Unterstützungsbedarf aus Sicht Cloud-nutzender Unternehmen		
39		
4	Qualitätsanalyse und -bewertung von Cloud-Services	41
	<i>J. Wollersheim, H. Krcmar</i>	
4.1	Einleitung.....	41
4.2	Qualität – eine Begriffsbestimmung	42
4.3	Qualitätsanalyse und -bewertung von Cloud-Services aus der Käufer-Perspektive	45
4.4	Zusammenfassung: identifizierter Unterstützungsbedarf aus Sicht Cloud-nutzender Unternehmen.....	47
4.5	Literaturverzeichnis	49
5	Cloud-Service-Zertifizierung.....	53
	<i>A. Sunyaev, S. Schneider</i>	
5.1	Zertifizierung von Cloud-Services.....	53
5.2	Herausforderungen bei der Zertifizierung von Cloud-Services ...	56
5.3	Fazit	57
5.4	Literaturverzeichnis	58
6	Vertrauensproblematiken im Cloud-Computing-Umfeld.....	59
	<i>L. Gebauer, M. Söllner, J.M. Leimeister</i>	
6.1	Die Bedeutung von Vertrauen im Cloud-Computing-Umfeld	59
6.2	Nutzungshemmnisse im Cloud-Computing-Umfeld.....	60
6.3	Vertrauensbeziehungen im Cloud-Computing-Umfeld	62

6.4	Zuordnung der Nutzungshemmnisse zu den Vertrauensbeziehungen	65
6.5	Zusammenfassung	67
6.6	Literaturverzeichnis	68

Teil D: Unterstützungsbedarf aus Sicht Cloud-anbietender Unternehmen 71

7	Anforderungserhebung für eine Online-Community für Open Service Innovation im Cloud-Computing-Umfeld	73
	<i>M. Kunz, P. Ebel, J.M. Leimeister</i>	
7.1	Einleitung	73
7.2	Theoretischer Hintergrund	74
	7.2.1 Online-Communities	74
	7.2.2 Ideen-Communities	75
7.3	Anforderungserhebung	76
	7.3.1 Anforderungen an den Innovationsprozess	77
	7.3.2 Anforderungen an die Online-Community	79
7.4	Schlussbetrachtung	84
7.5	Literaturverzeichnis	85
8	Relevante Rechtsfragen des Cloud-Computing	87
	<i>S. Jandt, S. Kroschwald, A. Roßnagel, M. Wicker</i>	
8.1	Privatrechtliche Beziehung zwischen Cloud-Anbieter und Cloud-Nutzer	87
8.2	Öffentliche-rechtliche Beziehung zwischen Cloud-Anbieter und Cloud-Nutzer	87
8.3	Datenschutzrecht	88
8.4	Materielles und prozessuales Strafrecht	88

Teil E: Die Value4Cloud-Mehrwertdienste 91

9	Service-Auswahl – Entwicklung von Merkmalskatalog und Klassifizierungssystem	93
	<i>P. Hoberg, H. Krcmar</i>	
9.1	Einleitung	93
9.2	Stand der Forschung	94
9.3	Der Value4Cloud-Kriterienkatalog	96

9.3.1	Basissicht	97
9.3.2	Technische Sicht	108
9.3.3	Funktionale Sicht	113
9.3.4	Operative Sicht.....	114
9.3.5	Rechtliche Sicht	116
9.4	Literaturverzeichnis	119
10	Servicebeschreibung – Entwicklung eines domänenspezifischen Vokabulars (eUSDL).....	121
	<i>J. Wollersheim, H. Krcmar</i>	
10.1	Einleitung.....	121
10.2	USDL-Erweiterung zur Beschreibung von Cloud-Services (eUSDL)	122
10.2.1	Bestehende Herausforderungen	123
10.2.2	Vorstellung der Servicebeschreibungssprache USDL ..	123
10.2.3	Vorgehen zur Identifikation des benötigten Vokabulars	125
10.2.4	Ergebnisbeschreibung – eUSDL	126
10.3	Entwicklung von Qualitätskriterien-Sets für variierende Beschaffungsobjekte	133
10.3.1	Bestehende Herausforderungen	133
10.3.2	Vorgehen zur Identifikation des Kriterien-Sets	133
10.3.3	Ergebnisbeschreibung – beispielhaftes Suchprofil	134
10.4	Entwicklung von Qualitätskriterien-Sets für die Nutzungsphase von Cloud-Services.....	137
10.4.1	Bestehende Herausforderungen	137
10.4.2	Vorgehen zur Identifikation des Kriteriensets	138
10.4.3	Ergebnisbeschreibung – kontinuierliche Qualitätsbewertung	138
10.5	Zusammenfassung der Ergebnisse und Ausblick.....	140
10.6	Literaturverzeichnis	141
11	Entwicklung und Implementierung eines Softwareprototyps zur Informationsunterstützung und Qualitätsbewertung.....	143
	<i>A. Reidt, H. Krcmar</i>	
11.1	Hintergrund des Prototyps	143
11.2	Datenmodell Plattform.....	144
11.3	Funktionen und Darstellung.....	147
11.3.1	Administrator	147
11.3.2	Service-Nutzer	149

11.3.3	Service-Provider.....	155
11.4	Zusammenfassung der Ergebnisse und Ausblick.....	157
12	Empfehlungen zur Gestaltung von Cloud-Service-Zertifizierungen ...	159
	<i>S. Schneider, J. Lansing, A. Sunyaev</i>	
12.1	Einleitung.....	159
12.2	Wahrnehmung von Cloud-Service-Zertifizierungen.....	162
12.3	Gestaltungsempfehlungen für Cloud-Service-Zertifizierungen ..	163
12.4	Fazit ..	168
12.5	Literaturverzeichnis	169
13	Vertrauensunterstützende Mehrwertdienste – Ein systematisches Vorgehen zur Förderung von Vertrauen im Cloud-Computing- Umfeld.....	171
	<i>L. Gebauer, M. Söllner, J.M. Leimeister</i>	
13.1	Prozess zur systematischen Vertrauensunterstützung	171
13.2	Schritt 1: Identifikation relevanter Unsicherheiten	173
13.3	Schritt 2: Identifikation relevanter Vertrauensdimensionen	175
13.4	Schritt 3: Identifikation relevanter Vertrauensdeterminanten	177
13.5	Schritt 4: Ableitung vertrauensbezogener Anforderungen.....	180
13.6	Schritt 5: Ableitung vertrauensunterstützender Mehrwertdienste.....	182
13.7	Zusammenfassung.....	184
13.8	Literaturverzeichnis	184
14	Open Service Innovation Online-Community für Cloud-Service-Ökosysteme	187
	<i>M. Kunz, P. Ebel, J.M. Leimeister</i>	
14.1	Einleitung.....	187
14.2	Zentrale Merkmale der Open Service Innovation Online-Community	188
14.2.1	Allgemeine Einführung.....	188
14.2.2	Ideen erstellen	190
14.2.3	Ideen ansehen.....	203
14.2.4	Weitere Funktionen.....	204
14.3	Schlussbetrachtung.....	205
14.4	Literaturverzeichnis	206
15	Datenschutzkonformes Cloud-Computing	207
	<i>S. Jandt, S. Kroschwald, A. Roßnagel, M. Wicker</i>	

15.1	Cloud-Computing und Datenschutzrecht	207
15.1.1	Gegenstand des Datenschutzrechts	208
15.1.2	Datenschutzrechtlich Beteiligte beim Cloud-Computing	209
15.1.3	Datenschutzrecht im Projekt Value4Cloud	210
15.2	Datenschutzrechtliche Anforderungen für Cloud-Nutzer	212
15.2.1	Welchen Datenschutznormen unterliegt der Cloud-Nutzer?	212
15.2.2	Unter welchen Voraussetzungen darf ein Cloud-Nutzer eine Cloud nutzen?	223
15.2.3	Welche Betroffenenrechte muss der Cloud-Nutzer berücksichtigen?	243
15.3	Datenschutzrechtliche Anforderungen für Cloud-Anbieter	246
15.3.1	Persönlicher Anwendungsbereich – der Cloud-Anbieter als verantwortliche Stelle	246
15.3.2	Räumliche Anwendbarkeit des Datenschutzrechts auf den Cloud-Anbieter	247
15.3.3	Zulässigkeit des verantworteten Datenumgangs	249
15.3.4	Zulässigkeit des Datenumgangs als Auftragnehmer	251
15.3.5	Technische und organisatorische Maßnahmen	252
15.4	Gestaltungsvorschläge für einen Dienst zur Nutzerunterstützung	252
15.4.1	Unterstützung bei der Anonymisierung, Pseudonymisierung und Datenverschlüsselung	253
15.4.2	Unterstützung bei der Ermittlung des datenschutzrechtlichen Verantwortungsbereichs der Beteiligten	254
15.4.3	Unterstützung bei der Feststellung des anwendbaren Datenschutzrechts	255
15.4.4	Unterstützung bei der Bestimmung der Zulässigkeit der Cloud-Nutzung	255
15.4.5	Unterstützung bei der Abwägung von Einwilligungslösungen	257
15.4.6	Unterstützung bei der Einhaltung der Vorgaben zur Auftragsdatenverarbeitung	257
15.4.7	Unterstützung beim grenzüberschreitenden Cloud-Computing	259
15.4.8	Unterstützung bei der Einhaltung von Betroffenenrechten und technisch-organisatorischen Maßnahmen	260

15.5	Literaturverzeichnis	261
16	Vertragliche Aspekte des Cloud-Computing	267
	<i>S. Jandt, S. Kroschwald, A. Roßnagel, M. Wicker</i>	
16.1	Allgemeine Geschäftsbedingungen beim Cloud-Vertrag.....	267
16.2	Cloud-Ressourcen als Mietgegenstand	268
16.3	Notwendige Regelungen im Cloud-Vertrag.....	269
16.3.1	Verfügbarkeit	270
16.3.2	Haftung und Gewährleistung	271
16.3.3	Beendigung und Rückabwicklung	272
16.3.4	Streitvermeidende Vertragsinhalte	273
16.4	Gestaltungsempfehlungen für Cloud-Verträge	274
16.4.1	Anforderungen an einen Cloud-Vertrag	275
16.4.2	Empfehlungen an den Cloud-Anbieter	276
16.5	Literaturverzeichnis	277
17	Strafrechtliche Risiken beim Cloud-Computing.....	279
	<i>S. Kroschwald, A. Roßnagel, M. Wicker</i>	
17.1	Einleitung	279
17.2	Strafrechtlich relevantes Verhalten der Cloud-Akteure	280
17.3	Strafbarkeitsrisiken der Cloud-Akteure	281
17.3.1	Strafbarkeitsrisiko des Cloud-Nutzers	281
17.3.2	Telekommunikationsdiensteanbieter	283
17.3.3	Öffentliche Verwaltung	284
17.3.4	Verletzung des Steuergeheimnisses	285
17.3.5	Verstoß gegen Datenschutzrecht	285
17.3.6	Strafbarkeitsrisiko des Cloud-Anbieters	287
17.4	Praktische Relevanz der Strafbarkeitsrisiken	293
17.5	Gestaltungsempfehlung für die Cloud-Akteure	294
17.5.1	Gestaltungsempfehlungen für Cloud-Nutzer	294
17.5.2	Gestaltungsempfehlung für Cloud-Anbieter	295
17.5.3	Unterstützung zur Vermeidung der Strafbarkeit	296
17.6	Literaturverzeichnis	297
18	Staatliche Zugriffe auf Daten in der Cloud.....	301
	<i>S. Kroschwald, A. Roßnagel, M. Wicker</i>	
18.1	Einleitung	301
18.2	Grundlagen der Ermittlungsmaßnahmen	302
18.2.1	Ermittlungen von Straftaten	303
18.2.2	Daten als Beweismittel.....	303

18.2.3	Heimliche Maßnahmen in der Strafprozessordnung	305
18.3	Zugriffe gegenüber dem Cloud-Nutzer	306
18.3.1	Ablauf der Ermittlungen	306
18.3.2	Zugriff am Ort des Cloud-Anbieters	307
18.3.3	Zugriffe am Ort des Cloud-Nutzers	311
18.3.4	Heimliche Zugriffe von entfernten Orten	313
18.3.5	Zugriffe auf die Datenübertragung	314
18.3.6	Untersuchung der Daten aus der Cloud	314
18.3.7	Zugriffe gegenüber dem Cloud-Anbieter	317
18.4	Gestaltungsempfehlungen	317
18.4.1	Gestaltungsempfehlungen für Cloud-Nutzer	318
18.4.2	Gestaltungsempfehlungen für Cloud-Anbieter	319
18.4.3	Ausländische Angebote und ausländische Strafverfolgungsbehörden	321
18.4.4	Cloud-Computing ohne zusätzliche strafprozessuale Risiken	322
18.5	Literaturverzeichnis	322

Teil F: Marktunterstützung durch Einsatz der Value4Cloud-Mehrwertdienste 325

19	Marktunterstützung in den Bereichen Bedarfsanalyse, Service-Auswahl und Service-Management	327
	<i>J. Wollersheim, H. Krcmar</i>	
19.1	Einleitung	327
19.2	Werkzeuge zur Unterstützung der Bedarfsanalyse	328
19.3	Werkzeuge zur Unterstützung der Service-Auswahl	331
19.4	Werkzeuge zur Unterstützung des Service-Managements	332
19.5	Zusammenfassung der Marktunterstützung	334
19.6	Literaturverzeichnis	335
20	Entwicklung eines Kriterienkatalogs zur Zertifizierung von Cloud-Services	337
	<i>S. Schneider, J. Lansing, F. Gao, A. Sunyaev</i>	
20.1	Einleitung	337
20.2	Vorgehensweise zur Taxonomieentwicklung	338
20.3	Ergebnisse	343
20.4	Zusammenfassung der Marktunterstützung durch Zertifizierungen	346

20.5	Literaturverzeichnis	347
21	Marktunterstützung durch vertrauensunterstützende Dienste	351
	<i>L. Gebauer, M. Söllner, J.M. Leimeister</i>	
21.1	Einleitung	351
21.2	Durchführung von Experteninterviews	351
21.3	Ableitung und Priorisierung vertrauensförderlicher Faktoren ...	352
21.4	Ableitung und Priorisierung vertrauensförderlicher Maßnahmen.....	353
21.5	Zusammenfassung.....	357
21.6	Literaturverzeichnis	357
22	Marktunterstützung durch Open-Service-Innovation	359
	<i>M. Kunz, P. Ebel, J.M. Leimeister</i>	
22.1	Einleitung	359
22.2	Funktionsweise und Einsatzgebiete von Ideenwettbewerben	359
22.3	Einordnung in den Innovationsprozess	361
22.4	Die Cloud-Computing-Stakeholder	362
22.5	Ablauf des Ideenwettbewerbs	364
22.6	Schlussbetrachtung.....	366
22.7	Literaturverzeichnis	367
23	Marktunterstützung durch rechtskonforme Gestaltung von Cloud-Services.....	369
	<i>S. Kroschwald, M. Wicker, A. Roßnagel</i>	
23.1	Einleitung.....	369
23.2	Datenschutz-Rechtsverträglichkeit	370
	23.2.1 Verschlüsselung	370
	23.2.2 Auftragsdatenverarbeitung.....	371
	23.2.3 Auslandsbezug	372
	23.2.4 Betroffenenrechte.....	373
23.3	Vertragsrechtsverträglichkeit	373
23.4	Strafrechtsverträglichkeit	375
23.5	Strafprozessrechtsverträglichkeit	376
24	Fallstudie: Werkzeug-unterstützte Analyse und Bewertung von Cloud-Services aus Anwendersicht	379
	<i>J. Wollersheim, A. Keller, F. Glatz</i>	
24.1	Einleitung	379
24.2	Das Geschäftsszenario der Fallstudie.....	380

24.3	Szenario-Analyse und Strukturierung enthaltener Problemstellungen	386
24.4	Einsatz unterstützender Werkzeuge zur Problemlösung	390
24.4.1	Werkzeug A: Analyserahmen für den Beschaffungsprozess beeinflussende Faktoren	390
24.4.2	Werkzeug B: Template zur Festlegung von Verantwortlichkeiten im Beschaffungsprozess	392
24.4.3	Werkzeug C: Schema zur Identifikation und Klassifizierung des Schutzbedarfs	393
24.4.4	Werkzeug D: Der Kriterienkatalog CloudServiceCheck als Template in der Anforderungsspezifikation	395
24.5	Zusammenfassung und Teilnehmer-Rückmeldungen	396
24.6	Literaturverzeichnis	397
25	Fallstudie: Open-Innovation	399
	<i>R. Eberlein, A. Eberl</i>	
25.1	Einleitung	399
25.2	SpaceNet AG – ein Überblick	400
25.2.1	Das Unternehmen	400
25.2.2	Produktentwicklung	400
25.2.3	Virtualisierung vs. Cloud	401
25.3	Praxisevaluation: Workshops	401
25.3.1	Übersicht	401
25.3.2	Methodik, Umsetzung, Ablauf	402
25.3.3	Ergebnisse	403
25.4	Exkurs: Open-Innovation mittels Online-Community	405
25.4.1	Umsetzung Testworkshop mit Studenten	405
25.4.2	Einschätzung Online-Portal	406
25.5	Quellverzeichnis	407
Teil G:	Geschäftsmodelle	409
26	Geschäftsmodelle für marktunterstützende Mehrwertdienste im Cloud-Computing-Ökosystem	411
	<i>P. Hoberg, J. Wollersheim, H. Krcmar</i>	
26.1	Einleitung	411
26.2	Das Produkt- und Leistungsprogramm	412
26.2.1	Anwendercoaching	414

26.2.2	Service-Auswahl	415
26.2.3	Anbietercoaching	416
26.2.4	Marktanalyse und Innovation.....	418
26.3	Allgemeine Marktlage.....	419
26.4	Ausblick und Kommunikation	421
26.5	Literaturverzeichnis	421
 Teil H: Anhang.....		423
27	Veröffentlichungen	425
Die Autoren.....		433

Teil A: Einleitung

1 Motivation, Bausteine und Vorgehensweise

J. Wollersheim, P. Hoberg, A. Reidt, H. Krcmar

1.1 Motivation und Ziele des Projekts

Ein Grund für die Zurückhaltung des deutschen Mittelstandes bei der Adoption von Cloud-Computing ist in der am Markt vorherrschenden Informationsasymmetrie zu finden. Sie erschwert es einerseits den Anwendern, Cloud-Services hinsichtlich ihrer individuellen Vorteilhaftigkeit und den verbundenen Risiken umfassend zu bewerten, und erschwert es andererseits den Anbietern, ihr Serviceangebot an den Bedürfnissen potenzieller Kunden auszurichten. Die Förderung des Informationsaustauschs zwischen mittelständischen Cloud-Anbietern und Cloud-Anwendern ist somit eine Grundvoraussetzung für die breitenwirksame Nutzung und Entwicklung innovativer Cloud-Angebote. Eine Erhebung unter deutschen CIOs hat gezeigt, dass Cloud-Computing im Jahr 2010 kaum eine große Rolle spielt (Krcmar/Leimeister 2010). Die nur geringe Adoption des Cloud-Computing-Modells im Jahr 2010 lässt sich vor allem auf die im deutschen Mittelstand weit verbreitete Skepsis gegenüber „Modethemen“ zurückführen. So bestehen aus Anwendersicht vor allem Zweifel hinsichtlich der Zuverlässigkeit der Services, der Datensicherheit und dem Datenschutz, der tatsächlich realisierbaren Vorteile, aber auch hinsichtlich der Rechtskonformität. Zudem führt die Komplexität der Thematik, die mangelnde Erfahrung mit konkreten Anwendungs- und Einsatzszenarien für den Mittelstand und das Fehlen von Leitfäden für die Auswahl, Einführung und den Betrieb von Cloud-Services zur bisher geringen Adoptionsrate (Golkowsky/Vehlow 2011, S. 29).

Oft sind es gerade die kleinen und mittelständischen Unternehmen, die Nischenmärkte entdecken und erschließen und somit neue innovative Angebote bzw. Geschäftsmodelle hervorbringen. Folglich birgt eine verbreitete Nutzung von Cloud-Services auch für Anbieter ein großes Potenzial. Um dieses zu nutzen, ist es jedoch essenziell, dass die Bedürfnisse der kleinen und mittelständischen Anwendungsunternehmen individuell im Innovationsprozess des Anbieters aufgegriffen werden, um so die Attraktivität der angebotenen Leistung für den Anwender zu erhöhen, seine unternehmerischen

Risiken zu reduzieren und zu einer höheren Innovationsbereitschaft beizutragen. Durch qualitativ hochwertige Forschungsergebnisse, die vor allem die mittelstandspezifischen Probleme von Cloud-Anbietern, Cloud-Anwendern und Interessenten analysieren und Handlungsempfehlungen ableiten, kann die Basis für eine breitenwirksame Bereitstellung und Nutzung von Serviceangeboten im deutschen Mittelstand geschaffen werden. Zusammenfassend können sechs zentrale Probleme benannt werden:

- Bislang hält sich der deutsche Mittelstand auf breiter Ebene trotz eindeutiger Vorteile des Cloud-Computing-Modells sowohl auf Anbieter- als auch auf Anwenderseite noch weitestgehend zurück. Dies ist vor allem auf eine im deutschen Mittelstand verbreitete generelle Skepsis sowie die Tatsache, dass die potenziellen Anwender auch noch zu wenig in die Innovationsgestaltung der Anbieter einbezogen werden und Lösungsangebote nicht ihren Bedarf adressieren, zurückzuführen.
- Viele Cloud-Computing-Angebote sind für Anwender undurchsichtig und es liegen große Informationsasymmetrien zwischen Anbieter und Anwender vor. Anwendern aus dem deutschen Mittelstand mangelt es an geeigneten, qualifizierten, vertrauenswürdigen Vorgehensweisen und Informationen, um Cloud-Services hinsichtlich ihrer individuellen Vorteilhaftigkeit und den damit verbundenen Risiken zu bewerten.
- Mittelständischen Anwendern mangelt es an Möglichkeiten und Metriken, die Qualität von Cloud-Services zum Zeitpunkt der Beschaffung – wie auch kontinuierlich während der Nutzung – hinreichend gut zu bewerten und Auswahl- und Vergleichsentscheidungen zu fundieren.
- Es existieren noch viel zu wenige zielgruppenspezifische Cloud-Angebote für mittelständische Anwender, etwa branchenspezifische Lösungen. Dies ist u.a. auf Hürden im Innovationsprozess sowie insb. die zu geringe Nutzung von Innovationspotenzialen der Anwender und das Fehlen einer kontinuierlichen (Weiter-) Entwicklung von Cloud-Service-Ideen zurückzuführen.
- Heutzutage lassen sich große Unsicherheiten bei Anwendern hinsichtlich der Rechtskonformität von Cloud-Service-Angeboten beobachten. Mittel-

ständische Anbieter stehen demgegenüber immer wieder vor der Herausforderung auch Nischen-orientierte, bedarfsspezifischere Serviceangebote rechtsverträglich zu gestalten.

Das Projekt Value4Cloud setzt hier an und entwickelt marktunterstützende Mehrwertdienste für Cloud-Services, die sowohl auf bestehenden Marktplätzen und Informationsportalen eingebunden, als auch als eigenständige Werkzeuge von Cloud-Anbietern oder -Anwendern genutzt werden können. Ziel ist es zum einen, mittelständische Anwender bspw. bei der Bewertung von Qualitäts- und Nutzenaspekten von Cloud-Services umfassend zu unterstützen, um Vertrauen in die Serviceangebote und Anbieter zu befördern. Dies erfordert, dass nicht nur technische, sondern auch strukturelle, organisatorische, ökonomische und rechtliche Hemmnisse für den Einsatz von Cloud-Services im Mittelstand zunächst einmal identifiziert und im nächsten Schritt beseitigt werden müssen. Die Value4Cloud-Projektergebnisse sind entsprechend darauf ausgerichtet, vertrauensunterstützende Komponenten und Funktionen, die u.a. die Rechtskonformität der Services unterstützen, für die Anwender ganzheitlich und transparent bereitzustellen. Zum anderen wurden geeignete Werkzeuge zur Kundeninteraktion entwickelt, um die Innovationsfähigkeit mittelständischer Anbieter zu fördern und darüber hinaus bei der rechtsverträglichen Gestaltung von Cloud-Services zu unterstützen.

1.2 Die Value4Cloud-Projektbausteine

Um die Herausforderungen von **Anwendern** von Cloud-Services und Unternehmen, die eine Anwendung in Erwägung ziehen, zu adressieren, setzt Value4Cloud in vier Kernbereichen an. Erstens benötigen Anwender für ihre Entscheidung bzgl. eines Cloud-Dienstes strukturierte Informationen über Angebote am Markt. Dazu entwickelt das Projekt Empfehlungen für eine Servicebeschreibung, mit der Cloud-Services leichter vergleichbar werden. Eine Kategorisierung der Dienste und Fallstudien erleichtern zusätzlich den Überblick. Zweitens entwickelt das Projekt ein auf der Servicebeschreibung aufbauendes Schema zur Bewertung der Servicequalität nach einheitlichen Kriterien, in dem wichtige Diensteigenschaften wie Leistungsumfang, Rechtskonformität und technische Eigenschaften strukturiert und vergleichbar wer-

den. Ergänzend wird eine Systematik zur Bewertung von Cloud-Services durch Anwender im Anschluss an eine gewisse Nutzungsphase evaluiert und weiterentwickelt. Drittens entwickelt das Projekt ein Werkzeug, um den Vergleich von Cloud-Services anhand der identifizierten Qualitätskriterien zu erleichtern (Benchmarking). Viertens werden vertrauensunterstützende Mehrwertdienste für mehr Transparenz in der Beschaffung, Auswahl und Nutzung entworfen.

Auf der anderen Seite wird es, ob der so geschaffenen Transparenz und Vergleichbarkeit, für Cloud-**Anbieter** noch wichtiger, marktgerechte Angebote zu schaffen, die den Anforderungen der Kunden an Qualität, Vertrauenswürdigkeit und Verlässlichkeit genügen. Cloud-Anwender erwarten von Cloud-Anbietern einerseits eine kostengünstige und effiziente Bereitstellung. Andererseits fordern sie jedoch auch kundenspezifische Innovationen. Value4Cloud unterstützt Cloud-Anbieter dabei, diesen Zielkonflikt zu meistern. Unterstützung von Cloud-Anbietern erfolgt hinsichtlich der rechtsverträglichen Gestaltung und innovativen Weiterentwicklung (Open-Innovation) von Cloud-Diensten. Darüber hinaus wird die Rechtsverträglichkeit neuer Angebote durch Leitfäden zur rechtskonformen Servicegestaltung adressiert. Diese beziehen sich etwa auf Fragen des Datenschutzes, des IT-Strafrechts und der Haftung. Ergänzend wird, drittens, ein Rahmenwerk zur Zertifizierung von Cloud-Services erarbeitet, das es Cloud-Anbietern erleichtert, passende Zertifizierungen zu identifizieren.

Abbildung 1 zeigt die vier Value4Cloud-Projektbausteine mit Anwender-Fokus sowie die drei Bausteine mit Anbieter-Fokus in der Übersicht.

Die in diesem Abschlussband vorgestellten Ergebnisse des Projekts Value4Cloud werden in den nachfolgenden Abschnitten weiter erläutert. Sie befördern den Markt für Cloud-Services, indem Service-Anwender insbesondere bei Aktivitäten der Servicebeschaffung und Service-Anbieter insbesondere hinsichtlich der Ausgestaltung und Vermarktung ihrer Leistungsangebote unterstützt werden. So können am Markt vorherrschende Informationsasymmetrien zwischen Anwender und Anbieter abgebaut, die Transparenz gestärkt und wohlinformierte Entscheidungen der am Markt agierenden Unternehmen hinsichtlich des Bereitstellungsmodells Cloud-Service gefördert werden.

Abbildung 1: Die Value4Cloud-Dienste in der Übersicht

1.2.1 Bedarfsspezifikation und Servicebeschreibung

Ziel dieses Bausteins im Projekt Value4Cloud ist es insbesondere, potenzielle Anwender von Cloud-Services beim Prozess der Anbieter- und Service-Auswahl zu unterstützen. Aufbauend auf der Unified Service Description Language – USDL, einer Vielzahl von Quellen in der wissenschaftlichen Fachliteratur und dem Feedback von Experten aus der Unternehmenspraxis wurde ein Katalog von Merkmalen abgeleitet. Dieser Katalog wurde im Projekt weiter geschärft und fokussiert die aus Anwendersicht entscheidenden Serviceeigenschaften. Er wird vom Konsortialführer des Projekts Value4Cloud als Zeitschrift unter dem Titel „CloudServiceCheck“ (ISSN 2197-5299) herausgegeben, um den sich ändernden Anforderungen an Cloud-Services in der Unternehmenspraxis in neuen Ausgaben gerecht zu werden. Abgerundet wird der Lösungsbaustein durch die enge Verknüpfung mit den Ergebnissen der anderen Projekte und ergänzenden White Papern. Die folgenden Beiträge in diesem Buch vertiefen die in diesem Projektbaustein adressierten Herausforderungen sowie die erzielten Ergebnisse: Kapitel 4, 9, 10, 11, 19 und 24.

1.2.2 Qualitätsbewertung und Benchmarking

Ziel dieses Projektbausteins ist eine möglichst strukturierte Bewertung der Qualität von Cloud-Services, sowohl zum Zeitpunkt der Beschaffung, wie auch zu beliebigen Zeitpunkten einer sich anschließenden Nutzungsphase. Der Lösungsansatz umfasst ein Set von Kriterien zur Bewertung der von Anwendern wahrgenommenen Qualität von Cloud-Services auf Basis der wissenschaftlichen Literatur, das an die Bedürfnisse des deutschen Mittelstandes

im Projektverlauf angepasst wurde. Ebenfalls wurde ein Bewertungsprozess entwickelt und prototypisch implementiert, der es ermöglicht, alle relevanten Akteure in die Qualitätsbewertung einzubinden. Dieser Prototyp konnte bereits während der Projektlaufzeit in Workshops des Projekts Value4Cloud mit Cloud-Anwendern eingesetzt und iterativ weiterentwickelt werden. Die folgenden Beiträge in diesem Buch vertiefen die in diesem Projektbaustein adressierten Herausforderungen sowie die erzielten Ergebnisse: Kapitel 4, 9, 10, 11, 19 und 24.

1.2.3 Vertrauensentwicklung in Cloud-Services und Serviceanbieter

Ziel dieses Bausteins ist die Entwicklung von Diensten und Werkzeugen, die eine Vertrauensentwicklung in der Anbahnungsphase einer Transaktion systematisch ermöglichen. Durch Kommunikation und Signalling-Komponenten wird bspw. Vertrauen in den Transaktionspartner sowie den Cloud-Computing-Service geschaffen und somit die Akzeptanz von Cloud-Computing gesteigert. Der Lösungsansatz umfasst jedoch nicht nur, einige vertrauensfördernde Mehrwertdienste zu konzipieren und zu evaluieren. Da Vertrauen sehr situationsabhängig ist (Söllner/Leimeister 2010), kann davon ausgegangen werden, dass auch nach Projektende neue Situationen zu beobachten sein werden, für die neue vertrauensfördernde Mehrwertdienste entwickelt werden müssen. Daher ist es Teil des Lösungsansatzes, möglichst allgemeingültige Lösungsschablonen zu generieren, mit Hilfe derer auf die jeweilige Situation angepasste vertrauensfördernde Mehrwertdienste entwickelt werden können. Die folgenden Beiträge in diesem Buch vertiefen die in diesem Projektbaustein adressierten Herausforderungen sowie die erzielten Ergebnisse: Kapitel 6, 13 und 21.

1.2.4 Kundenorientierte Weiterentwicklung – Open Innovation

Ziel dieses Bausteins im Projekt Value4Cloud ist die betreuende Unterstützung von Innovationsaktivitäten im gesamten Cloud-Service-Ökosystem. In diesem Zusammenhang wird das Konzept der Open Innovation verfolgt, das die Einbindung der verschiedenen Stakeholder im Cloud-Computing-Ökosystem nicht nur erlaubt, sondern gezielt vorantreibt. Dabei können z.B. Infrastruktur- und Hardwareanbieter, Plattformanbieter, IT-Dienstleistungs-

anbieter, Dienstleistungsbroker und Kunden zu den einzubindenden Stakeholdern des Cloud-Computing-Ökosystems gezählt werden. Der Lösungsansatz umfasst die Entwicklung entsprechender Werkzeuge, um Kunden, externe Partner und Lieferanten als Innovationsquelle für neue Cloud-Services in den Innovationsprozess eines Cloud-Anbieters zu integrieren. Darauf aufbauend werden für die Stakeholder des Cloud-Computing Ökosystems nach Werkzeugen und Methoden gesucht, die beim Heben der identifizierten Integrationspotenziale im Rahmen der Innovationsentwicklung unterstützen, bspw. eine Online Community und Ideenwettbewerbe. Die folgenden Beiträge in diesem Buch vertiefen die in diesem Projektbaustein adressierten Herausforderungen sowie die erzielten Ergebnisse: Kapitel 7, 14, 22 und 25.

1.2.5 Rechtskonforme Bereitstellung und Nutzung

Ziel dieses Projektbausteins ist es, die rechtlichen Anforderungen zu analysieren und Gestaltungsvorschläge für rechtskonforme Cloud-Services zu entwickeln. Der Lösungsansatz umfasst die rechtskonforme Gestaltung von Cloud-Services für den Mittelstand unter besonderer Berücksichtigung des Daten- und Geheimnisschutzes, vertraglicher Aspekte und strafrechtlicher Risiken. Abgerundet wird der Baustein durch die Analyse staatlicher Zugriffe auf Clouds und sich daraus ergebende Anforderungen für Anbieter und Anwender von Cloud-Services. Die folgenden Beiträge in diesem Buch vertiefen die in diesem Projektbaustein adressierten Herausforderungen sowie die erzielten Ergebnisse: Kapitel 8, 15, 16, 17, 18 und 23.

1.2.6 Zertifizierung von Cloud-Services

Zertifizierungen von Cloud-Services können Entscheidungsträger bei der Auswahlentscheidung unterstützen, Transparenz am Markt schaffen, Vertrauen und Akzeptanz auf der Anwenderseite erhöhen sowie es Cloud-Anbietern ermöglichen, ihre Systeme und Prozesse zu überprüfen und zu verbessern (Sunyaev/Schneider 2013). Ziel dieses Projektbausteins ist es zunächst, eine Übersicht über die am Markt vorhandenen Zertifikate zu gewinnen und ein Rahmenwerk daraus zu entwickeln. Im Anschluss werden dann Empfehlungen zur Gestaltung von Cloud-Service-Zertifizierungen entwickelt. Diese Zertifikate berücksichtigen nicht nur die ebenfalls im Pro-

jekt Value4Cloud eruierten Qualitätsdimensionen von Cloud-Services (siehe Kapitel 2), sondern wurden auch unter Berücksichtigung der Methodenkompetenzen des Valuepartners SQS AG im Bereich der Bewertung von Software- und Dienstleistungsqualität entwickelt. So konnten praxisrelevante und marktnahe Ergebnisse sichergestellt werden. Die folgenden Beiträge in diesem Buch vertiefen die in diesem Projektbaustein adressierten Herausforderungen sowie die erzielten Ergebnisse: Kapitel 5, 12 und 20.

1.3 Vorgehen und Partner für den nachhaltigen Transfer der Ergebnisse

Die gewonnenen Ergebnisse wurden kontinuierlich in Workshops mit Teilnehmern aus der Unternehmenspraxis pilotiert und diskutiert. Durch diesen regelmäßigen Erfahrungsaustausch, die Integration von Zwischenergebnissen in die Workshops, aber auch deren Publikation auf der Webseite des Projekts Value4Cloud sowie insbesondere durch den Austausch auf wissenschaftlichen Konferenzen wurde die Fokussierung, aber auch die Verallgemeinerbarkeit der Projektergebnisse gewährleistet. Zusätzlich wurden wesentliche Einzelergebnisse des Projekts so aufbereitet, dass sie besonders auf die Herausforderungen kleiner Unternehmen und deren Bedürfnisse abgestimmt sind. Entstandene White Paper und Werkzeuge werden zum einen über die Webseite des Projekts zum Download angeboten (www.Value4Cloud.de), fließen jedoch insbesondere in das auch nach Projektende vom Projektkonsortium offerierte Angebot an Workshops ein (siehe hierzu auch Teil G dieses Buches). Auf diese Weise werden neben der Webseite weitere Kanäle genutzt, um einen breitenwirksamen und nachhaltigen Transfer der im Projekt entstandenen Ergebnisse in die Unternehmen des deutschen Mittelstands sicherzustellen.

Durch die Einbindung einer Vielzahl von Unternehmensvertretern bereits während der Projektlaufzeit konnten praktikable Ergebnisse insbesondere für mittelständische Unternehmen sichergestellt und durch praxisnahe Erprobung nachgewiesen werden. Zu diesem Zweck wurden im Projekt bereits Zwischenergebnisse aufbereitet und auf Veranstaltungen von Verbänden wie VOICE, BITKOM oder BiccNet präsentiert und mit den teilnehmenden Fachvertretern von Unternehmen diskutiert. Auch auf Messen wie der Cebit

und in selbst ausgerichteten Workshops zu Schwerpunktthemen des Projekts Value4Cloud wurde der Austausch und die Diskussion gesucht und einzelne Aspekte im Dialog mit Unternehmensvertretern besprochen. So konnten die im Zeitverlauf erarbeiteten Konzepte, Methoden, Modelle und Werkzeuge zur Förderung von Vertrauen, Rechtsverträglichkeit, Qualität und Nutzung von Cloud-Services bereits während der Projektlaufzeit zeitnah an die Praxis mittelständischer Unternehmen angepasst und durch die Kommunikation breitenwirksam überführt werden. Publikationen des Projekts Value4Cloud im Rahmen einer Vielzahl von wissenschaftlichen Konferenz- und Zeitschriftenbeiträgen, Pressemitteilungen, die seit 2013 regelmäßig erscheinende Zeitschrift CloudServiceCheck sowie begleitende Artikel zu einzelnen Projektergebnissen in der Fachpresse haben hierzu ebenso beigetragen (für eine umfassende Übersicht: siehe Publikationsübersicht im Anhang dieses Buches). Darüber hinaus haben erste Zwischenergebnisse auch bereits Eingang in die universitäre Lehre der Technischen Universität München, der Universität Kassel und der Universität zu Köln gefunden.

1.3.1 Das Vorgehen

Die Entwicklung der Projektergebnisse im Projekt Value4Cloud erfolgte zu großen Teilen iterativ. Die im Rahmen des Projektes entstandenen Ergebnisse konnten durch dieses Vorgehen bereits während ihrer Entwicklung, im Entwurfs- oder Prototypstatus, in unterschiedlichen Szenarien mit Anwendern und Anbietern aus dem deutschen Mittelstand pilotiert und diskutiert werden. Im nächsten Schritt erfolgte eine Aktualisierung der Ergebnisse sowie zum Teil weitere prototypische Implementierungen und Feldtests. Dem iterativen Entwicklungsmodell folgend, flossen die Ergebnisse dieser Tests in die Weiterentwicklung der Methoden und Instrumente kontinuierlich ein und stellten so die praxisorientierte Entwicklung in mehreren Schritten sicher. In die Pilottests und Workshops wurden nicht nur alle geförderten Partner des Projekts Value4Cloud einbezogen, sondern auch weitere Unternehmen, die Interesse am Thema äußerten. [Abbildung 2](#) skizziert die Arbeitspakete des Projekts im Zeitverlauf, deren inhaltliche Ausrichtungsschwerpunkte sowie die sechs gleichverteilte Meilensteine im Projektverlauf.

Abbildung 2: Arbeitspakete und Meilensteine

1.3.2 Die Projektpartner

Unter der Konsortialführung der fortiss GmbH – An-Institut der Technischen Universität München – wurde das Projekt Value4Cloud gemeinsam mit vier weiteren, geförderten Partner durchgeführt – der Universität Kassel, der Universität zu Köln, der SpaceNet AG und gate, dem Garchinger Technologie und Gründerzentrum GmbH. Die im Projekt tätigen Mitarbeiter dieser fünf Partner haben teils differierende Perspektiven und unterschiedliche Expertise in das Projekt eingebracht und so dazu beigetragen, die Ergebnisse aus unterschiedlichen Blickwinkeln zu beleuchten und weiterzuentwickeln. Die Einbindung weiterer Experten, über das geförderte Projektkonsortium hinaus, erfolgte während des gesamten Projektverlaufs, jedoch insbesondere zur Evaluation und Diskussion von Zwischen- und Abschlussergebnissen. Zielsetzung dieser kontinuierlichen Einbindung ergänzender Expertise war es, Projektergebnisse zu schaffen, die sich durch Praxisrelevanz und Praktikabilität für Unternehmen des deutschen Mittelstands auszeichnen. Hierbei erwiesen sich die iterative Weiterentwicklung der Projektergebnisse und die frühzeitige Diskussion von Zwischenergebnissen als zentrale Elemente. Durch die regelmäßigen, gemeinsamen Diskussionen im Team der geförderten Projektpartner und zahlreiche Rückmeldungen und Erfahrungswerte der

darüber hinaus eingebundenen Experten wurde eine stete Verbesserung der Projektergebnisse erst möglich.

1.4 Aufbau dieses Abschlussbandes

In diesem Abschlussband werden nachfolgend die Ergebnisse des Projekts Value4Cloud zusammenfassend dargestellt. Im Anschluss an diesen einleitenden Beitrag folgen in **Teil B** dieses Buches zunächst Beiträge zu der Erläuterung der Ausgangslage beim Start des Projekts Value4Cloud, der definitorischen Abgrenzung von Begriffen sowie einer Analyse des Cloud-Service-Marktes und der sich etablierenden Wertschöpfungsstrukturen. Aufbauend auf dieser definitorischen wie analytischen Basis folgt in **Teil C** die Aufarbeitung des vorherrschenden Unterstützungsbedarfs aus der Sicht Cloud-nutzender Unternehmen, gefolgt von der Aufarbeitung des Unterstützungsbedarfs von Cloud-Anbietern in **Teil D**.

Die Beiträge in Abschnitt fünf fokussieren die Beschreibung der erzielten Projektergebnisse. Diese sind darauf ausgelegt, den zuvor erarbeiteten Unterstützungsbedarf passgenau zu adressieren. Mögliche Einsatzszenarien der entwickelten Ergebnisse in der Unternehmenspraxis folgen in **Teil E**. Der Fokus dieses Abschnitts liegt entsprechend auf dem Wissenstransfer, der praktischen Anwendbarkeit der Ergebnisse und der Analyse der durch die entwickelten Werkzeuge erzielten Marktunterstützung. **Teil F** schließt dieses Buch mit einem Beitrag zu nachhaltigen Geschäftsmodellen für die im Projekt entwickelten marktunterstützenden Dienstleistungen ab. Das entwickelte Workshop-Modell stellt sicher, dass die im Projekt entstandenen Ergebnisse auch über die Laufzeit des Projektes hinaus in einer ansprechenden Form dem deutschen Mittelstand bereitgestellt werden können und eine Weiterentwicklung der Ergebnisse im Dialog mit der Unternehmenspraxis sichergestellt ist.¹

1 Für die folgenden Ausführungen gilt, dass diese lediglich eine Momentaufnahme darstellen können und, wie immer bei solchen Untersuchungen, der aktuelle Stand der Technik zu beachten ist.

1.5 Literaturverzeichnis

- Golkowsky, C.; Vehlow, M. (2011):** Cloud Computing im Mittelstand – Erfahrungen, Nutzen und Herausforderungen, PwC, Frankfurt am Main, Deutschland 2011.
- Krcmar, H.; Leimeister, S. (2010):** CIO-Umfrage 2010 – Selbstverständnis und Themenschwerpunkte der IT-Entscheider im Jahr 2010. Technische Universität München – Lehrstuhl für Wirtschaftsinformatik, München, Deutschland 2010.
- Söllner, M.; Leimeister, J.M. (2010):** Did they all get it wrong? Towards a better measurement model of trust. Präsentiert auf der Academy of Management Annual Meeting 2010, Montréal, Kanada.
- Sunyaev, A.; Schneider, S. (2013):** Cloud Services Certification. In: Communications of the ACM, Vol. 56 (2013) No. 2, S. 33–36.

Teil B:
**Der Markt für Cloud-
Computing-Services**

2 Ausgangslage und Definitorisches

*L. Gebauer, M. Kunz, P. Hoberg, S. Kroschwald, A. Reidt, S. Schneider,
M. Wicker, J. Wollersheim*

2.1 Cloud-Computing

„The rise of the cloud is more than just another platform shift that gets geeks excited. It will undoubtedly transform the IT industry, but it will also profoundly change the way people work and companies operate. It will allow digital technology to penetrate every nook and cranny of the economy and of society, creating some tricky political problems along the way.” (The Economist, 23. Oct. 2008).

Der vorliegende Beitrag dient dazu, ein gemeinsames Verständnis der verwendeten Begrifflichkeiten zum Cloud-Computing zu schaffen. In den nachfolgenden Beiträgen dieses Sammelbandes werden anschließend Cloud-Services und ihre Bereitstellungsmodelle näher betrachtet werden. Hierauf aufbauend widmen sich dann die folgenden Beiträge den Bestandteilen des interdisziplinären Forschungsprojekts Value4Cloud – ausgehend von einer Beschreibung des notwendigen Unterstützungsbedarfs in der Unternehmenspraxis, der dieses Projekt motiviert hat, bis hin zu den im Projekt entwickelten Lösungsbausteinen und ihrer Anwendung.

Bei der Abwägung von Vorteilen und Risiken unterschiedlicher Betriebs- und Bereitstellungsmodelle zur Deckung des Bedarfs an Informations- und Kommunikationsleistungen haben die meisten Unternehmen bislang den dedizierten, also eigenständigen und nur auf einen bestimmten Zweck ausgerichteten, (Eigen-)Betrieb bestimmter Informations- und Kommunikationssysteme (IuK-Systeme), wie z.B. Buchhaltungssoftware, Software für die Produktionsprogrammplanung oder Server für die Datenhaltung, aus Sicherheits- und wettbewerblichen Gründen für notwendig erachtet. Nachfrageschwankungen, die Vielfältigkeit der Kundenanforderungen und eine geringer werdende Produktlebensdauer erfordern jedoch von Unternehmen die Fähigkeit zur flexiblen Anpassung ihrer meist hoch komplexen IuK-Systeme, um auf Veränderungen schnell und effizient reagieren zu können. Häufig ist dies mit erheblichen Investitionen in IuK-Systeme und hohen Fixkosten für deren Betrieb und Wartung verbunden. Hieraus ist der Wunsch vieler Unternehmen entstanden, den Investitionsaufwand zu reduzieren und Fixkosten zu

variabilisieren. Es soll abhängig von der tatsächlichen Nutzung nur für das bezahlt werden, was auch gebraucht wird. Da viele der benötigten IuK-Systeme als Commodity, d.h. als Standard, wahrgenommen werden, wurde aus der Frage, was an Systemen benötigt wird, die Frage, in welcher Form und von wem die von den Systemen bereitgestellte Leistung in Zukunft zur Verfügung gestellt werden soll. Cloud-Computing hat sich als eine mögliche Antwort auf diese Frage entwickelt.

Wie das einleitende Zitat bereits verdeutlicht, ist Cloud-Computing keine neue Technik. Cloud-Computing ist ein neues Bereitstellungsmodell für IuK-Systeme, auf das Unternehmen zur teil- oder vollautomatisierten Unterstützung ihrer Prozesse zurückgreifen können. Böhm et al. (2009, S. 8) führen aus: „Cloud-Computing ist ein auf Virtualisierung basierendes IT-Bereitstellungsmodell, bei dem Ressourcen sowohl in Form von Infrastruktur als auch Anwendungen und Daten als verteilter Service über das Internet durch einen oder mehrere Leistungserbringer bereitgestellt werden. Diese Services sind nach Bedarf flexibel skalierbar und können verbrauchsabhängig abgerechnet werden“. Cloud-Computing verbindet bekannte Techniken, wie Grid Computing, SOA (Service-Orientierte Architektur) und Virtualisierung (Youseff et al. 2008, S. 1), mit geschäftsorientierten Gestaltungsansätzen, wie etwa der Leistungstiefengestaltung im Bereich der IT eines Unternehmens (IT-Outsourcing), und geht einher mit einer kontinuierlichen Entflechtung traditioneller Wertschöpfungsketten (Böhm et al. 2009, S. 8ff.).

Auch der jüngeren Begriffsdefinition durch das National Institute for Standards and Technology (NIST) liegt dieses sowohl technisch als auch betriebswirtschaftlich motivierte Verständnis zugrunde. Das NIST bezeichnet Cloud-Computing als „[...] a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction“ (NIST 2011, S. 2). Cloud-Services stellen demzufolge eine Ansammlung leicht nutzbarer und zugreifbarer Ressourcen (wie Anwendungssoftware, Entwicklungsplattformen oder Hardware) dar. Diese Ressourcen können dynamisch, ohne größeren Aufwand und mit minimaler Interaktion mit dem Dienstleister an eine variable Last angepasst und ent-

Tabelle 1: Cloud-Service-Charakteristika (In Anlehnung an NIST 2011, S. 2)

Cloud-Service-Charakteristika	
On demand self-Service	Ein Anwender kann Cloud-Services unilateral beschaffen, so wie er sie benötigt, etwa Rechenkapazität, Netzwerkspeicher oder Software-Anwendungen, automatisch und ohne menschliche Interaktion mit jedem Cloud-Anbieter.
Netzwerk-zugriff	Cloud-Services werden über ein Netzwerk bereitgestellt. Der Zugriff erfolgt über vereinheitlichte Mechanismen, etwa Webseiten oder technisch aufwendigere Schnittstellen.
Ressourcen-bündelung	Die für die Bereitstellung eines Cloud-Services benötigten Ressourcen sind gebündelt und werden mit Hilfe eines mandantenfähigen Systems von mehreren Cloud-Anwendern gleichzeitig verwendet. Abhängig vom jeweiligen Bedarf werden einem Cloud-Anwender dabei Ressourcen zugewiesen oder entzogen.
Skalierbarkeit / Elastizität	Cloud-Services können schnell und flexibel bereitgestellt werden. Für den Cloud-Anwender erscheinen die ihm zur Verfügung gestellten Ressourcen unendlich und können zu jeder Zeit in jeder Menge abgerufen werden.
Messbarkeit	Zur Information für Cloud-Anbieter und Cloud-Anwender wird die Ressourcennutzung überwacht, gemessen und darüber in einem angemessenen Abstraktionsgrad berichtet.

sprechend rekonfiguriert werden. Dem Cloud-Anbieter wird somit eine optimale Ressourcenauslastung ermöglicht, da sich die Lastschwankungen seiner Kunden etwas ausgleichen und durch Skaleneffekte ein effizienterer Betrieb ermöglicht wird.

Der Definition des NIST (2011) folgend, weisen IT-Dienstleistungen, die in Form von Cloud-Computing bereitgestellt werden, die in [Tabelle 1](#) aufgeführten, charakteristischen Eigenschaften auf.

Die Eigenschaften von Cloud-Computing und die sich daraus ergebenden Vor- und Nachteile werden kontrovers diskutiert. So findet Cloud-Computing in der deutschen Öffentlichkeit und unter Fachvertretern von Unternehmen ein geteiltes Echo. Einer Befragung zufolge stehen immer mehr Unternehmen in Deutschland dem Thema Cloud-Computing aufgeschlossen und interessiert gegenüber, wobei gleichzeitig der Anteil der Skeptiker zu-

nimmt (KPMG 2013). Um diese auf den ersten Blick schwer miteinander zu vereinbarenden Ergebnisse näher zu beleuchten und Widersprüche aufzulösen, bedarf es zunächst einer weiteren Begriffsdifferenzierung und Abgrenzung des Bereitstellungsmodells Cloud-Computing und seiner Ausprägungsformen.

2.2 Cloud-Services und ihre Bereitstellungsmodelle

Entsprechend der Dienstleistungstypologie nach Leimeister (2012, S. 27) ist Cloud-Computing eine elektronische Dienstleistung, die sich durch einen hohen IT-Einsatz auszeichnet. Diese Dienstleistung kann dabei sowohl als reine IT-Dienstleistung ohne Personaleinsatz als auch als IT-unterstützte Dienstleistung angeboten werden, bei der neben der Technik auch Personal eingesetzt wird, um eine Leistung zu erbringen. Diese beiden Typen Cloud-basierter Dienstleistungen werden im Nachfolgenden stets als „Cloud-Services“ zusammengefasst, da es im Einzelfall schwer festzustellen ist, ob der Cloud-Anbieter für die Bereitstellung neben technischen Ressourcen auch Personal einsetzt. Ausschlaggebend für die Qualifizierung einer IT-Dienstleistung als Cloud-Service ist demnach nicht die Form der Leistungserbringung (z.B. die technische und organisatorische Umsetzung der Leistungserstellung), sondern die Form der Bereitstellung der IT-Dienstleistung (siehe [Tabelle 1](#)).

Aus Sicht des Leistungsanbieters und auch seiner Kunden dient die Bereitstellung von IT-Ressourcen in Form eines Cloud-Services gleichermaßen der Komplexitäts- sowie der Kostenreduktion. Ein Cloud-Service bezeichnet somit, wie jede Dienstleistung, ein intangibles Gut, dessen Erzeugung durch die Integration eines externen Faktors in den Leistungserstellungsprozess gekennzeichnet ist, der durch diesen Faktor angestoßen wird.

Cloud-Services lassen sich anhand der durch sie bereitgestellten Funktionalität grob einer von drei Klassen zuordnen: Software-Services, Plattform-Services und Infrastruktur-Services. In Literatur und Praxis wird auch von drei Service-Modellen gesprochen, deren Bezeichnungen auf die besondere Form der Bereitstellung der Services abstellen. So werden die Modelle Software-as-a-Service (SaaS), Plattform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS) unterschieden.

Eine als Cloud-Service bereitgestellte Anwendungssoftware (SaaS) stellt dem Anwender die Funktionalität einer vollwertigen Applikation zur Verfügung (Durkee 2010). Services der Plattformebene (PaaS) ermöglichen es dem Cloud-Anwender, mit Hilfe der vom Cloud-Anbieter zur Verfügung gestellten Laufzeit- und Programmierungsumgebungen zugekaufte oder selbst erstellte Applikationen in der Cloud auszuführen (NIST 2011). Auf der Infrastrukturebene (IaaS) werden dem Kunden laut NIST-Definition Rechen-, Speicher-, Netzwerk- und andere IT-Basisressourcen zur Verfügung gestellt.

Vom Service-Modell ist das Bereitstellungsmodell zu unterscheiden. Im Hinblick auf die Art des Bezugs von Cloud-Services wird zwischen verschiedenen Bereitstellungsmodellen und diversen Mischformen unterschieden. Die häufigsten Formen sind die Private Cloud und die Public Cloud. Der Definition des BITKOM (2010) folgend stellen **Private Clouds** eine Form der Bereitstellung von IT-Services exklusiv für einen vorab festgelegten Anwenderkreis dar. Sie bezeichnen zumeist unternehmensinterne Rechenzentren, die nicht über ein verbrauchsabhängiges Abrechnungsmodell der Öffentlichkeit zugänglich gemacht werden (Armbrust et al. 2009). „Management und Betrieb werden innerhalb eines Unternehmens oder einer gemeinsamen Organisation abgewickelt. Der Zugang zum Service ist somit per Definition beschränkt auf von dem Betreiber autorisierte Personen innerhalb eines definierten Anwenderkreises und erfolgt in der Regel über ein Intranet oder ein Virtual Private Network (VPN)“ (BITKOM 2010, S. 18).

Die Anwender einer **Public Cloud** sind demgegenüber nicht zwingend rechtlich oder partnerschaftlich miteinander verbunden (BITKOM 2010). Services aus der Public Cloud stehen jedem interessierten Anwenderunternehmen am Markt zur Verfügung. Unterschiedliche, zum Teil untereinander im Wettbewerb stehende Anwenderunternehmen teilen sich die vom Cloud-Anbieter bereitgestellten Ressourcen. Die Möglichkeit der exakten Zuordnung der von einem Cloud-Anwender tatsächlich genutzten Cloud-Ressourcen im Pool des Cloud-Anbieters wird dabei jedoch nicht angestrebt; die Daten der Anwender werden voneinander isoliert, aber physische Ressourcen des Anbieters wie Server oder Speicherplatten werden gemeinsam genutzt (BITKOM 2010). Public Clouds werden zumeist von IT-Dienstleistern für eine Vielzahl unterschiedlicher Kunden betrieben, wobei sich der Anbieter

gegenüber seinen Kunden in keiner besonderen rechtlichen oder wirtschaftlichen Abhängigkeit befindet, die die wirtschaftliche Entscheidungsfreiheit maßgeblich einschränken würde.

Ein Vorteil des **Private-Cloud**-Modells ist, dass eine IT-Betriebsumgebung unter Kontrolle des Cloud-Anwenders innerhalb der Unternehmens-Firewall genutzt werden kann (BITKOM 2010). Potenzielle Sicherheitsbedenken hinsichtlich der gemeinsamen Nutzung von Ressourcen mit anderen, im Wettbewerb stehenden Unternehmen entfallen. Zudem können die Serviceangebote der Private Cloud individuell auf die Anforderungen des nutzenden Unternehmens angepasst werden (funktionale Eigenschaften ebenso wie etwa Update-Zyklen), denn im Gegensatz zu Services aus der Public Cloud müssen Private-Cloud-Services nicht einer Vielzahl unterschiedlicher Kundenanforderungen gerecht werden. Demgegenüber besteht jedoch der Nachteil, dass mit einer ‚Private Cloud‘ Größendegressionseffekte nur bedingt realisiert werden können.

Die Nutzungsanteile beider Bereitstellungsmodelle durch Unternehmen unterscheiden sich in Deutschland erheblich, wie eine Analyse aus dem Jahr 2012 zeigt (KPMG 2013). So nutzten 2012 bereits 34 % der befragten Unternehmen das Modell „Private Cloud“, während das Modell „Public Cloud“ lediglich von 10 % der befragten Unternehmen in Anspruch genommen wurde. Ähnlich geringe Nutzungszahlen des Modells Public Cloud auf dem deutschen Markt errechnete auch der Branchenverband BITKOM. Laut BITKOM greifen lediglich 6 % der deutschen Unternehmen auf Services aus der Public Cloud zurück (Kempf 2012).

2.3 Herausforderungen für Cloud-Anwender und Cloud-Anbieter

Die Gründe für die geringe Nutzungsrate von Public-Cloud-Services sind vielfältig und reichen von technischen, betriebswirtschaftlichen und rechtlichen Unsicherheiten, über mangelndes Vertrauen in die Sicherheit der ausgelagerten Daten, bis hin zur Angst, sich zu stark an einen Cloud-Anbieter zu binden (Krcmar/Leimeister 2010). Krcmar und Leimeister (2010) zufolge bestehen aus Cloud-Anwendersicht vor allem Zweifel hinsichtlich der Zuverlässigkeit der Cloud-Services, der tatsächlich realisierbaren Vorteile, aber

auch hinsichtlich der Rechtskonformität vor allem im Hinblick auf die Datensicherheit und den Datenschutz. Die Komplexität der Thematik, die mangelnde Erfahrung mit konkreten Anwendungs- und Einsatzszenarien und das Fehlen von praxisnahen Leitfäden für die Auswahl, die Einführung und die Nutzung von Cloud-Services erschweren die Verbreitung von Cloud-Computing, insbesondere im deutschen Mittelstand (Golkowsky/Vehlow 2011, S. 29).

Um die Akzeptanz von Cloud-Computing bei Unternehmen unterschiedlicher Größe und folglich die Cloud-Anwenderzahlen signifikant zu erhöhen, gilt es, diese genannten Herausforderungen zu adressieren und wahrgenommene Hürden zu reduzieren. Daher ist das Ziel des interdisziplinären Forschungsprojektes Value4Cloud die Erforschung und Einwicklung marktunterstützender Mehrwertdienste zur Förderung von Vertrauen, Rechtsverträglichkeit, Qualität und Nutzung von Cloud-Services, insbesondere für den Mittelstand. Ein Mehrwertdienst bezeichnet dabei einen Dienst, der „zusätzlich zum Kern-Service angeboten wird und wertsteigernd wirkt“ (Leimeister 2012, S. 424). Marktunterstützende Mehrwertdienste für Cloud-Services dienen dementsprechend dem verbesserten Handel mit den Marktakteuren oder dem erleichterten Austausch von Cloud-Services zwischen diesen. Beispiele sind etwa Dienste und Werkzeuge, die potenzielle Kunden von Cloud-Services dabei unterstützen, ihren Beschaffungsprozess zu strukturieren oder Vertrauen in den Anbieter zu erlangen. Projektergebnisse richten sich jedoch ebenso an die Anbieter von Cloud-Services und unterstützen diese bspw. bei der rechtsverträglichen Gestaltung ihrer Leistungen oder der innovativen Weiterentwicklung ihres Leistungsangebots. Value4Cloud unterstützt somit sowohl Anbieter als auch Anwender bei der Bewältigung der bestehenden Herausforderungen.

Die nachfolgenden Abschnitte erläutern zunächst die Herausforderungen für Unternehmen, die Cloud-Service anwenden möchten, gefolgt von den Herausforderungen für Anbieterunternehmen. Die genannten Aspekte werden im Verlauf dieses Buches vertiefend thematisiert und erläutert.

2.3.1 Spezifikation des Service-Bedarfs

Die Marketingpraxis der Cloud-Anbieter sowie die Vielzahl neuer, unbekannter Cloud-Services erschweren es potenziellen Kunden, den Überblick über den Cloud-Markt zu behalten und für sie geeignete Services zu identifizieren. Darüber hinaus erfordern die Eigenschaften von Cloud-Services wie bspw. das Self-Service-Prinzip auch Veränderungen in der IT-Beschaffungspraxis von Anwender-Unternehmen. Traditionelle Beschaffungsverfahren für individualisierte Dienstleistungen (etwa IT-Outsourcing) sind ebenso wenig anwendbar, wie traditionelle Beschaffungsverfahren für vollständig standardisierte IT-Produkte (etwa PCs, Drucker, Office-Software). Aufgrund der Self-Service-Eigenschaft von Cloud-Services ist aus Sicht des beschaffenden Unternehmens eine andere Art der Bedarfsspezifikation notwendig. Es reicht nicht, die eigenen Anforderungen zu spezifizieren, es ist notwendig, diese Anforderungen selbstständig mit möglichen Angeboten abzugleichen und ggf. dem Angebot anzupassen, da es sich bei Cloud-Services um standardisierte Dienstleistungen mit nur zum Teil individualisierbaren Eigenschaften handelt.

2.3.2 Bewertung der Service-Qualität

Möchte ein Unternehmen Cloud-Services anwenden, so steht es zum Zeitpunkt der Service-Beschaffung vor der Herausforderung, die Qualität der angebotenen Services wie auch der dahinter stehenden Anbieter im Detail zu beurteilen. Nur so ist dem Unternehmen eine Beurteilung der gebotenen Qualität möglich, was wiederum Voraussetzung für die Aussage ist, ob die gebotene Qualität ausreichen wird, um die eigenen Anforderungen zu bedienen. Aufbauend auf der im vorhergehenden Abschnitt 2.1 beschriebenen Bedarfsspezifikation des beschaffenden Unternehmens kann ein Abgleich der eigenen Anforderungen mit den Leistungsversprechen der Angebote erfolgen.

Qualität bezeichnet dabei den Grad der Anforderungserfüllung durch den Service. Qualität ist somit ein Maß, das sowohl von den eigenen Anforderungen an eine Leistung abhängt, als auch vom Erfüllungsgrad diesbezüglich. Der diesem Verständnis zugrunde liegende Qualitätsbegriff stimmt mit der internationalen Norm ISO 9000 überein, in der Qualität definiert wird als

„Degree to which a set of inherent characteristics fulfils requirements“. Um bei der Bewertung der Service-Qualität keine wichtigen Anforderungen zu übersehen, ist eine strukturierte Vorgehensweise unter Rückgriff auf etablierte Templates und Normungen wie etwa die Norm ISO/IEC 25010 empfehlenswert.

2.3.3 *Vertrauen in der Wirtschaftsinformatik*

Vertrauen ist ein Thema, mit dem sich bereits verschiedenste wissenschaftliche Disziplinen, wie die Philosophie, die Psychologie, die Betriebswirtschaftslehre und die Wirtschaftsinformatik (WI), beschäftigt haben. Da Vertrauen ein sehr facettenreiches Konstrukt ist und jede dieser Disziplinen eine eigene Sichtweise auf Vertrauen einnimmt, hat sich keine einheitliche Definition des Begriffs entwickelt (Wang/Emurian 2005). In der Wirtschaftsinformatik wird Vertrauen definiert als der *„Eindruck des Vertrauensgebers, dass ein bestimmter Vertrauensnehmer ihm in einer Situation, die von Unsicherheit und Verwundbarkeit des Vertrauensgebers charakterisiert ist, dabei behilflich sein wird, seine Ziele zu erreichen“* (Söllner et al. 2012, S. 114). Dementsprechend ist Vertrauen in Situationen vollkommener Sicherheit und einem bekannten Ergebnis nicht notwendig, da weder positive Erwartungen noch Verwundbarkeit bestehen (Söllner et al. 2012). Bei der Übertragung der Definition von Vertrauen auf den Cloud-Computing-Kontext ergibt sich Folgendes: Der Vertrauensgeber, also der Cloud-Computing-Nutzer, lagert geschäftskritische Aufgaben an einen externen Dienstleister aus und verfügt nicht über ausreichende Kontroll- und Überwachungsmöglichkeiten, sodass sich dieser in eine Situation von Unsicherheit und Verwundbarkeit begibt. Dies hat zur Folge, dass der Cloud-Computing-Nutzer nur darauf vertrauen kann, dass der Vertrauensnehmer, also der Cloud-Computing-Anbieter, über ausreichende Kompetenzen und Fähigkeiten verfügt, um den übertragenen Aufgaben und Pflichten zuverlässig nachzukommen.

Zudem untergliedert die WI-Forschung Vertrauen in drei unterschiedliche Komponenten (vgl. Leimeister et al. 2005). Die Vertrauensbereitschaft (im englischen Original: *dispositional trust*) ist die grundsätzliche Bereitschaft anderen zu vertrauen, welche auf den Persönlichkeitsmerkmalen des Vertrau-

Abbildung 1: Die Dreiteilung von Vertrauen in der WI-Forschung (Darstellung in Anlehnung an Leimeister et al. 2005)

ensgebers (Cloud-Computing-Nutzer) beruht. Das interpersonelle Vertrauen (im englischen Original: *interpersonal trust*) ist das Maß an Vertrauen, welches der Vertrauensgeber dem Vertrauensnehmer (Cloud-Computing-Anbieter) entgegenbringt, basierend auf der Beurteilung bestimmter Eigenschaften des Vertrauensnehmers. Im Gegensatz dazu ist das Systemvertrauen (im englischen Original: *system trust*) das Maß an Vertrauen, welches der Vertrauensgeber dem technischen System oder einer Institution entgegenbringt, basierend auf der Beurteilung bestimmter Eigenschaften des technischen Systems bzw. der Institution (siehe [Abbildung 1](#)).

Diese Dreiteilung spielt vor allem im Kontext von Cloud-Computing eine bedeutsame Rolle, da die (potenziellen) Cloud-Computing-Nutzer nicht nur Vertrauen in den Cloud-Computing-Anbieter, sondern auch Vertrauen in die Technik selbst entwickeln müssen (vgl. Gebauer et al. 2012). Dementsprechend müssen im Kontext von Cloud-Computing sowohl das interpersonelle Vertrauen zum Anbieter als auch das Systemvertrauen in die Cloud-Computing-Technik adressiert werden.

2.3.4 Rechtskonforme Bereitstellung und Nutzung von Services

Rechtmäßigkeit meint die Vereinbarkeit von Cloud-Angeboten und die Vereinbarkeit der Cloud-Nutzung mit dem geltenden Recht. Dabei wird zunächst das auf Cloud-Computing anwendbare Recht festgestellt und die darauf folgenden gesetzlichen Anforderungen sowohl für den Cloud-Anbieter als auch für den Cloud-Anwender untersucht. Die Ergebnisse dieser Untersuchung werden sodann mit dem konkreten Cloud-Service abgeglichen. Erfüllt der

Cloud-Service die Anforderungen der Rechtskonformität nicht, ist er oder seine Nutzung so nicht zulässig. Kann ein Cloud-Anbieter oder ein Cloud-Anwender seine rechtlichen Pflichten im Cloud-Kontext nicht erfüllen, muss er auf das Angebot beziehungsweise die Nutzung des Services verzichten.

Über die Rechtmäßigkeit hinaus ist bei der rechtlichen Untersuchung von Cloud-Computing die Rechts- und Verfassungsverträglichkeit zu berücksichtigen. Dabei werden die den Rechtsnormen zugrunde liegenden Ziele der Vorschriften oder gar des Grundgesetzes beleuchtet und daraufhin diejenigen Cloud-Services als rechtlich wünschenswert identifiziert, die diese Ziele am effektivsten gewährleisten. Die Rechtsverträglichkeit geht folglich über die Rechtsanwendung des geltenden Rechts auf Cloud-Computing und damit über die Rechtmäßigkeit hinaus und zielt darauf ab, die Services im Bereich des Cloud-Computing so zu beeinflussen, dass sie möglichst am weitesten mit den Rechtszielen übereinstimmen. Rechts- und Verfassungsverträglichkeit ist damit mehr als nur Rechtmäßigkeit: Sind Cloud-Services rechtsverträglich, sind sie und ihre Inanspruchnahme nicht nur nach den Gesetzen zulässig. Statt die Rechtsvorgaben nur im Sinne einer Minimalzielerfüllung umzusetzen, bereiten rechtsverträgliche Cloud-Services im Hinblick auf die Schutzziele der Verfassung einen möglichst optimalen Schutz der Beteiligten und Betroffenen.

2.3.5 *Innovative Weiterentwicklung von Cloud-Services*

Veränderungen im wirtschaftlichen Umfeld – z.B. durch gestiegenen Wettbewerb und Preisdruck, sich ständig verändernde Kundenbedürfnisse und Marktstrukturen – zwingen Unternehmen dazu, eigene Innovationen schneller und effizienter voranzutreiben als bisher. Eine Möglichkeit bildet dabei die Öffnung des unternehmensinternen Innovationsprozesses nach Außen gegenüber allen relevanten Interessensgruppen, um neue Potenziale erschließen zu können (Leimeister 2012). Sowohl in Praxis als auch Theorie zeigt sich hierbei, dass die wichtigste Interessensgruppe der Kunde ist, welcher über Akzeptanz und Nutzung und somit letztlich über den Erfolg eines Produktes oder einer Dienstleistung maßgeblich entscheidet (Marston et al. 2011; Kunz et al. 2013). Ein solcher Ansatz vermindert das Risiko, dass neu geschaffene Angebote an den Bedürfnissen der Kunden vorbeigehen und somit diese nur

bedingt oder nur unzureichend ansprechen. Die Öffnung des Innovationsprozesses nach Außen wird auch als „Open Innovation“ bezeichnet und beschreibt dabei einen Paradigmenwechsel von der ausschließlichen Entwicklung von Produkten und Dienstleistungen in unternehmenseigenen Forschungs- und Entwicklungsabteilungen (Reichwald et al. 2009). Dabei soll das Wissen sowohl interner als auch externer Quellen in die unternehmerischen Tätigkeiten einbezogen werden (Chesbrough 2006). Nach Reichwald et al. (2009) wird der Open-Innovation-Ansatz wie folgt definiert: „Open Innovation beschreibt den Innovationsprozess als einen vielschichtigen offenen Such- und Lösungsprozess, der zwischen mehreren Akteuren über die Unternehmensgrenzen hinweg abläuft“ (Reichwald et al. 2009, S. 95). Zentrale Gedanken hierbei sind zum einen die bessere Möglichkeit zur Erhebung von Bedürfnisinformationen von Kunden und zum anderen die verbesserte Lösungssuche durch ein heterogenes Netzwerk an Experten (Reichwald et al. 2009). „Open Service Innovation“ stellt die Erweiterung des „Open Innovation“-Ansatzes um die Dienstleistungskomponente dar und zeigt auf, wie Kunden in den Entwicklungsprozess innovativer Dienstleistungen einbezogen werden können (Chesbrough 2011). Dies begründet sich darin, dass eine Orientierung hin zu Dienstleistungen ein zunehmendes und wichtiges Wachstums- und Differenzierungsmerkmal für Unternehmen gegenüber Konkurrenzprodukten darstellt.

2.3.6 Unterstützung von Anbietern bei der Zertifizierung von Services

Zertifizierungen von Cloud-Services können Entscheidungsträger bei der Auswahlentscheidung unterstützen, Transparenz am Markt schaffen, Vertrauen und Akzeptanz auf der Anwenderseite erhöhen sowie es Cloud-Service-Anbietern ermöglichen, ihre Systeme und Prozesse zu überprüfen und zu verbessern (Sunyaev/Schneider 2013). Eine Zertifizierung ist definiert als „eine offizielle, schriftliche Feststellung durch einen unparteiischen Dritten, dass ein bestimmtes Objekt bestimmte von einer unabhängigen Stelle festgelegte Forderungen erfüllt (Konformität im Sinne der Übereinstimmung). Das schriftliche Dokument, das diese Tatsache festhält, wird Zertifikat genannt.“ (Bruhn 2008, S. 424; in Anlehnung an Zollondz 2006, S. 346). Die Vergabe eines Zertifikats kann, je nach Ausgestaltung, eine konkrete

Rechtswirkung entfalten oder aber außerhalb des Rechts beispielsweise als vermarktbare Qualitätsmerkmal dienen. Insofern ist zu unterscheiden zwischen gesetzlich geregelten und nicht gesetzlich geregelten Zertifikaten. Je nach konkreter Rechtswirkung können gesetzlich geregelte Zertifikate ihrerseits beispielsweise (öffentlich-rechtliche) Beweis-, Bindungs- oder Vermutungswirkungen gegenüber Vertragsparteien, Behörden oder anderweitig Betroffenen entfalten (Bieback 2008; Seidel 2000).

2.4 Literaturverzeichnis

- Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; Zaharia, M. (2009):** Above the Clouds: A Berkeley View of Cloud Computing, Electrical Engineering and Computer Sciences University of California at Berkeley, Berkeley, USA, 2009.
- Bieback, K. (2008):** Zertifizierung und Akkreditierung – Das Zusammenwirken staatlicher und nichtstaatlicher Akteure in gestuften Prüfsystemen, Nomos, Baden-Baden, Deutschland 2008.
- BITKOM (2010):** Cloud Computing – Was Entscheider wissen müssen, BITKOM, Berlin, Deutschland 2010.
- Böhm, M.; Leimeister, S.; Riedl, C.; Krcmar, H. (2009):** Cloud Computing: Outsourcing 2.0 oder ein neues Geschäftsmodell zur Bereitstellung von IT-Ressourcen? In: Information Management & Consulting, Vol. 24 (2009) No. 2, S. 6-14.
- Bruhn, M. (2008):** Qualitätsmanagement für Dienstleistungen: Grundlagen, Konzepte, Methoden (7. Ausgabe), Springer, Heidelberg, Deutschland 2008.
- Chesbrough, H.W. (2006):** Open innovation: The new imperative for creating and profiting from technology, Harvard Business School Press, Chichester, Großbritannien 2006.
- Chesbrough, H.W. (2011):** Open Services Innovation: Rethinking Your Business to Grow and Compete in a New Era, Wiley Chichester, Großbritannien 2011.
- DIN EN ISO 9000: (2000):** DIN EN ISO 9000:2000-12 Qualitätsmanagementsysteme – Grundlagen und Begriffe, Beuth Verlag, Berlin, Deutschland 2000.
- Durkee, D. (2010):** Why Cloud Computing Will Never Be Free. In: Communications of the ACM, Vol. 53 (2010) No. 5, S. 62-69.
- Gebauer, L.; Söllner, M.; Leimeister, J.M. (2012):** Hemmnisse bei der Nutzung von Cloud Computing im B2B-Bereich und die Zuordnung dieser zu den verschiedenen Vertrauensbeziehungen. Präsentiert auf der ConLife Academic Conference 2012, Köln, Deutschland.
- Kunz, M.; Gebauer, L.; Ebel, P.A.; Leimeister, J.M. (2013):** Applying an Open Innovation Method for Identifying Challenges in the Cloud Business Environment. Präsentiert auf der ConLife Academics 2013, Berlin, Deutschland.
- Golkowsky, C.; Vehlows, M. (2011):** Cloud Computing im Mittelstand – Erfahrungen, Nutzen und Herausforderungen, PwC, Frankfurt am Main, Deutschland 2011.

- Kempf, D. (2012):** Cloud Computing. http://www.bitkom.org/files/documents/BITKOM_Cloud_Vortrag_Prof_Kempf_07_03_2012.pdf, zugegriffen am 28.7.2014
- KPMG (2013):** Cloud Monitor 2013, KPMG & BITKOM, Düsseldorf, Deutschland 2013.
- Krcmar, H.; Leimeister, S. (2010):** CIO-Umfrage 2010 – Selbstverständnis und Themenschwerpunkte der IT-Entscheider im Jahr 2010. Technische Universität München – Lehrstuhl für Wirtschaftsinformatik, München, Deutschland 2010.
- Leimeister, J.M. (2012):** Dienstleistungengineering und -management, Springer, Heidelberg, Deutschland 2012.
- Leimeister, J.M.; Ebner, W.; Krcmar, H. (2005):** Design, Implementation, and Evaluation of Trust-Supporting Components in Virtual Communities for Patients. In: Journal of Management Information Systems, Vol. 21 (2005) No. 4, S. 101-135.
- Marston, S.; Li, Z.; Bandyopadhyay, S.; Zhang, J.; Ghalsasi, A. (2011):** Cloud computing – The business perspective. In: Decision Support Systems, Vol. 51 (2011) No. 1, S. 176-189.
- NIST (2011):** The NIST Definition of Cloud Computing – Recommendations of the National Institute of Standards and Technology – Special Publication 800-145, U.S. Department of Commerce 2011.
- o.A. (2008):** Let it rise – A survey of corporate IT. In: The Economist, Vol. 23. Oct. 2008 (2008).
- Reichwald, R.; Piller, F.; Ihl, C.; Seifert, S. (2009):** Interaktive Wertschöpfung: Open Innovation, Individualisierung und neue Formen der Arbeitsteilung, Gabler, Wiesbaden, Deutschland 2009.
- Seidel, A. (2000):** Privater Sachverstand und staatliche Garantenstellung im Verwaltungsrecht, C.H. Beck, München, Deutschland 2000.
- Söllner, M.; Hoffmann, A.; Hoffmann, H.; Leimeister, J.M. (2012):** Vertrauensunterstützung für sozio-technische ubiquitäre Systeme. In: Zeitschrift für Betriebswirtschaft, (2012) No. 4, S. 109-140.
- Sunyaev, A.; Schneider, S. (2013):** Cloud Services Certification. In: Communications of the ACM, Vol. 56 (2013) No. 2, S. 33–36.
- Wang, Y.D.; Emurian, H.H. (2005):** An overview of online trust: Concepts, elements, and implications. In: Computers in Human Behavior, Vol. 21 (2005) No. 1, S. 105-125.
- Youseff, L.; Butrico, M.; Da Silva, D. (2008):** Toward a unified ontology of cloud computing. Präsentiert auf dem Grid Computing Environments Workshop, S. 1-10.
- Zollondz, H.-D. (2006):** Grundlagen Qualitätsmanagement – Einführung in Geschichte, Begriffe, Systeme und Konzepte (2. Ausgabe), Oldenbourg, München, Deutschland 2006.

3 Service-Typen und Wertschöpfungsnetzwerke

P. Hoberg, H. Krcmar

3.1 Vom traditionellen IT-Outsourcing zum Cloud-Computing

Der Trend zum Bezug von IT-Services aus der Cloud ist das Ergebnis einer Veränderung der Anforderungen, die Unternehmen an die IT zur Unterstützung ihrer Geschäftsprozesse stellen. Viele Unternehmen sehen große Teile der von ihnen benötigten IT-Ressourcen als einfache Konsumware an (Bharadwaj/Saxena 2009). Diese Kommodifizierung von Teilen der IT wirkt sich negativ auf die Investitionsbereitschaft aus. Entsprechend verlangen Unternehmen vermehrt nach kosteneffizienten Lösungen, die sich flexibel einem schwankenden Ressourcenbedarf anpassen lassen.

Das traditionelle Bereitstellungsmodell des IT-Outsourcings, bei dem dedizierte IT-Ressourcen physisch am Standort des Kunden oder des Dienstleisters vorgehalten werden (Leimeister et al. 2010), wird diesen Anforderungen aufgrund der mit dieser Bereitstellungsform verbundenen hohen Fixkosten nicht gerecht. Cloud-Computing, als eine Form der „ressourcenfreien Bereitstellung von technologischen Kapazitäten“ (Böhm et al. 2009, S. 9), hat sich zu einer aussichtsreichen Alternative entwickelt, die verspricht, augenscheinlich divergierende Kundenanforderungen (Kostenreduzierung bei gleichzeitig höherer Flexibilität) miteinander zu verbinden. Es folgt dem generell zu beobachtenden Trend vom Anbieten von Produkten zum Anbieten von Lösungen (siehe Kapitel 2).

IT muss zu großen Teilen nicht mehr gekauft, sondern kann gemietet und als Dienstleistung über das Internet oder ein privates Netzwerk dem Kunden bereitgestellt werden. Dies umfasst neben Infrastrukturdiensten wie virtualisierten Rechen-, Speicher- oder Netzwerkressourcen spezialisierte Plattformen, die Entwicklungs- und Laufzeitumgebungen zur Verfügung stellen, auf deren Basis Softwareanwendungen entwickelt, betrieben und angeboten werden können (Böhm et al. 2009). Analog zu den in Kapitel 2 beschriebenen

nen Service-Modellen lassen sich damit drei Typen von Cloud-Services identifizieren: Software-Services, Plattform-Services und Infrastruktur-Services.

Im Prinzip muss ein Unternehmen, das seine IT aus der Cloud bezieht, bis auf einen Internetanschluss und netzwerkfähige Endgeräte keine eigenen IT-Ressourcen zur Unterstützung seiner Geschäftsprozesse mehr vorhalten. Google zeigt anhand des Chromebook¹, wie eine nahezu investitionsfreie, professionelle Arbeitsplatzlösung aussehen kann. Die Akzeptanz eines solchen Ansatzes ist in Unternehmen aufgrund der damit verbundenen umfangreichen externen Abhängigkeiten bisher jedoch gering.

Cloud-Computing lässt sich als eine Weiterentwicklung der serviceorientierten Entwicklung und Bereitstellung von Informationstechnologie betrachten. Der Servicegedanke bzw. die Serviceorientierung stellt ein Mittel zur Strukturierung großer Systeme dar (Masak 2007). Sie dient gleichermaßen der Komplexitäts- und Kostenreduktion dieser Systeme, denn, im Sinne der Wiederverwendung, bedeutet Serviceorientierung die Erbringung einer von mehreren Systemeinheiten benötigten Leistung durch eine einzelne Einheit, die diese für die anderen bereitstellt.

Böhm et al. (2009) folgend führt das Prinzip der Serviceorientierung zusammen mit einer fortschreitenden technischen Standardisierung der Cloud-Services zu einem Aufbrechen der klassischen Wertschöpfungsstrukturen im IT-Service Markt. Beim traditionellen IT-Outsourcing tritt der Dienstleister gegenüber seinem Kunden als Full-Service-Dienstleister auf. Vom Transfer der von einer Auslagerung betroffenen Systeme und Organisationseinheiten über Integrationsleistungen bis hin zum Betrieb und der Weiterentwicklung der Systeme bietet der Dienstleister alles aus einer Hand an. Dabei handelt es sich meist um individuell auf die Anforderungen des Kunden angepasste Leistungen. Im Gegensatz dazu handelt es sich bei Cloud-Service-Anbietern um Systemdienstleister. Die angebotenen Cloud-Services sind standardisiert und werden für einen anonymen Markt konzipiert. Sie orientieren sich also weder technisch noch funktional an den individuellen Bedürfnissen eines Kunden, sondern sollen, ganz im Gegenteil, die Anforderungen eines breiten

1 <http://www.sueddeutsche.de/digital/google-entwicklerkonferenz-in-san-francisco-chromebooks-sollen-microsoft-kunden-abjagen-1.1096315>, zuletzt zugegriffen am 04.04.2014

Kundenspektrums bedienen. Die Cloud-Services werden dabei häufig über Plattformen (Bsp.: Cloud Commons² oder Google Apps Marketplace³) angeboten, über welche die Services sowohl vertrieben als auch betrieben werden.

Cloud-Services müssen jeweils eine logisch in sich abgeschlossene Funktionalität aufweisen (Elfatraty 2007). Komplexe, zusammengesetzte Cloud-Services orientieren sich in Bezug auf ihre Funktionszerlegung an der Zerlegung fachlicher Probleme in deren fachliche Teilprobleme. Auf diese Weise können durch Komposition von Cloud-Services Lösungen für komplexe Probleme generiert werden, um Unternehmen eine flexible Anpassung an sich ändernde geschäftliche Anforderungen zu ermöglichen (Böhm et al. 2009).

Hierfür sind anbieterübergreifende Standards für Schnittstellen und Datenaustauschformate notwendig, die in technischer Hinsicht gewährleisten, dass die Funktionalität einfacher Cloud-Services (z.B. von Software-Services) durch Kombination mit anderen Services erweitert werden können. Eine IT-Lösung lässt sich so nach dem Baukastenprinzip aus den Angeboten unterschiedlicher Cloud-Service-Anbieter zusammenstellen. Auf diese Weise entstehen zusammengesetzte Lösungen, die in der Lage sind, komplexe Unternehmensprozesse zu unterstützen (Böhm et al. 2009).

3.2 Veränderte Wertschöpfungsstrukturen im Cloud-Computing

Plattformen für den Betrieb und Vertrieb von Cloud-Services und die Möglichkeit zur Komposition komplexer Serviceangebote aus einfacheren Services haben die Eintrittsbarrieren in den Markt für IT-Services verringert. Als Folge wird die traditionelle, kundenzentrierte Wertschöpfungskette in der IT-Service-Industrie zukünftig durch ein komplexes Wertschöpfungsnetzwerk bestehend aus einer Vielzahl häufig unbekannter, kleiner und mittlerer Dienstanbieter ersetzt (Böhm et al. 2010; Hoberg et al. 2012; Leimeister et al. 2010; Böhm et al. 2011).

2 <http://www.cloudcommons.com>, zuletzt zugegriffen am 20.02.2014

3 <https://www.google.com/enterprise/marketplace>, zuletzt zugegriffen am 20.02.2014

Um die Auswirkungen des Cloud-Computing auf die Wertschöpfungsstruktur des IT-Service-Marktes zu untersuchen, hat der Lehrstuhl für Wirtschaftsinformatik der Technischen Universität München eine Analyse von mehr als zweitausend Cloud-Computing-Diensten durchgeführt. In ihrer Studie identifizieren und beschreiben Böhm et al. (2010) die Rollen, die ein Akteur im Markt für Cloud-Services einnehmen kann, welche Leistungsangebote und Leistungsbedarfe mit den einzelnen Rollen verknüpft sind und welche Austauschbeziehungen zwischen den Rollen bestehen. Den Autoren folgend, beschreibt eine Rolle eine Menge vergleichbarer Leistungsangebote oder Leistungsbedarfe, die von einem Marktakteur (hier: einem Unternehmen) bei anderen Marktakteuren nachgefragt oder anderen Marktakteuren angeboten wird. Ein Akteur kann dabei in verschiedenen Rollen agieren.

Böhm et al. (2010) identifizieren acht generische Rollen (siehe [Abbildung 1](#)): *Anwendungs-, Plattform- und Infrastrukturanbieter* stellen dabei die Basisfunktionen im Sinne von Software, Entwicklungs- und Laufzeitumgebung bzw. Rechen-, Speicher- und Netzwerkkapazitäten zur Verfügung. Diese werden von *Aggregatoren* und *Integratoren* zu kundenspezifischen Lösungen kombiniert. Beide unterscheiden sich lediglich darin, dass Integratoren eine individuelle Lösung für einen spezifischen Kunden entwickeln, während Aggregatoren diese Lösung einer größeren Anzahl von Kunden als eigenen Dienst anbieten. Cloud-Services können entweder direkt genutzt oder über eine *Marktplattform* bereitgestellt werden. Die Marktplattform übernimmt dabei neben dem Zusammenbringen von Angebot und Nachfrage auch Abrechnungsfunktionen. *Berater* stellen keine Cloud-Services bereit, sondern bieten Beratungsleistungen für unterschiedliche Akteure. *Konsumenten* stellen schließlich den Endanwender eines Cloud-Services dar.

Ausgehend von diesen acht generischen Rollen stellen Böhm et al. (2010) das Cloud-Computing-Ökosystem als generisches Wertschöpfungsnetzwerk dar. Den Autoren folgend handelt es sich hierbei um ein System unabhängiger Akteure, die durch ihre Zusammenarbeit einen inkrementellen Wertbeitrag schaffen. Durch die Erstellung elementarer Dienste (z.B. Infrastruktur, Software) und deren Verfeinerung (z.B. Aggregation) wird innerhalb des Netzwerkes, entlang eines Pfades hin zum Konsumenten Wert geschaffen (Böhm et al. 2010). Grundlage für die Entstehung dieses Ökosystems stellen modulare, ubiquitär einsetzbare Cloud-Services dar (Böhm et al. 2010).

Abbildung 1: Wertschöpfungsnetzwerk im Cloud-Computing (Böhm et al. 2010, S. 8)

Böhm et al. (2009) führen aus, dass ein Cloud-Service, wie er von einem Konsumenten gesehen wird, der sich keine Gedanken über die Art und Weise der Implementierung und Bereitstellung macht, eine Komposition verschiedener Services darstellt. Dem neuen Wertschöpfungsmodell folgend, beziehen Konsumenten, Aggregatoren und Integratoren Services in Form von SaaS, PaaS oder IaaS direkt vom Dienstanbieter bzw. über eine Marktplattform (Böhm et al. 2010). Zur Leistungserstellung greifen Anwendungs- bzw. Plattformanbieter im Modell auf die jeweils zugrunde liegenden Basisdienste (PaaS bzw. IaaS) zurück (Böhm et al. 2010). Aggregatoren und Integratoren kombinieren eine beliebige Anzahl verschiedener Services, um einen Mehrwert für ihre Kunden zu schaffen, und die Beratung stellt den anderen Rollen diverse Beratungsleistungen zur Verfügung (Böhm et al. 2010).

3.3 Standardisierungsproblem im Cloud-Markt

Bisher haben sich für Cloud-Services keine einheitlichen Schnittstellen- und Kommunikationsstandards etablieren können. Eine Zersplitterung des Cloud-Service-Marktes ist die Folge, in dem verschiedene Anbieter versuchen, mittels proprietärer Formate eigene, abgeschottete Ökosysteme um ihre Services herum aufzubauen. Böhm et al. (2009; 2010) illustrieren dies anhand des amerikanischen Unternehmens Salesforce. Salesforce ist einer der größten Anbieter von Unternehmensanwendungen für das Kundenbeziehungsmanagement (CRM) aus der Cloud. Wie im Bereich der Smartphone-Betriebssysteme mit ihren Stores für Fremdanbietersoftware ebenfalls üblich, bietet Salesforce neben einem eigenen Software-Service (Salesforce CRM) einen Plattform-Service in Form einer proprietären Laufzeit- und Entwicklungsumgebung an. Diese Laufzeit- und Entwicklungsumgebung ermöglicht es Nutzern von Salesforce CRM einerseits, eigene Erweiterungen für das CRM-System zu entwickeln. Andererseits können Drittanbieter die Plattform dafür nutzen, eigene Applikationen zu entwickeln und über die Salesforce-Plattform zu vertreiben. Salesforce tritt dem Beispiel aus Böhm et al. (2009; 2010) folgend im Markt in verschiedenen Rollen auf, als Plattformbetreiber, Softwareanbieter und Marktplatzbetreiber.

Der Einsatz proprietärer Technologien erschwert Anwenderunternehmen die Nutzung von Cloud-Services in unterschiedlichen Ökosystemen. Auf die-

se Weise wird zum einen die Angebotsvielfalt für die Anwenderunternehmen verringert. Aufgrund der Investitionen, die Anwenderunternehmen sowohl für die anforderungsspezifische Anpassung von Cloud-Services, deren technische Integration in das Unternehmen und für die möglicherweise notwendigen organisatorischen und prozessualen Anpassungen im Unternehmen aufwenden, entstehen zum anderen Wechselkosten, die von vielen Unternehmen als Risiko wahrgenommen werden. Denn analog zur Entwicklungshistorie etablierter Ökosysteme (z.B. Video-, Musik- und Automobilindustrie) ist auch im Markt für Cloud-Services eine Konsolidierung durch Fusion oder Marktaustritt von Anbietern zu erwarten. Die zukünftige Entwicklung des Cloud-Marktes ist entsprechend mit großen Unsicherheiten behaftet. Dies macht es für Entscheidungsträger in Kundenunternehmen schwierig, eine geeignete Cloud-Strategie zu entwickeln.

3.4 Literaturverzeichnis

- Bharadwaj, S.S.; Saxena, K.B.C. (2009):** Building Winning Relationships in Business Process Outsourcing Services. In: *Industrial Management & Data Systems*, Vol. 109 (2009) No. 7, S. 993-1011.
- Böhm, M.; Koleva, G.; Leimeister, S.; Riedl, C.; Krcmar, H. (2010):** Towards a Generic Value Network for Cloud Computing. Präsentiert auf dem 7th International Workshop on Economics of Grids, Clouds, Systems, and Services, Ischia, Italien.
- Böhm, M.; Leimeister, S.; Riedl, C.; Krcmar, H. (2009):** Cloud Computing: Outsourcing 2.0 oder ein neues Geschäftsmodell zur Bereitstellung von IT-Ressourcen? In: *Information Management & Consulting*, Vol. 24 (2009) No. 2, S. 6-14.
- Böhm, M.; Leimeister, S.; Riedl, C.; Krcmar, H. (2011):** Cloud Computing – Outsourcing 2.0 or a new Business Model for IT Provisioning? In: *Application Management: Challenges – Service Creation – Strategies* (Vol. 1). Keuper, F.; Oecking, C.; Degenhardt, A. (Hrsg.). Gabler, Wiesbaden, Deutschland 2011.
- Elfatry, A. (2007):** Dealing with change: components versus services. In: *Communications of the ACM*, Vol. 50 (2007) No. 8, S. 35-39.
- Hoberg, P.; Wollersheim, J.; Krcmar, H. (2012):** The Business Perspective on Cloud Computing – A Literature Review of Research on Cloud Computing. Präsentiert auf der 18th Americas Conference on Information Systems (AMCIS), Seattle, USA.
- Leimeister, S.; Riedl, C.; Böhm, M.; Krcmar, H. (2010):** The business perspective of cloud computing: Actors, roles, and value networks. Präsentiert auf der 18th European Conference on Information Systems, Pretoria, Südafrika.
- Masak, D. (2007):** SOA? – Serviceorientierung in Business und Software, Springer, New York 2007.

Teil C:
Unterstützungsbedarf
aus Sicht Cloud-nutzender
Unternehmen

4 Qualitätsanalyse und -bewertung von Cloud-Services

J. Wollersheim, H. Krcmar

4.1 Einleitung

Informationen bezüglich der von einem Cloud-Service zu erwartenden Qualität sind eine wichtige Voraussetzung für die Cloud-Service-Nutzung in vielerlei Hinsicht. Dies gilt nicht nur für Qualitätsinformationen, die von Unternehmen im Beschaffungsprozess benötigt und genutzt werden, um zu beurteilen, ob die Qualitätseigenschaften eines Cloud-Service geeignet sind, den unternehmensspezifischen Bedarf zu decken. In Folge sind Qualitätsinformationen auch für die Verbreitung des Bereitstellungsmodells Cloud-Service in der Wirtschaft als solche eine notwendige Voraussetzung, da etwa positiv wie negativ wahrgenommene Qualität die zukünftige Servicenutzung beeinflusst (Kettinger et al. 2009; Riedl et al. 2009).

Forschung hinsichtlich einzelner Qualitätsparameter findet bereits vereinzelt und isoliert statt, wie etwa die strukturierte Auflistung von Sicherheitsanforderungen oder anderer Qualitätsparameter bezüglich der Produkteigenschaften von Cloud-Services und somit der Ergebnisqualität zeigt (Hoberg et al. 2012a; CSA 2011; BSI 2012; ENISA 2009). Diese auf Eigenschaften der Ergebnisqualität fokussierenden Qualitätsparameter lehnen sich dabei an Rahmenwerke wie die IT-Grundschutzkataloge des BSI (BSI 2011) oder Forschungsergebnisse im Bereich der Softwarequalität an (Alsultanny/Wohaishi 2009). Darüber hinaus werden auch Qualitätsparameter thematisiert, die sich auf die Qualitätswahrnehmung zum Zeitpunkt der Nutzung, also die Prozessqualität beziehen. Spezifisch für Aspekte der Prozessqualität von Cloud-Services wurden von Benlian et al. (2011) oder auch Gorla (2011) Kriterien-Sets entwickelt, aufbauend auf den grundlegenden Forschungsarbeiten zu SERVQUAL und alternativen Skalen zur Messung der wahrgenommenen Servicequalität (Parasuraman et al. 1988; Cronin Jr/Taylor 1992; Kettinger/Lee 1997; Parasuraman et al. 2005; Kettinger/Lee 2005).

Die schematische Zusammenführung beider Qualitätsdimensionen, der Ergebnisqualität und der Prozessqualität, zu einem vollständigen Bild von

der Qualität eines IT-Services aus Kundensicht wurde von den internationalen Normierungsgremien (ISO/IEC 25010 2011), aber auch von einzelnen Forschungsteams wie Lepmets et al. (2011; 2012) oder Siegel/Perdue (2012) aufgegriffen. Die erzielten, schematischen Ergebnisse sind jedoch sehr grobgranular und bei weitem nicht so detailliert auf Cloud-Services angepasst, wie die wesentlich spezifischeren Ergebnisse hinsichtlich der einzelnen Qualitätsdimensionen Ergebnis- und Prozessqualität.

Es erscheint notwendig, diese Ergebnisse stärker zusammenzuführen und sie an die Anforderungen des betrieblichen Beschaffungsprozesses wie auch die Anforderungen der kontinuierlichen Service-Governance und Steuerung anzupassen. Hierzu ist es jedoch zunächst notwendig, die bei der Beschaffung und Steuerung von Cloud-Services bestehenden Unterstützungsanforderungen zu eruieren.

Die nachfolgenden Abschnitte dieses Beitrags zeigen die Spezifika der Qualitätsanalyse von Cloud-Services auf und arbeiten den bestehenden Unterstützungsbedarf von Cloud-Anwendern und solchen Unternehmen heraus, die die Beschaffung von Cloud-Services in Erwägung ziehen. Der identifizierte Unterstützungsbedarf diente im Projekt Value4Cloud als Basis einzelner Arbeitspakete und wird entsprechend durch Werkzeuge unterstützt, die im Laufe des Projekts entwickelt wurden (siehe Beiträge in den Kapiteln 9, 10, 11, 19 und 24 in diesem Buch).

4.2 Qualität – eine Begriffsbestimmung

Im Gegensatz zu maßgeschneiderten IT-Services sind Cloud-Services per Definition standardisiert und nur zu kleinen Teilen kundenindividuell anpassbar. Der Erstellungsprozess von Cloud-Services erfolgt hochindustrialisiert unter Nutzung von Größendegressionseffekten und für einen aus Sicht des Serviceanbieters anonymen und dezentralen Markt (Chen/Wu 2013; Benlian/Hess 2011). Diese geringe Individualisierung ist von potenziellen Service-Anwendern und Interessenten bereits in ihren Beschaffungsprozessen zu berücksichtigen. Interessenten sind gefordert, ihren Bedarf voll- und eigenständig zu definieren, am Markt nach geeigneten Lösungen zu suchen und diese im Anschluss zu bewerten. Der Versand grob skizzierter Anforderungslisten, verbunden mit der Bitte an potenzielle Anbieter, eine individuell aus-

gestaltete und die Anforderungen exakt adressierende Dienstleistung als Lösung vorzuschlagen, ist bei der Beschaffung von Cloud-Services nicht anwendbar. Der Rückgriff auf das Know-how und die Problemlösungskompetenz der Dienstleister ist im Bereitstellungsmodell „Cloud-Service“ in diesem Maße nicht vorgesehen (Wollersheim et al. 2013b; Wollersheim/Krcmar 2013). Die Spezifikation der eigenen Qualitätsanforderungen, die Beurteilung des Erfüllungsgrades sowie alternativer Lösungsoptionen und der anschließende Abgleich mit den eigenen Qualitätsanforderungen muss bei der Beschaffung von Cloud-Services durch die beschaffende Organisation selbst durchgeführt werden. Der Rückgriff auf bekannte Aktivitäten und Prozesse zur Beschaffung standardisierter Produkte, wie Office-Suiten oder IT-Hardware, kann Anregungen liefern, greift jedoch zu kurz. Bei der Beschaffung standardisierter Produkte beschränkt sich die Qualitätsprüfung auf Produkteigenschaften. Der bei Dienstleistungen wie Cloud-Services jedoch ebenso wichtige Aspekt der Prozessqualität wird zumeist nicht adressiert. Da der Konsum von Dienstleistungen eine andauernde Austauschbeziehung zwischen Anbieter und Kunde begründet, sind Qualitätsmetriken erforderlich, die nicht nur Produkteigenschaften einzelner Ergebnisse beurteilen, sondern die auch Qualitätsaspekte der Service-Nutzungsphase umfassen. Gemäß Grönroos (2007) können zwei Dimensionen verwendet werden, um das entstehende Set von Qualitätsmerkmalen aus der Sicht des Kunden zu strukturieren: eine Dimension, die solche Merkmale umfasst, die sich auf das Ergebnis einer Dienstleistung beziehen, und eine Dimension, die Qualitätsmerkmale des Leistungserstellungs- und Nutzungsprozesses fokussiert (Grönroos 2007, 73). Dabei ist zu beachten, dass die Qualität während des Nutzungsprozesses vom Leistungsempfänger sehr individuell wahrgenommen wird und auch erst nach einer gewissen Nutzungszeit umfassend beurteilt werden kann (Grönroos 2007, 75).

Ergänzend werden Merkmale des Anbieters und sein Image am Markt in einer weiteren Qualitätsdimension zusammengefasst. Diese Qualitätsdimension dient als Filter für Qualitätswahrnehmungen in den Dimensionen „Ergebnisqualität“ und „Prozessqualität“, kann jedoch auch genutzt werden, um fehlende Werte zu interpolieren. Einem Anbieter aufgrund seines Images zu-

Abbildung 1: Dimensionen von Dienstleistungsqualität (Grönroos 2011, 1984, 2007)

geschriebene Qualitätseigenschaften können beispielsweise fehlende eigene Qualitätserfahrungen und somit Lücken in der Bewertung der Prozessqualität kompensieren. [Abbildung 1](#) illustriert diesen Zusammenhang. Das dargestellte und in dieser Arbeit verwendete Modell zur Strukturierung von Qualitätsmerkmalen in die Dimensionen „Ergebnisqualität“, „Prozessqualität“ und „Image“ versteht sich als konzeptioneller Rahmen und nicht als unmittelbares Messmodell (Grönroos 2007, 89).

Neben diesen drei Qualitätsdimensionen wurden in der Literatur auch andere Vorschläge diskutiert (Garvin 1987; Rust/Oliver 1994; Dabholkar et al. 2000; Brady 2001), die im Rahmen dieses Projektes jedoch nicht weiter verfolgt werden. Qualität als solche sollte nach dem in dieser Studie verwendeten Verständnis nicht gemessen werden (Grönroos 2001, S. 151; Geiger/Kotte 2008, S. 71).

Welche Merkmale von Cloud-Services konkret innerhalb der einzelnen Dimensionen wie „Ergebnisqualität“, „Prozessqualität“ oder „Image“ vom Kunden erwartet werden, ist unterschiedlich. In Abhängigkeit von den individuell verschiedenen Anforderungen an einen Service ist auch die Qualitätswahrnehmung bezüglich dieses Services für jeden Kunden nahezu individuell. Sie kann jedoch durch den Kunden einer Dienstleistung mit Adjektiven wie schlecht, gut und ausgezeichnet beurteilt werden (Geiger/Kotte 2008, S. 71).

4.3 Qualitätsanalyse und -bewertung von Cloud-Services aus der Käufer-Perspektive

Aufbauend auf den bereits im wissenschaftlichen Kontext von Wollersheim/Krcmar (2013, 2014) erfolgten Veröffentlichungen zum Thema werden nachfolgend die wesentlichen Aspekte von Servicequalität im betrieblichen Kontext, Servicequalität in Zusammenhang mit betrieblichen Beschaffungsprozessen und der besonders zu berücksichtigenden Qualitätsaspekte von Cloud-Services kurz zusammengefasst.

Der Einkaufsprozess ist zwischen privaten Konsumenten und Organisationen unterschiedlich (Wilson 2000). Der Einkauf von Produkten und Dienstleistungen in Organisationen wird von einer Vielzahl von Faktoren und Personen beeinflusst (Webster/Wind 1972, S. 13). Entscheidungen werden aufgrund von nachvollziehbaren Bewertungsergebnissen bezüglich der spezifizierten Anforderungen an die Produkt- und Prozessqualität eines zu beschaffendes Gutes (siehe vorheriger Abschnitt) getroffen. Hierbei ist zu beachten, dass sowohl die Auswahl der Kriterien als auch die Auswahl der bewertenden Personen und somit die Bewertung als solche von einer Vielzahl von Faktoren beeinflusst werden kann. Nach Backhaus/Voeth (2010, S. 38) – konkretisiert um den Einflussfaktor „Technik“ (vgl. TOE Framework von Tornatzky/Fleischer 1990) und aufbauend auf früheren Forschungsergebnissen (Webster/Wind 1972; Campbell 1985; Johnston/Lewin 1996) – können die vier Dimensionen „Umwelt“, „Organisation“, „Beschaffungsgut/Technologie“ und „interpersonelle/individuelle Faktoren“ zur Strukturierung dieser Einflussfaktoren auf den Beschaffungsprozess verwendet werden.

- **Umwelt:** Einflussfaktoren dieser Dimension umfassen bspw. Eigenschaften der Industrie und des wirtschaftlichen Ökosystems des beschaffenden Unternehmens oder gesetzliche Regularien.
- **Organisation:** Einflussfaktoren dieser Dimension umfassen die formalen und informalen Prozesse und Regeln innerhalb der beschaffenden Organisation, wie etwa bei der Beschaffung von IT-Services, zu berücksichtigende Schutzklassen und zugehörige Schutzmechanismen.

- **Beschaffungsgut/Technologie:** Einflussfaktoren dieser Dimension umfassen Produkt- und Technologieeigenschaften wie bspw. die Eigenschaften von Cloud-Services (gemäß Definition der NIST 2011).
- **Interpersonelle/individuelle Faktoren:** Diese Dimension umfasst bspw. Einflussfaktoren aufgrund von Zuständigkeitsverteilungen zwischen Abteilungen oder die Expertise und das Wissen einzelner Entscheidungsträger im Team.

Einflüsse in diesen vier Dimensionen bestimmen die im Prozess durchgeführten Aktivitäten, die Auswahl der beteiligten Personen, die individuelle Ausgestaltung der Qualitätsanforderungen und auch die Qualitätskriterien bzw. die Bewertung anhand der Kriterien. Die Qualitätsanforderungen sind wesentlicher Teil der Anforderungsspezifikation eines Unternehmens im Beschaffungsprozess. Bei der Beteiligung mehrerer Personen an der Beziehung zwischen Kunden- und Dienstleisterunternehmen, also dem Regelfall bei Beschaffungen im betrieblichen Kontext, ist die gesamte Personengruppe innerhalb des beschaffenden Unternehmens als Kunde zu betrachten (Grönroos 2007; March 1962). Diese Gruppe von Personen, die am Einkauf und der anschließenden Leistungsnutzung beteiligt ist, wird in der Literatur auch als „buying center“ bezeichnet und ist in ihrer Gesamtheit verantwortlich für die Spezifikation der Qualitätsanforderungen sowie Adressat bezüglich etwaiger Bewertungen der Servicequalität zum Zeitpunkt der Beschaffung, wie auch im Anschluss an die Leistungserbringung (Grönroos 2007, 359). Die Qualitätswahrnehmung jedes Einzelnen (Einkäufer, Nutzer des Cloud-Services, Mitarbeiter der den Service integrierenden IT-Abteilung, etc.) ist zu berücksichtigen, um ein vollständiges Bild der Qualitätsanforderungen wie auch der diesen Anforderungen gegenüberstehenden Qualitätswahrnehmung von Unternehmenskunden zu erhalten. Die Ermittlung der Anforderungen an einen Cloud-Service, und somit die Qualitätserwartungen, ist eine der initialen Aufgaben im betrieblichen Beschaffungsprozess. Diverse Qualitätsaspekte verlangen eine Berücksichtigung, es sind Qualitätsanforderungen zu definieren und im Anschluss ist die wahrgenommene Qualität diesen Anforderungen gegenüberzustellen.

Bezüglich welcher Qualitätsaspekte konkrete Anforderungen im Rahmen des Beschaffungsprozesses definiert werden sollten, ist Gegenstand aktueller Forschung, etwa von Repschläger et al. (2012) oder auch Hoberg et al. (2012a). Die Autoren schlagen leicht voneinander abweichende Kataloge von Qualitätskriterien vor, um diesen Bedarf zu adressieren. Neben diesen Kriterienkatalogen im akademischen Umfeld entstanden auch erste Kataloge in der Unternehmenspraxis, die sich auf spezielle Qualitätsaspekte wie etwa Sicherheitseigenschaften von Cloud-Services konzentrierten (BSI 2012; CSA 2009). Um jedoch für Unternehmen kleiner und mittlerer Größe möglichst effizient einsetzbar zu sein, werden vordefinierte Sets von Serviceeigenschaften benötigt. Diese Sets können einen Überblick über wichtige Kernmerkmale bieten und verhindern somit, dass sich Unternehmen in einzelnen Details verlieren. Auch ermöglichen sie den Verweis auf weiterführende Aspekte, sollte ein spezifischer Qualitätsaspekt für das beschaffende Unternehmen von besonderer Bedeutung sein.

4.4 Zusammenfassung: identifizierter Unterstützungsbedarf aus Sicht Cloud-nutzender Unternehmen

Um diesen Unterstützungsbedarf weiter zu konkretisieren, wurde die wissenschaftliche und praxisorientierte Literatur analysiert und solche Merkmale von Cloud-Services identifiziert, die für Kunden bei der Beschaffung zumeist eine Rolle zu spielen scheinen. Im Anschluss an die Literaturstudie wurden Merkmale ergänzt, die in Gruppeninterviews mit Personen ermittelt werden konnten, die bereits Erfahrung mit der Beschaffung von Cloud-Services besitzen. Das Ergebnis wurde im Kontext des Projektes Value4Cloud veröffentlicht (unter anderem in Hoberg et al. 2012b; Wollersheim et al. 2013a, 2013b). Auf diese Weise konnte der Unterstützungsbedarf in der Unternehmenspraxis sowie die entwickelten Lösungsbausteine im Projekt Value4Cloud weiter konkretisiert werden. Insbesondere die durchgeführten Interviews ermöglichten eine offene Diskussion des Unterstützungsbedarfs Cloud-nutzender Unternehmen im Beschaffungsprozess und der für sie besonders relevanten Eigenschaften von Cloud-Services. Zusammenfassend konnten, im Laufe des durchgeführten Forschungsprozesses, die folgenden Unterstützungsbedarfe identifiziert werden:

- **Unterstützungsbedarf bzgl. der Eruiierung und Strukturierung des eigenen IT-Bedarfs:** Bei Cloud-Services ist aus Sicht des beschaffenden Unternehmens zu Beginn der Akquisition eine wesentlich exaktere Bedarfsspezifikation notwendig, als etwa bei der Beschaffung standardisierter IT-Produkte oder individueller IT-Dienstleistungen, die vom Anbieter passgenau bereitgestellt werden. Um bei der Bedarfsspezifikation alle relevanten Parameter und Akteure zu berücksichtigen, ist es zunächst notwendig, etwaige Einflussfaktoren auf das eigene Unternehmen und den zu etablierenden Beschaffungsprozess zu kennen. Erst im Anschluss kann der Bedarf anhand der für das Unternehmen wichtigen Kriterien spezifiziert werden. Hierbei sind nicht nur die Anforderungen einer Vielzahl von Kollegen im Unternehmen zu berücksichtigen, sondern auch der Schutzbedarf der Daten, die durch den Service verarbeitet werden sollen. Sind diese etwa für das Unternehmen von besonderer Bedeutung, so kommt der Sicherheit des zu beschaffenden Cloud-Services ein vergleichsweise höherer Stellenwert zu. Dies ist bei der Eruiierung des Leistungsbedarfs und der Initiierung des Beschaffungsprozesses zu bedenken.
- **Bedarf an Unterstützung im Auswahlprozess, etwa bzgl. der Zuordnung von Verantwortlichkeiten und der Festlegung von Auswahlkriterien:** Sind die wesentlichen Anforderungen innerhalb des beschaffenden Unternehmens bekannt, muss dem eruierten Bedarf das Angebot gegenübergestellt werden. Um beim Abgleich Missverständnisse zwischen Service-Anbieter und Kunde zu vermeiden, ist ein möglichst eindeutiges Vokabular nötig, um sowohl den angebotenen Service zu beschreiben, als auch den Bedarf zu spezifizieren.
- **Bedarf an Unterstützung bzgl. der kontinuierlichen Steuerung von Cloud-Services:** Anders als bei IT-Hardware können Cloud-Services nicht einer umfassenden Wareneingangsprüfung unterzogen werden, um alle Qualitätsaspekte abschließend zu beurteilen. Es ist eine kontinuierliche Überwachung der Dienstleistung notwendig. Anhand welcher Kriterien diese Überwachung etabliert werden sollte, aber auch wie diese durch das den Cloud-Service nutzende Unternehmen umzusetzen ist, sind offene Fragen, denen sich insbesondere mittelständische Unternehmen

ohne Erfahrung in der Dienstleistersteuerung gegenüber sehen. Welche Qualitätseigenschaften von Cloud-Services einer kontinuierlichen Überwachung bedürfen, etwa um Minderleistung und damit verbundene Verletzungen von Service Level Agreements festzustellen oder auch um eine Datenbasis zu dem Service-Anbieter zu schaffen, etwa als Input für zukünftige Investitionsentscheidungen, wird in Kapitel 10 in diesem Buch adressiert.

Eine detaillierte Beschreibung der im Projekt Value4Cloud entwickelten Werkzeuge zur Adressierung und Lösung dieser Anforderungen in Unternehmen des deutschen Mittelstandes folgt in den nachfolgenden Beiträgen dieses Buches.

4.5 Literaturverzeichnis

- Alsultanny, Y.A.; Wohaishi, A.M. (2009):** Requirements of Software Quality Assurance Model. Präsentiert auf der 2nd International Conference on Environmental and Computer Science (ICECS), Hammamet, Tunesien, S. 19-23.
- Backhaus, K.; Voeth, M. (2010):** Industriegütermarketing (9. Ausgabe), Vahlen, München, Deutschland 2010.
- Benlian, A.; Hess, T. (2011):** Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. In: Decision Support Systems, Vol. 52 (2011) No. 1, S. 232-246.
- Benlian, A.; Koufaris, M.; Hess, T. (2011):** Service Quality in Software-as-a-Service: Developing the SaaS-QUAL Measure and Examining Its Role in Usage Continuance. In: Journal of Management Information Systems (JMIS), Vol. 28 (2011) No. 3, S. 85-126.
- Brady, M.K. (2001):** Some New Thoughts on Conceptualizing Perceived Service Quality: A Hierarchical Approach. In: Journal of Marketing, Vol. 65 (2001) No. 3, S. 34-49.
- BSI (2011):** IT-Grundschutz-Kataloge, Bundesamt für Sicherheit in der Informationstechnik – BSI, Bonn, Deutschland 2011.
- BSI (2012):** Eckpunktepapier – Sicherheitsempfehlungen für Cloud Computing Anbieter – Mindestanforderungen in der Informationssicherheit, Bundesamtes für Sicherheit in der Informationstechnik – BSI, Bonn, Deutschland 2012.
- Campbell, N.C.G. (1985):** An interaction approach to organizational buying behavior. In: Journal of Business Research, Vol. 13 (1985) No. 1, S. 35-48.
- Chen, P.-y.; Wu, S.-y. (2013):** The Impact and Implications of On-Demand Services on Market Structure. In: Information Systems Research, Vol. 24 (2013) No. 3, S. 750-767.

- Cronin Jr, J.J.; Taylor, S.A. (1992):** Measuring Service Quality: A Reexamination and Extension. In: *Journal of Marketing*, Vol. 56 (1992) No. 3, S. 55-68.
- CSA (2009):** Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance – CSA, Seattle, USA 2009.
- CSA (2011):** Consensus Assessments Initiative Questionnaire. <https://cloudsecurityalliance.org/research/cai/>, zugegriffen am 28.07.2014.
- Dabholkar, P.A.; Shepherd, C.D.; Thorpe, D.I. (2000):** A Comprehensive Framework for Service Quality: An Investigation of Critical Conceptual and Measurement Issues Through a Longitudinal Study. In: *Journal of Retailing*, Vol. 76 (2000) No. 2, S. 139-173.
- ENISA (2009):** Cloud Computing – Benefits, risks and recommendations for information security, European Network and Information Security Agency (ENISA) 2009.
- Garvin, D.A. (1987):** Competing on the eight dimensions of quality. In: *Harvard Business Review*, Vol. 65 (1987) No. 6, S. 101-109.
- Geiger, W.; Kotte, W. (2008):** Handbuch Qualität (5. Ausgabe), Vieweg, Wiesbaden, Deutschland 2008.
- Gorla, N. (2011):** An assessment of information systems service quality using SERVQUAL+. In: *The DATA BASE for Advances in Information Systems*, Vol. 42 (2011) No. 3, S. 46-70.
- Grönroos, C. (1984):** A service quality model and its marketing implications. In: *European Journal of Marketing*, Vol. 18 (1984) No. 4, S. 36-44.
- Grönroos, C. (2001):** The perceived service quality concept—a mistake? In: *Managing Service Quality*, Vol. 11 (2001) No. 3, S. 150-152.
- Grönroos, C. (2007):** Service Management and Marketing: Customer Management in Service Competition (3. Ausgabe), Wiley, Chichester, Großbritannien 2007.
- Grönroos, C. (2011):** In The Marketplace There Is Only Service – Facilitating Customers' Value Creation. Präsentiert auf der 19th European Conference on Information Systems (ECIS), Helsinki, Finnland.
- Hoberg, P.; Wollersheim, J.; Krcmar, H. (2012a):** The Business Perspective on Cloud Computing – A Literature Review of Research on Cloud Computing. Präsentiert auf der 18th Americas Conference on Information Systems (AMCIS), Seattle, USA.
- Hoberg, P.; Wollersheim, J.; Krcmar, H. (2012b):** Service Descriptions for Cloud Services – The Customer's Perspective. Präsentiert auf der ConLife Academic Conference 2012, Köln, Deutschland.
- ISO/IEC 25010 (2011):** Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE), 2011.
- Johnston, W.J.; Lewin, J.E. (1996):** Organizational buying behavior: Toward an integrative framework. In: *Journal of Business Research*, Vol. 35 (1996) No. 1, S. 1-15.
- Kettinger, W.J.; Lee, C.C. (1997):** Pragmatic Perspectives on the Measurement of Information Systems Service Quality. In: *MIS Quarterly*, Vol. 21 (1997) No. 2, S. 223-240.

- Kettinger, W.J.; Lee, C.C. (2005):** Zones Of Tolerance: Alternative Scales For Measuring Information Systems Service Quality. In: *MIS Quarterly*, Vol. 29 (2005) No. 4, S. 607-623.
- Kettinger, W.J.; Park, S.H.; Smith, J. (2009):** Understanding the consequences of information systems service quality on IS service reuse. In: *Information & Management*, Vol. 46 (2009) No. 6, S. 335-341.
- Lepmets, M.; Cater-Steel, A.; Gacenga, F.; Ras, E. (2012):** Extending the IT service quality measurement framework through a systematic literature review. In: *Journal of Service Science Research*, Vol. 4 (2012) No. 1, S. 7-47.
- Lepmets, M.; Ras, E.; Renault, A. (2011):** A Quality Measurement Framework for IT Services. Präsentiert auf der Annual SRII Global Conference, San Jose, USA, S. 767-774.
- March, J.G. (1962):** The Business Firm as A Political Coalition. In: *The Journal of Politics*, Vol. 24 (1962) No. 04, S. 662-678.
- NIST (2011):** The NIST Definition of Cloud Computing – Recommendations of the National Institute of Standards and Technology – Special Publication 800-145, U.S. Department of Commerce 2011.
- Parasuraman, A.; Zeithaml, V.A.; Berry, L.L. (1988):** SERVQUAL: A Multiple-Item Scale for Measuring Consumer Perceptions of Service Quality. In: *Journal of Retailing*, Vol. 64 (1988) No. 1, S. 12-40.
- Parasuraman, A.; Zeithaml, V.A.; Malhotra, A. (2005):** E-S-QUAL: A multiple-item scale for assessing electronic service quality. In: *Journal of Service Research*, Vol. 7 (2005) No. 3, S. 213-233.
- Repschlaeger, J.; Zarnekow, R.; Wind, S.; Turowski, K. (2012):** Cloud Requirements Framework: Requirements And Evaluation Criteria To Adopt Cloud Solutions. Präsentiert auf der 20th European Conference on Information Systems (ECIS), Barcelona, Spanien.
- Riedl, C.; Böhmman, T.; Rosemann, M.; Krcmar, H. (2009):** Quality management in service ecosystems. In: *Information Systems and E-Business Management*, Vol. 7 (2009) No. 2, S. 199-221.
- Rust, R.T.; Oliver, R.L. (1994):** Service quality: insights and managerial implications from the frontier. In: *Service quality: New directions in theory and practice*. Rust, R.T.; Oliver, R.L. (Hrsg.). Sage Publications, Thousand Oaks, USA 1994, S. 1-19.
- Siegel, J.; Perdue, J. (2012):** Cloud Services Measures for Global Use: The Service Measurement Index (SMI). Präsentiert auf der Service Research and Innovation Institute (SRII) Global Conference, San Jose, USA, S. 411-415.
- Tornatzky, L.; Fleischer, M. (1990):** The process of technology innovation, Lexington Books, Lexington, USA 1990.
- Webster, F.E.; Wind, Y. (1972):** A General Model for Understanding Organizational Buying Behavior. In: *Journal of Marketing*, Vol. 36 (1972) No. 2, S. 12-19.
- Wilson, D.F. (2000):** Why divide consumer and organizational buyer behaviour? In: *European Journal of Marketing*, Vol. 34 (2000) No. 7, S. 780-796.

Wollersheim, J.; Hoberg, P.; Krcmar, H. (2013a): How to specify cloud service demand – An approach recognizing planned application. Präsentiert auf der ConLife Academics 2013, Berlin, Deutschland.

Wollersheim, J.; Hoberg, P.; Krcmar, H. (2013b): Procurement of Cloud Services: Seven Principles to Success. Präsentiert auf der 13th International Research Symposium on Service Excellence in Management (QUIS), Karlstad, Schweden, S. 423-431.

Wollersheim, J.; Krcmar, H. (2013): Purchasing processes for cloud services – An exploratory study of process influencing factors. Präsentiert auf der 22nd Annual IPSERA Conference, Nantes, Frankreich, S. 1285-1295.

Wollersheim, J.; Krcmar, H. (2014): Quality analysis approaches for cloud services – Towards a framework along the customer's activity cycle. In: Trusted Cloud Computing. Reussner, R.; Rumpe, B.; Krcmar, H. (Hrsg.). Springer, Wiesbaden, Deutschland.

5 Cloud-Service-Zertifizierung

A. Sunyaev, S. Schneider

5.1 Zertifizierung von Cloud-Services¹

Das Cloud-Ökosystem lässt sich durch Unsicherheit und einen Mangel an Transparenz beschreiben. Zu den wesentlichen Prämissen für eine breitenwirksame Adoption von Cloud-Computing am Markt zählen die Bewältigung gegenwärtiger Vertrauensprobleme im Cloud-Computing und die Förderung von transparentem Informationsaustausch zwischen Cloud-Service-Nutzern und Cloud-Service-Providern. Die Zertifizierung von Cloud-Services durch eine unabhängige Zertifizierungsinstitution kann den Mangel an Transparenz, Vertrauen und Akzeptanz adressieren (Sunyaev/Schneider 2013).

Der Prozess zur Zertifizierung eines Cloud-Services sollte die Prüfung des Rechenzentrums vor Ort sowie umfangreiche Evaluationen der Verträge und Services umfassen. Um eine solche Zertifizierung zu erhalten, sollte ein Cloud-Service spezifische Qualitätsvorgaben einschließlich vertraglicher Anforderungen (z. B. Service Level Agreements), gesetzlicher Vorgaben (z. B. Datenschutzrichtlinien) und Sicherheitserfordernisse (z. B. Verschlüsselung) erfüllen (siehe dazu Kapitel 12). Zusätzlich können industriespezifische Anforderungen gelten (z. B. im Bereich des Gesundheitswesens). Bewertungen der Servicequalität durch die Kunden eines Providers oder durch unabhängige Dritte können das Vertrauen und die Akzeptanz potenzieller Kunden in einen Service verbessern. Dieser Ansatz wurde erfolgreich in anderen Dienstleistungsgewerben angewandt, z. B. in den Bereichen Handel, Medien und Unterhaltung (Dellarocas 2003). Eine Zertifizierung ist besonders in den folgenden beispielhaften Szenarien hilfreich:

Sicherheit und Vertrauen. Die Implementierung von Cloud-Computing erzeugt weitere Herausforderungen in Bezug auf IT-Sicherheit. Neben tech-

1 Aufbauend auf der bereits im wissenschaftlichen Kontext von Sunyaev/Schneider (2013) erfolgten Veröffentlichung zum Thema dieses Abschnitts werden nachfolgend die wesentlichen Aspekte kurz zusammengefasst.

nischen Herausforderungen, müssen Kunden Vertrauen in die Sicherheit und Verlässlichkeit eines Services haben, um eine Nutzung zu fördern. Beispielsweise beim Onlinebanking oder Onlineshopping sind SSL-Zertifikate, welche von Zertifizierungsstellen ausgegeben werden, ein verbreitetes Vorgehen zur Verifizierung der Glaubwürdigkeit einer Webseite und zur Förderung des Vertrauens von Kunden. Sogenannte ‚Extended Validation‘ SSL-Zertifikate unterscheiden sich in der Struktur oder Kryptographie nicht von anderen (günstigeren) SSL-Zertifikaten, verlangen jedoch umfangreiche Identitätsprüfungen der anfragenden Organisation. Dementsprechend ist die Online-transaktion selbst nicht sicherer (bezogen auf die Verschlüsselung), aber die Zertifizierung wird dem Nutzer auffälliger präsentiert und die umfangreiche Validierung fördert die wahrgenommene Vertrauenswürdigkeit der Webseite.

Im Zusammenhang mit Cloud-Computing kann eine Zertifizierung durch eine unabhängige Zertifizierungsstelle das Vertrauen auf dieselbe Weise verbessern wie im Bereich von Onlinebanking und Onlineshopping. Neben der Identität des Providers kann ein Cloud-Zertifikat die Sicherheit der Infrastruktur und die IT-Sicherheitsmaßnahmen des Cloud-Service-Providers evaluieren. Wir erachten die Zertifizierung der Services von großen Infrastruktur-, Plattform- und Software Providern als besonders wichtig, da diese Provider als Knotenpunkte für enorme Datenmengen fungieren. Somit betreffen Sicherheitslücken oder Systemausfälle bei diesen großen Providern eine Vielzahl von Cloud-Service-Nutzern.

Rechtskonformität und Datenschutz. Aktuelle Diskussionen um gesetzliche Konflikte zwischen dem United States Patriot Act und der europäischen Datenschutzdirektive (95/46/EC) verstärken die Notwendigkeit von gesetzlich konformen Cloud-Services. Zudem haben einzelne Mitgliedsstaaten der EU die sechszehn Jahre alte Datenschutzdirektive auf verschiedenste Weise implementiert. Als Konsequenz müssen sich Cloud-Service-Provider mit 27 verschiedenen Regelungen auseinandersetzen, um alle Datenschutzgesetze der 27 EU-Mitgliedsstaaten einzuhalten. Die Datenschutz-Grundverordnung der EU soll hier Abhilfe schaffen, da es bei der Grundverordnung den Mitgliedsstaaten nicht möglich ist, die Vorgaben durch nationale Regelungen zu verändern (Briegleb 2013). Die Implementierung eines Zertifizierungsrah-

menwerks mit klaren Richtlinien für Datenschutz und gesetzliche Compliance von Cloud-Services kann Provider bei Entwurf und Implementierung von konformen Cloud-Services unterstützen. Cloud-Service-Zertifizierungen, die die Einhaltung von solch einem gesetzlichen und datenschutzrechtlichen Framework prüfen, können Nutzer bei der Einführungsentscheidung unterstützen, da sie sich auf die laufende gesetzliche Einhaltung von zertifizierten Cloud-Services verlassen können. Gleichmaßen können sich Software-as-a-Service-Provider bei der Wahl eines Plattform- oder Infrastruktur-Providers, welche die nationalen oder industriespezifischen Anforderungen ihrer Kunden einhalten müssen, auf Cloud-Service-Zertifizierungen stützen.

Transparenz. Als Folge der Finanz- und Wirtschaftskrise ab 2007 haben viele Kunden ihr Vertrauen in die Bankenindustrie verloren. Risikoreiche, komplexe und intransparente Finanzprodukte (z. B. durch Hypotheken gesicherte Wertpapiere) wurden im Kapitalmarkt als angeblich sichere Investitionen platziert. Überträgt man diese Situation auf Cloud-Services, wissen Nutzer häufig nicht einmal, dass sie einen Cloud-Service nutzen, geschweige denn, wo ihre Daten verarbeitet und gespeichert werden. Ein Software-as-a-Service-Provider in Deutschland könnte einen Cloud-Service bereitstellen, der Ressourcen verschiedener Cloud-Services in Europa, Asien und Nordamerika integriert. Genauso ist zu beobachten, dass immer mehr lokale Anwendungen auf Cloud-Services zurückgreifen, um z. B. Datensicherungen durchzuführen, ohne dass sich der Nutzer darüber im Klaren ist. Ein Provider könnte einen Service innerhalb einer Plattform-as-a-Service-Umgebung in den Vereinigten Staaten implementieren, welche wiederum Datenbanken eines Infrastructure-as-a-Service-Providers in Irland nutzt und Rechenleistung eines Cloud-Marktplatzes wie Spotcloud einsetzt (ein Marktplatz für Cloud-Service-Provider, um ungenutzte Cloud-Kapazitäten zu verkaufen). Cloud-Nutzer werden einen Vertrag mit dem deutschen Provider abschließen und mit diesem in der Annahme interagieren, dass die strengen deutschen Datenschutzbestimmungen zutreffen. Aber tatsächlich ist es völlig undurchsichtig, wo die Daten verarbeitet und gespeichert werden. Die Aufklärung über die Wechselbeziehungen eines Services als Teil der Zertifizierungsanforderungen könnte komplexe Providerkooperationen und Interaktionen klarstellen.

5.2 Herausforderungen bei der Zertifizierung von Cloud-Services

Zertifizierungen von Cloud-Services können Unsicherheiten bei deren Adoption beheben und dadurch Nutzer bei der Adoptionsentscheidung unterstützen. Jedoch bringt die Einhaltung von Zertifizierungsstandards Herausforderungen mit sich, die berücksichtigt werden müssen:

Insbesondere kleine und mittelständische Cloud-Service-Provider könnten unter Wettbewerbsnachteilen leiden, da sie nicht immer ein ausreichendes Budget zur Verfügung haben, um ihre Cloud-Services zu zertifizieren. Aus diesem Grund sollten Zertifizierungen einerseits erschwinglich sein und andererseits umfassend genug sein, insbesondere in Hinblick auf Vor-Ort-Auditierung und Umfang der Zertifizierung.

Die Anforderungen zum Erhalt von Zertifizierungen können dazu führen, dass kleine Cloud-Service-Provider ihre Services nicht in einer kosteneffizienten Weise anbieten können. Im Gegensatz dazu differenzieren sich große Cloud-Service-Provider durch die Ermöglichung signifikanter Kosteneinsparungen und hoher Ressourcenelastizitäten im Wettbewerb. Daher können große Cloud-Service-Provider die Auditierung ihrer physischen Einrichtungen, Services und Prozesse vernachlässigen und ein ähnliches Ergebnis einer Zertifizierung allein durch ihren Ruf erreichen. Dahingegen werden kleine Cloud-Service-Provider zur Zertifizierung gedrängt, damit sie sich am Markt differenzieren können. Dies führt zu einem Wettbewerbsnachteil für kleine Cloud-Service-Provider.

Zertifizierungen müssen das Gleichgewicht zwischen ihrer Komplexität und der Verwendbarkeit aufrechterhalten. Wenn sehr strikte Anforderungen durch die Zertifizierung gefordert werden, kann sie Innovationen behindern. Dies ist insbesondere im Kontext von Cloud-Computing kritisch, da innovative und wegweisende Services sowie kurze Innovationszyklen zu den Hauptvorteilen von Cloud-Computing gehören. Um den schnellen Innovationszyklen der IT-Industrie gerecht zu werden, muss ein Zertifizierungsrahmenwerk flexibel und adaptionsfähig sein. Aufgrund der unterschiedlichen Cloud-Service-Angebote besteht bei einem verständlichen und weit anwendbaren Zertifizierungsrahmenwerk das Risiko, dass dieses in eine Sammlung von allgemeingültigen und übergreifenden Standards konvergiert.

Dies würde jedoch den gewünschten Ergebnissen einer Zertifizierung widersprechen.

Um die Akzeptanz von Zertifizierungen zu gewährleisten, müssen vertrauenswürdige Zertifizierungsinstitutionen beauftragt werden. Damit eine ausreichende Glaubwürdigkeit der zertifizierten Cloud-Services gegeben ist, müssen sowohl Entscheidungsträger der Cloud-Service-Provider als auch -Nutzer der Zertifizierungsautorität vertrauen.

Existierende Cloud-Service-Zertifizierungen sind für einen definierten Zeitraum gültig (üblicherweise für zwei Jahre) und spiegeln nur eine Zeitpunktaufnahme über die Situation vor und während der Zeit der Auditierung wider. Ob die zertifizierten Kriterien während des Gültigkeitszeitraums der Zertifizierung weiterhin gültig sind, kann nicht sichergestellt werden. Durch die Implementierung (teil-)automatisierter Zertifizierungsprozesse für ein kontinuierliches Monitoring der zertifizierten Cloud-Services, zusätzlich zu periodischen Vor-Ort-Audits (beispielsweise zweijährig), kann ein konstantes Qualitätslevel der Services überwacht und bestätigt werden. Reguläre Vor-Ort-Audits können dies aus Gründen mangelnder Wirtschaftlichkeit nicht realisieren.

5.3 Fazit

Betrachtet man die aktuelle Situation des Cloud-Computing-Marktes, so müssen bestehende Hindernisse für eine effektive Entwicklung und Verbreitung von innovativen Cloud-Services adressiert werden. Eine standardisierte Zertifizierung von Cloud-Services zielt darauf ab, Vertrauen zu etablieren und die Akzeptanz von Cloud-Computing zu erhöhen. Sowohl kleine, mittlere und große Cloud-Service-Provider als auch Cloud-Service-Nutzer können von Cloud-Service-Zertifizierungen profitieren. Kleinere und regionale Cloud-Service-Provider können durch praxisorientierte und marktrelevante Zertifizierungen für ihre Cloud-Services im Markt hervorstechen und einen größeren Kundenstamm gewinnen. Weiterhin können mittelgroße Cloud-Service-Provider gesetzeskonforme und kundenspezifische Anforderungen implementieren, wozu große Service-Provider aufgrund ihrer hoch standardisierten Lösungen nicht immer in der Lage sind. Durch die Bekanntmachung von hochwertigen Eigenschaften, wie bspw. die Transparenz ihrer Services,

Rechtssicherheit, zuverlässige Service-Levels und eine hohe Sicherheit ihrer Rechenzentren, können große Provider andere SaaS-Provider überzeugen, ihre IaaS- oder PaaS-Services zu nutzen, anstatt eigene interne Infrastrukturen zu betreiben. Durch den Entwurf von vertrauenswürdigen Cloud-Service-Zertifizierungen können Cloud-Nutzer Risiken und Vorteile für individuelle Cloud-Services identifizieren und bei ihrer Adoptionsentscheidung berücksichtigen.

Organisationen wie bspw. die Cloud Security Alliance und EuroCloud haben erste Zertifizierungsprogramme für Individuen, Provider oder Services entwickelt (vgl. Kapitel 12). Die Zeit wird zeigen, ob Zertifizierungen die Herausforderungen bezüglich Transparenz, Vertrauen und Akzeptanz senken können und ob aktuelle Provider den aufgeführten Herausforderungen der Zertifizierung gewachsen sind. Ebenso wird sich herausstellen, ob Cloud-Service-Nutzer bereit sind, einen Aufpreis für zertifizierte Cloud-Services zu bezahlen (Lansing/Sunyaev 2013). Die Einführung einer Zertifizierung für Cloud-Services kann ein Weg sein, die momentanen Herausforderungen im Cloud-Computing zu adressieren, und ist ein Schritt vorwärts zu einem vertrauensvolleren und transparenteren Cloud-Computing-Ökosystem.

5.4 Literaturverzeichnis

- Briegleb, V. (2013):** EU-Parlament gibt grünes Licht für Datenschutzreform. <http://heise.de/-1983124>, zugegriffen am 28.07.2014.
- Dellarocas, C. (2003):** The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms. In: *Management Science*, Vol. 49 (2003) No. 10, S. 1407–1424.
- Lansing, J.; Sunyaev, A. (2013):** Does Pain Result in Gain? Assessing Cloud Service Certifications' Effectiveness. Präsentiert auf der 34th International Conference on Information Systems, Mailand, Italien.
- Sunyaev, A.; Schneider, S. (2013):** Cloud Services Certification. In: *Communications of the ACM*, Vol. 56 (2013) No. 2, S. 33–36.

6 Vertrauensproblematiken im Cloud-Computing-Umfeld

L. Gebauer, M. Söllner, J.M. Leimeister

6.1 Die Bedeutung von Vertrauen im Cloud-Computing-Umfeld

Vier Jahre in Folge war Cloud-Computing, gemäß der jährlich durchgeführten BITKOM-Umfrage „*IT Trends des Jahres*“, das wichtigste Thema in der IKT-Branche (BITKOM 2010, 2011, 2012, 2013). Cloud-Computing wird gehandelt als „*long-held dream of computing as a utility*“ (Armbrust et al. 2010, S. 50), der sich endlich bewahrheitet. Es bietet Unternehmen eine Lösung, um hohe Wartungskosten zu senken, die Auslastung und Nutzung der Hardwareressourcen zu optimieren, den internen Energieverbrauch zu verringern sowie agiler auf geänderte Geschäftsanforderungen zu reagieren (IDC 2011). Dennoch zeigen Studien und Umfragen, dass Cloud-Computing im B2B-Bereich eher zurückhaltend genutzt wird (Golkowsky/Vehlow 2011; IDC 2011). Vor allem der Mittelstand hat noch enormen Aufholbedarf (BITKOM 2014).

Die bisherige Forschung zeigt, dass eine Zurückhaltung bei der Akzeptanz und Nutzung neuer Technologien sowohl auf einen Mangel an Vertrauen (z.B. Söllner/Leimeister 2012; Gefen et al. 2003) als auch auf die Wahrnehmung von Risiken (z.B. Featherman/Pavlou 2003; Luo et al. 2010) zurückzuführen ist. Vertrauen und Risiko sind zwei voneinander unabhängige Wahrnehmungsgrößen (Joubert/Belle 2009), die sich dennoch gegenseitig beeinflussen. Das Maß an entgegengebrachtem Vertrauen wirkt sich positiv auf die Bereitschaft Risiken einzugehen aus (z.B. Glover/Benbasat 2010).

Auch im Zuge der Akzeptanz und Nutzung von Cloud-Computing bestehen Risiken und Hemmnisse seitens der (potenziellen) Kunden (z.B. Gebauer et al. 2012; Armbrust et al. 2010; Ackermann et al. 2011), wobei die Einschätzung der Vertrauenswürdigkeit als ein erfolgskritischer Faktor bei der Auswahl des Cloud-Computing-Anbieters gesehen wird (Repschlaeger et al. 2012). Nach dem Trendforscher Sven Gábor Jánszky ist Cloud-Computing ein Geschäft des Vertrauens, denn „*die Frage, welchem Unternehmen der*

Kunde erlaubt, seine Daten zu verwalten, seine Recommendation-Systeme anzubieten und seine elektronischen Assistenten zu installieren, wird zur strategisch wichtigsten Marktmacht“ (Jánszky 2012, S. 4). Dieser Kommentar bestärkt, dass Vertrauen bzw. Vertrauenswürdigkeit zu einem der wichtigsten Erfolgsfaktoren von Cloud-Computing-Anbietern avancieren wird.

Um sowohl die Akzeptanz als auch die Nutzung von Cloud-Computing im B2B-Bereich, speziell im deutschen Mittelstand, zu erhöhen, sollten dementsprechend die Anbieter von Cloud-Computing-Diensten die Nutzungshemmnisse der (potenziellen) Kunden bestmöglich adressieren und gleichzeitig Maßnahmen zur Vertrauensförderung einsetzen. Um die Cloud-Computing-Anbieter bei dieser Aufgabe zu unterstützen, werden in den nachfolgenden Abschnitten die Nutzungshemmnisse für Cloud-Computing zusammenfassend erläutert. Anhand der verschiedenen Komponenten von Vertrauen (siehe Abschnitt 2.3.3) wird abgeleitet, zu welchen Entitäten im Cloud-Computing-Umfeld die (potenziellen) Kunden Vertrauen aufbauen müssen. Abschließend werden die herausgestellten Nutzungshemmnisse für Cloud-Computing im B2B-Bereich den identifizierten Vertrauensbeziehungen zugeordnet.

6.2 Nutzungshemmnisse im Cloud-Computing-Umfeld

Um einen umfassenden Überblick über die Nutzungshemmnisse gegenüber Cloud-Computing im B2B-Bereich zu geben, wurden die Erkenntnisse von drei verschiedenen Überblicksartikeln (Armbrust et al. 2010; Ackermann et al. 2011; Marston et al. 2011) zusammengefasst. Die Überblicksartikel betrachten die Nutzungshemmnisse aus verschiedenen Perspektiven. Armbrust et al. (2010) zeigen generelle Hindernisse bei der Nutzung von Cloud-Computing auf, Ackermann et al. (2011) betrachten die Risiken aus technischer Perspektive und Marston et al. (2011) aus betriebswirtschaftlicher Sicht.

Die anhand der Überblicksartikel gewonnenen Erkenntnisse wurden miteinander auf Überschneidungen und Unterschiede verglichen, kategorisiert und in einer Tabelle zusammengefasst ([Tabelle 1](#)). Im Ergebnis wurden zwölf

Tabelle 1: Hemmnisse für die Nutzung von Cloud-Computing im B2B-Bereich
(Quelle: Gebauer et al. 2012)

Hemmnis	Beschreibung	Quelle
Diskontinuität/ Ausfall des Dienstes	Störungen des Betriebsalltags sowie von betriebsnotwendigen Anwendungen durch temporäre Unterbrechungen oder komplette Ausfälle des Dienstes	A, B, C
System- angriffe	Gefährdung der Informationssicherheit durch externe Systemangriffe, Anbieter verantwortlich für Bereitstellung und Funktionsfähigkeit geeigneter Sicherheitstechniken	A
Netzwerk- störungen	Störungen durch nicht ausreichende Bereitstellung von Netzwerkbandbreite (z.B. Schwankungen, Ausfälle, zu lange Ladezeiten bei der Bearbeitung von Prozessen)	A, B
Begrenzte Skalier- barkeit	Begrenzte oder zu langsame Adaption des Dienstes an aktuelle Leistungsanforderungen vom Kunden (z.B. flexibler Bedarf an Speicherplatz und Rechenleistung)	A, B
Daten- übertragung	Zeit- und kostenintensive Übertragung großer Datenmengen (z.B. im Terabyte-Bereich) über das Netzwerk	B
Mangelnde Daten- integrität	Mangelnde Transparenz hinsichtlich der Datenübertragung, Datenmodifikation und Zugriffshierarchien. Anbieter verantwortlich für korrekte Identifizierung, Authentifizierung und Autorisierung von Nutzern zur Verhinderung von Datenmissbrauch und unautorierten Zugriffen	A, B
Abhängig- keit vom Anbieter	Datenverteilung auf mehrere Cloud-Computing-Anbieter nicht möglich, starke Anwenderabhängigkeit vom Anbieter, Gefahren für Anwender: willkürliche Preisfestsetzung, Reliabilitätsprobleme, Anbieterbankrott, etc.	B
Abhängig- keit von anderen Nutzern	Viele Kunden nutzen die gleiche Cloud, wobei Fehlverhalten von Nutzern auch Auswirkungen für die restlichen Nutzer haben kann, z.B. verstößt ein Cloud-Computing-Nutzer gegen geltendes Recht, sind staatliche Behörden befugt den gesamten Server zu beschlagnahmen	B

Hemmnis	Beschreibung	Quelle
Kontroll-möglich-keiten	Mangelnde Kontrolle über Speicherort, Updates und sonstige automatische Wartungsarbeiten	A, B, C
Mangelnde Reliabilität	Mangelndes Vertrauen, ob das System gemäß den Nutzererwartungen operiert (z.B. ungenügende Softwarequalität, unzureichende Leistung)	A, C
Mangelnde rechtliche Standards	Keine einheitlichen Standards, Gesetze und Verträge hinsichtlich Datenschutz, Datensicherheit, Datenzugriff, Datenlokation, Anbieterwechsel, Anbieterbankrott, etc.	A, B, C
Gefährdung interne IT	Gefährdung der internen IT in Bezug auf Datensicherheit, Kompatibilität und Jobsicherheit	C
<i>Anmerkung: Quelle A entspricht Ackermann et al. (2011), Quelle B entspricht Armbrust et al. (2010) und Quelle C entspricht Marston et al. (2011).</i>		

Kategorien an Nutzungshemmnissen gegenüber Cloud-Computing im B2B-Bereich identifiziert (Gebauer et al. 2012). In der ersten Spalte der Tabelle wurden die Nutzungshemmnisse stichwortartig zusammengefasst und in der zweiten Spalte detailliert beschrieben. In der dritten Spalte findet sich die Zuordnung, in welchen Quellen weitere Informationen zu den entsprechenden Hemmnissen zu finden sind.

6.3 Vertrauensbeziehungen im Cloud-Computing-Umfeld

Vertrauen setzt sich aus drei verschiedenen Komponenten zusammen (vgl. Leimeister et al. 2005): Vertrauensbereitschaft, interpersonelles Vertrauen und Systemvertrauen (siehe Kapitel 2). Vertrauen in komplexe technische Systeme wird als Netzwerk verschiedener Vertrauensbeziehungen verstanden (Muir 1994), da an der Leistungserbringung verschiedenste Entitäten beteiligt sind und gegenseitige Vertrauensbeziehungen etabliert werden müssen (z.B. Söllner/Leimeister 2012). Als Entitäten werden in der Informatik Objekte bezeichnet, die eindeutig identifiziert werden können, wie eine Person, ein Unternehmen, ein Ereignis, ein Zustand, eine Sache oder Gegenstand (Chen 1976). Ziel ist, anhand der verschiedenen Komponenten von Vertrau-

en, ein Vertrauensnetzwerk für das Cloud-Computing-Umfeld zu entwickeln, um herauszustellen, zu welchen Entitäten ein (potenzieller) Cloud-Computing-Kunde Vertrauen aufbauen muss.

Die Komponente *Vertrauensbereitschaft* umfasst die grundsätzliche Bereitschaft Anderen zu vertrauen. Diese entwickelt sich sowohl durch Erfahrungen im alltäglichen Leben als auch durch Persönlichkeitsmerkmale und wird als eine relativ stabile Persönlichkeitseigenschaft betrachtet (Rotter 1980). Die Vertrauensbereitschaft hat einen Einfluss auf die Ausprägung von Vertrauen (z.B. Kim et al. 2008; Joubert/Belle 2009) und sogar auf die Nutzungsabsicht (z.B. Luo et al. 2010). Da diese Vertrauenskomponente als stabile Persönlichkeitseigenschaft anzusehen ist, kann diese durch Maßnahmen des Cloud-Computing-Anbieters nicht adressiert werden und wird deshalb im Weiteren nicht tiefergehend betrachtet.

Die Vertrauenskomponenten *interpersonelles Vertrauen* und *Systemvertrauen* hingegen sind durch den Anbieter gestaltbar (Joubert/Belle 2009; Söllner/Leimeister 2012; Leimeister et al. 2005). Diese machen deutlich, dass der (potenzielle) Cloud-Computing-Nutzer eine Vertrauensbeziehung zum Cloud-Computing-Anbieter als Person (interpersonelles Vertrauen) und eine Vertrauensbeziehung zur Technik selbst (Systemvertrauen) aufbauen muss (vgl. Gebauer et al. 2012). Daraus ergeben sich die ersten beiden Entitäten des Vertrauensnetzwerks im Cloud-Computing-Umfeld ([Abbildung 1](#)).

Im Cloud-Computing-Umfeld bestehen noch zwei weitere Besonderheiten, die es bei der Entwicklung des Vertrauensnetzwerks zu berücksichtigen gilt. Zum einen können die (potenziellen) Cloud-Computing-Nutzer den Dienst nur zuverlässig nutzen, wenn eine ausreichende und dauerhafte Internetverbindung sichergestellt ist. Dementsprechend ist die dritte Entität, zu der Cloud-Computing-Nutzer eine Vertrauensbeziehung aufbauen müssen, der ausgewählte Netzbetreiber. Unter Netzbetreibern werden die verschiedenen Internetanbieter, die am Markt existieren, zusammengefasst. Cloud-Computing-Dienste werden über das Internet bereitgestellt, weshalb den Netzbetreibern eine erfolgskritische Rolle zukommt. Gelingt es dem Netzbetreiber des Cloud-Computing-Nutzers nicht, kontinuierlich die geforderte Bandbreite zur Verfügung zu stellen, kann dies zu Diskontinuitäten bis hin zu

Abbildung 1: Vertrauensbeziehungen im Cloud-Computing-Umfeld
(Quelle: Gebauer et al. 2012)

kompletten Ausfällen führen. Dadurch ist die Sicherheit der Betriebsabläufe durch die Nutzung von Cloud-Computing gefährdet. Die Vertrauensbeziehung des Cloud-Computing-Kunden zu seinem Netzbetreiber bezieht sich darauf, dass dieser stets eine ausreichende Bandbreite zur Verfügung stellt, um Störungen des Betriebsalltages auszuschließen.

Die zweite Besonderheit im Cloud-Computing-Umfeld besteht darin, dass verschiedene Nutzer auf ein und die gleiche Cloud zugreifen können. Demzufolge besteht bei Fehlverhalten oder rechtswidrigen Handlungen von anderen Cloud-Computing-Nutzern die Gefahr, dass die Nutzung des Cloud-Computing-Dienstes unvermittelt durch die Behörden für alle Nutzer gesperrt werden kann (siehe Kapitel 18). Dies hat zur Folge, dass (potenzielle)

Cloud-Computing-Nutzer ebenfalls eine Vertrauensbeziehung zu den anderen Cloud-Computing-Nutzern aufbauen müssen. Dementsprechend muss sich die Vertrauensbeziehung des Cloud-Computing-Nutzers zu den anderen Nutzern darauf beziehen, dass diese ebenfalls hinreichend Verantwortung für einen reibungslosen Zugriff tragen.

Zusammenfassend müssen (potenzielle) Cloud-Computing-Nutzer vier Vertrauensbeziehungen aufbauen (Gebauer et al. 2012): zum Cloud-Computing-Anbieter, zum technischen System, zum ausgewählten Netzbetreiber und schließlich auch zu den anderen Nutzern der Cloud ([Abbildung 1](#)).

6.4 Zuordnung der Nutzungshemmnisse zu den Vertrauensbeziehungen

In diesem Abschnitt werden nun die identifizierten Nutzungshemmnisse den Entitäten des Vertrauensnetzwerks zugeordnet ([Abbildung 2](#)). Die überwiegende Anzahl der Nutzungshemmnisse können direkt durch den Cloud-Computing-Anbieter adressiert werden. Dieser kann mit Hilfe geeigneter Maßnahmen versuchen, die Hemmnisse der (potenziellen) Cloud-Computing-Anwender abzubauen. Zum Beispiel, indem dieser detailliert darlegt, welche Schutzmaßnahmen vor *Systemangriffen* durchgeführt werden, die Anwender rechtzeitig über Updates und dadurch bedingte Betriebsstörungen informiert oder die Nutzer über die *rechtlichen Standards* aufklärt.

Der Cloud-Computing-Anbieter ist ebenfalls dafür verantwortlich, die Funktionsfähigkeit der von ihm angebotenen Cloud-Computing-Technik sicherzustellen. Dennoch wird die Cloud-Computing-Technik als eigene Entität betrachtet, weil der (potenzielle) Cloud-Computing-Kunde unabhängig vom Anbieter auch der Cloud-Computing-Technik an sich vertrauen muss. Gegenüber der Technik bestehen die Nutzungshemmnisse *Diskontinuität/ Ausfall des Dienstes* und *mangelnde Reliabilität*. Ein wesentliches Nutzungshemmnis gegenüber Cloud-Computing besteht darin, dass der Betriebsalltag enorm beeinträchtigt ist, wenn die Bereitstellung gestört ist oder gar ausfällt, da betriebsnotwendige und geschäftskritische Anwendungen nicht zur Verfügung stehen. Auch bestehen generelle Bedenken, ob die Cloud-Computing-Technik gemäß den Nutzererwartungen operiert.

Abbildung 2: Vertrauensbeziehungen im Cloud-Computing-Umfeld und Zuordnung der Nutzungshemmnisse (Quelle: Gebauer et al. 2012)

Neben den Cloud-Computing-Anbietern wird das Nutzungshemmnis *mangelnde rechtliche Standards* zusätzlich den Cloud-Computing-Nutzern zugeordnet, da diese in der eigenen Verantwortung stehen, sich über die aktuelle Rechtslage und die eigenen rechtlichen Pflichten im Zuge der Nutzung von Cloud-Computing zu informieren (siehe Kapitel 15 bis 18). Dennoch kann der Cloud-Computing-Anbieter den (potenziellen) Kunden proaktiv bei der Schaffung der rechtlichen Informiertheit und Sicherstellung von rechtmäßigem Verhalten unterstützen. Zudem sollte der (potenzielle) Cloud-Computing-Anwender vor der Nutzung sicherstellen, dass die Implementierung von Cloud-Computing-Diensten mit der bestehenden IT-Infrastruktur kompatibel ist und sich diesbezüglich mit dem Cloud-Computing-Anbieter abstimmen.

Wie schon erwähnt, bestehen ebenfalls gegenüber den anderen Cloud-Computing-Nutzern Nutzungshemmnisse, da sich die Anwender eine Cloud teilen. Die Konsequenzen des Fehlverhaltens anderer Cloud-Computing-Nutzer können Auswirkungen auf die gesamte Cloud-Computing-Nutzerschaft haben. Speichert ein Cloud-Computing-Nutzer beispielsweise rechtswidrige Inhalte, sind die staatlichen Behörden befugt, die Cloud-Computing-Server als Beweismittel zu beschlagnahmen (siehe Kapitel 18). Auch kann es fahrlässig oder vorsätzlich passieren, dass Cloud-Computing-Nutzer die Server mit Schadprogrammen infizieren, die ebenfalls Konsequenzen für die gesamte Nutzerschaft haben (siehe Kapitel 17).

Durch diese Zuordnung wird deutlich, mit welchen Nutzungshemmnissen sich (potenzielle) Cloud-Computing-Kunden auseinander setzen und welche Entität diese prinzipiell zu verantworten hat. Auch wenn der Cloud-Computing-Anbieter nicht alle Hemmnisse auslöst, sollte dieser dennoch versuchen, alle Hemmnisse der (potenziellen) Cloud-Computing-Kunden zu adressieren, um mit Hilfe von vertrauensunterstützenden Maßnahmen sowohl das Vertrauen als auch die Akzeptanz zu fördern.

6.5 Zusammenfassung

Mit dem Kapitel „Vertrauensproblematiken im Cloud-Computing-Umfeld“ wurde ein Überblick geschaffen, welche Besonderheiten sich in Bezug auf Vertrauen im Cloud-Computing-Umfeld ergeben. Der Aufbau von Vertrauen und der Abbau von Nutzungshemmnissen können als erfolgskritische Faktoren für die Akzeptanz und die Nutzung von Cloud-Computing angesehen werden.

Daher wurden in diesem Kapitel die Hemmnisse gegenüber der Nutzung von Cloud-Computing-Diensten zusammengetragen und kategorisiert. Insgesamt wurden zwölf verschiedene Kategorien von Nutzungshemmnissen erarbeitet. Zudem wurde aufgezeigt, dass der (potenzielle) Cloud-Computing-Anwender aufgrund der Besonderheiten im Cloud-Computing-Umfeld nicht nur zu dem Cloud-Computing-Anbieter, sondern zu drei weiteren Entitäten (Cloud-Computing-Technik, Netzbetreiber und anderen Cloud-Computing-Nutzern) Vertrauen aufbauen muss.

Abschließend wurden die identifizierten Kategorien an Nutzungshemmnissen den entsprechenden Entitäten des Vertrauensnetzwerks zugeordnet, um aufzuzeigen, welche Entität das Hemmnis auslöst bzw. zu verantworten hat. Auch wenn eine derartige Zuordnung der Nutzungshemmnisse vorgenommen wurde, liegt es beim Cloud-Computing-Anbieter, diesen entgegenzuwirken und das Vertrauen in den angebotenen Cloud-Computing-Dienst zu fördern.

6.6 Literaturverzeichnis

- Ackermann, T.; Miede, A.; Buxmann, P.; Steinmetz, R. (2011):** Taxonomy of Technological IT Outsourcing Risks: Support for Risk Identification and Quantification. Präsentiert auf der 19th European Conference on Information Systems (ECIS), Helsinki, Finnland.
- Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; Zaharia, M. (2010):** A view of cloud computing. In: Communications of the ACM, Vol. 53 (2010) No. 4, S. 50-58.
- BITKOM (2010):** IT- und Telekommunikations-Trends 2010. http://www.bitkom.org/files/documents/BITKOM-Presseinfo_IT-Trends_2010_-_13_01_2010.pdf,
zugegriffen am 28.07.2014.
- BITKOM (2011):** Cloud Computing ist erneut IT – Trend des Jahres. http://www.bitkom.org/files/documents/BITKOM-Presseinfo_IT-Trends_2011_-_18_01_2011.pdf,
zugegriffen am 28.07.2014.
- BITKOM (2012):** Die Hightech-Trends des Jahres 2012 http://www.bitkom.org/files/documents/BITKOM-Presseinfo_IT-Trends_des_Jahres_18_01_2012.pdf,
zugegriffen am 28.07.2014.
- BITKOM (2013):** Die wichtigsten Hightech – Themen 2013 http://www.bitkom.org/files/documents/BITKOM_Presseinfo_Hightech-Trends_16_01_2013.pdf,
zugegriffen am 28.07.2014.
- BITKOM (2014):** Nutzung von Cloud Computing in Unternehmen wächst. http://www.bitkom.org/files/documents/Presseinfo_BITKOM_und_KPMG_zum_Cloud-Monitor_30_01_2014.pdf,
zugegriffen am 28.07.2014.
- Chen, P.P.-S. (1976):** The entity-relationship model – toward a unified view of data. In: ACM Transactions on Database Systems (TODS), Vol. 1 (1976) No. 1, S. 9-36.
- Featherman, M.S.; Pavlou, P.A. (2003):** Predicting e-services adoption: a perceived risk facets perspective. In: International Journal of Human-Computer Studies, Vol. 59 (2003) No. 4, S. 451-474.
- Gebauer, L.; Söllner, M.; Leimeister, J.M. (2012):** Hemmnisse bei der Nutzung von Cloud Computing im B2B-Bereich und die Zuordnung dieser zu den verschiedenen Vertrauensbeziehungen. Präsentiert auf der ConLife Academic Conference 2012, Köln, Deutschland.

- Gefen, D.; Karahanna, E.; Straub, D.W. (2003):** Trust and TAM in Online Shopping: An Integrated Model. In: MIS Quarterly, Vol. 27 (2003) No. 1, S. 51-90.
- Glover, S.; Benbasat, I. (2010):** A Comprehensive Model of Perceived Risk of E-Commerce Transactions. In: International Journal of Electronic Commerce, Vol. 15 (2010) No. 2, S. 47-78.
- Golkowsky, C.; Vehlow, M. (2011):** Cloud Computing im Mittelstand – Erfahrungen, Nutzen und Herausforderungen, PwC, Frankfurt am Main, Germany, 2011.
- IDC (2011):** Cloud Computing in Deutschland. http://www.idc.de/press/presse_mc_cloud2011.jsp, zugegriffen am 28.07.2014.
- Jánszky, S.G. (2012):** CloudComputing – Der unverstandene Megatrend. www.2bahead.com/uploads/media/2012-05-11_Trendanalyse_Der_unverstandene_Megatrend_Cloud.pdf, zugegriffen am 28.07.2014.
- Joubert, J.; Belle, J.-P.V. (2009):** The Importance of Trust and Risk in M-Commerce: A South African Perspective. Präsentiert auf der 13th Pacific Asia Conference on Information Systems, Hyderabad, Indien.
- Kim, D.J.; Ferrin, D.L.; Rao, H.R. (2008):** A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. In: Decision Support Systems, Vol. 44 (2008) No. 2, S. 544-564.
- Leimeister, J.M.; Ebner, W.; Krcmar, H. (2005):** Design, Implementation, and Evaluation of Trust-Supporting Components in Virtual Communities for Patients. In: Journal of Management Information Systems, Vol. 21 (2005) No. 4, S. 101-135.
- Luo, X.; Li, H.; Zhang, J.; Shim, J.P. (2010):** Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. In: Decision Support Systems, Vol. 49 (2010) No. 2, S. 222-234.
- Marston, S.; Li, Z.; Bandyopadhyay, S.; Zhang, J.; Ghalsasi, A. (2011):** Cloud computing – The business perspective. In: Decision Support Systems, Vol. 51 (2011) No. 1, S. 176-189.
- Muir, B.M. (1994):** Trust in automation: Part I. In: Ergonomics, Vol. 37 (1994) No. 11, S. 1905-1922.
- Repschlaeger, J.; Zarnekow, R.; Wind, S.; Turowski, K. (2012):** Cloud Requirements Framework: Requirements And Evaluation Criteria To Adopt Cloud Solutions. Präsentiert auf der 20th European Conference on Information Systems (ECIS), Barcelona, Spanien.
- Rotter, J.B. (1980):** Interpersonal trust, trustworthiness, and gullibility. In: American Psychologist, Vol. 35 (1980) No. 1, S. 1.
- Söllner, M.; Leimeister, J.M. (2012):** Opening up the Black Box: The Importance of Different Kinds of Trust in Recommender System Usage. Präsentiert auf der 72nd Academy of Management Annual Meeting, Boston, USA.

Teil D:
Unterstützungsbedarf
aus Sicht Cloud-anbietender
Unternehmen

7 Anforderungserhebung für eine Online-Community für Open Service Innovation im Cloud-Computing-Umfeld

M. Kunz, P. Ebel, J.M. Leimeister

7.1 Einleitung

Unsicherheiten auf Seiten möglicher Kunden gegenüber dem Cloud-Computing tragen wesentlich zur geringen Adaption dieser Dienstleistung und damit zur mangelnden Ausschöpfung ökonomischer Potenziale bei (Kunz et al. 2014). Dieser Umstand hängt u. a. damit zusammen, dass die Bedürfnisse zukünftiger Nutzer in den wenigsten Fällen in die Erstellung neuer Cloud-Computing-Services einfließen. Eine direkte Beteiligung der Nutzer an Innovationsprozessen und Neuentwicklungen von Cloud-Services stellt eine Möglichkeit zur Bekämpfung dieser Unsicherheiten dar (Leimeister 2012). Durch eine solche direkte Kooperation im Innovationsprozess können Bedürfnisse – vor allem im Hinblick auf Vertrauens- und Sicherheitsthemen – identifiziert und nutzergerechte Lösungen entwickelt werden. Solch eine interaktive Wertschöpfung im Innovationsprozess durch die Beteiligung (ausgewählter) Nutzer außerhalb des Unternehmens (Janzik 2012), die damit verbundene Erweiterung der Innovationsquellen und der Einbezug ihrer Ideen sowie Konzepte (Möslein/Neyer 2009) wird als „Open Innovation“ bezeichnet (siehe hierzu auch [Abbildung 1](#)).

Open Innovation bietet gegenüber dem herkömmlichen Innovationsprozess von Unternehmen (Closed Innovation) einige Vorteile. Dazu gehören u. a. eine Verkürzung der Innovationsdauer, eine Senkung der Innovationskosten, frühere oder bessere Absatzchancen, eine Erhöhung der Marktakzeptanz, eine Früherkennung neuer Technologietrends, ein Zugriff auf Bedürfnis- und Lösungsinformationen und eine Vergrößerung der Ideenbasis (Schaffert/Wieden-Bischof 2009).

Die Umsetzung des Open-Innovation-Ansatzes kann durch unterschiedliche Instrumente erfolgen. Beispielfhaft seien die Lead-User-Methode, Inno-

Abbildung 1: Closed Innovation vs. Open Innovation (In Anlehnung an Chesbrough (2003), Reichwald/Piller (2006), Ebner (2008))

vation Toolkits, Ideenwettbewerbe, die Broadcast-Search-Methode, Innovationstechnologien und Innovation-Communities genannt. Letzteres bietet den großen Vorteil, dass sehr viele Stakeholder orts- und zeitunabhängig in den Innovationsprozess eingebunden werden können. Die Interaktivität der Community, verbunden mit der Möglichkeit, erstellte Beiträge zu kommentieren und zu überarbeiten, trägt zu einer hohen Qualität der Beiträge bei. Die Kollaboration zwischen dem (zumindest potenziell) großen Kreis an Community-Mitgliedern bietet die Möglichkeit, viele unterschiedliche Sichtweisen zu integrieren und damit sämtliche Kundenbedürfnisse möglichst ganzheitlich zu erfassen. Im Rahmen des Projektes Value4Cloud wurde daher auf das Mittel der Open Innovation Community zurückgegriffen, um die Bedürfnisse zukünftiger Anwender möglichst frühzeitig zu identifizieren und neue, kundengerechte Cloud-Computing-Services zu entwickeln.

7.2 Theoretischer Hintergrund

7.2.1 Online-Communities

Der Begriff der Online-Community wurde in der Literatur bislang nicht einheitlich definiert. Dies ist zum einen der Tatsache geschuldet, dass die Online-Community aus der Perspektive unterschiedlicher Wissenschafts-

disziplinen erforscht wird (z.B. Psychologie, Verwaltungswissenschaften und Informatik) und jede Disziplin ein eigenes Begriffsverständnis hat (Leimeister/Krcmar 2004). Zum anderen wird der Begriff der Online-Community auch außerhalb der Wissenschaft vielfach als so genanntes „Buzzword“ verwendet, was ein einheitliches Begriffsverständnis zusätzlich erschwert (Leimeister/Krcmar 2004).

Unter einer Online-Community – nach Panten (2005) synonym zu einer virtuellen Community – versteht Leimeister et al. (2005) „(...) eine besondere Form von Gemeinschaft und damit eine Unterart sozialer Gruppen. Sie ist ein Zusammenschluss von Menschen mit einem Bedürfnis nach Information und Interaktion oder dem Bedürfnis, eine spezifische Rolle in einer Gemeinschaft auszufüllen. Grundlage und verbindendes Element ist eine gemeinsame Idee oder ein gemeinsames Ziel (...), das auf Basis von impliziten oder expliziten Verhaltensregeln verfolgt wird. Die Interaktion wird durch ein technisches Subsystem vermittelt und unterstützt, das den Aufbau von Vertrauen und ein Gemeinschaftsgefühl auch ohne unmittelbare physische Präsenz der Gemeinschaftsmitglieder ermöglicht. Zusammen mit dem technischen Subsystem, bestehend aus der Community-Plattform und der Infrastruktur des Internet, bilden Virtuelle Gemeinschaften damit interdependente sozio-technische Systeme.“ (S. 37).

7.2.2 Ideen-Communities

Ideen-Communities stellen eine Spezialform der Online-Communities dar. Ideen-Communities werden mit dem Ziel initiiert, Nutzern eine Plattform für die Äußerung und die gemeinsame Weiterentwicklung von unternehmensrelevanten Innovationsideen bereitzustellen (Leimeister/Krcmar 2004). Die Ideen-Community wird vom Unternehmen beobachtet. Es können darüber hinaus Bedürfnisinformationen von Kunden aufgenommen werden. Auf Basis von Fallstudien wurden folgende Merkmale von Ideen Communities identifiziert (Bretschneider 2012):

- Die Akteure sind Kunden des jeweiligen Unternehmens.
- Der thematische Bezugspunkt der Ideen Community sind Innovationsideen aus dem Produktumfeld.

- Die Schlüsselinteraktionen innerhalb der Ideen Community sind die Entwicklung und Bewertung von Innovationsideen sowie die Kollaboration bezüglich der Innovationsideen.
- Initiator oder Betreiber der Ideen Community ist ein einzelnes Unternehmen.
- Das Unternehmen ist der Nutznießer der Innovationsideen.
- Die Ideengeber werden nicht vergütet.
- Unter den Teilnehmern bestehen soziale Beziehungen.

Die Ideen-Community eignet sich für einen Innovationsprozess im Bereich des Cloud-Computings insbesondere deswegen, da mittels dieser erste Ideen zu neuen Cloud-Services generiert und bewertet werden können. Auf Basis dieser Ideen können Unternehmen letztlich ihre Produkte entwickeln oder diese durch die Online-Community bzw. ausgewählte Stakeholder weiterentwickeln lassen.

7.3 Anforderungserhebung

Der Funktionsumfang von Online Communities ist in vielen Fällen sehr einfach gehalten (Ebel et al. 2012). Beteiligte Mitglieder können lediglich eigene Ideen festhalten und in begrenztem Umfang mit anderen Mitgliedern über deren Weiterentwicklung diskutieren (Ebner et al. 2009; Leimeister et al. 2009). Eingereichte Ideen werden oftmals nicht über eine einfache Anfangsbeschreibung hinaus weiterentwickelt, sondern an die zuständigen Unternehmen weitergeleitet (Blohm et al. 2011). Dies kann jedoch Probleme auf Seiten des zuständigen Unternehmens nach sich ziehen, und zwar wenn eingereichte Ideen nicht mit dem Wissen und den Fähigkeiten von Mitarbeitern des jeweiligen Unternehmens kompatibel sind (Ahuja/Katila 2001) oder aufgrund des rudimentären Detailierungsgrades der Ideen von diesen Mitarbeitern nicht verstanden und umgesetzt werden können (Szulanski 1996; Ebel et al. 2012). Dies kann in vielen Fällen dazu führen, dass vielversprechende Ideen nicht umgesetzt oder die darin enthaltenen Kundenwünsche und Lö-

sungsansätze nicht adäquat adressiert werden und so für den eigentlichen Nutzer keinen Mehrwert stiften (Ebel et al. 2012).

Um dieses Risiko möglichst gering zu halten, wurden im Rahmen des Projektes neue Werkzeuge und Methoden entwickelt, die eine kollaborative Weiterbearbeitung von Ideen über eine Online-Community-Plattform ermöglichen sollen. Der größte Nutzen eines solchen Konzeptes kann dabei in der verbesserten Internalisierung von vielversprechenden Ideen im Unternehmen und der signifikanten Weiterentwicklung der einzelnen Serviceideen gesehen werden (Ebel et al. 2012). Dies führt letztlich zu einer Ausweitung des Open-Innovation-Ansatzes über die frühen Phasen der Ideengenerierung hinaus.

Dazu sollen im Folgenden die wesentlichen Grundlagen zur Unterstützung dieses kollaborativen Ausarbeitungsprozesses von Ideen und Geschäftsmodellen kurz erläutert werden.

7.3.1 Anforderungen an den Innovationsprozess

7.3.1.1 Collaboration Engineering

Um den zu unterstützenden Innovationsprozess zu analysieren, wird auf das Collaboration Engineering zurückgegriffen. Durch die Anwendung der Prinzipien des Collaboration Engineering lassen sich kollaborative Aufgaben, in diesem Fall die Erstellung innovativer Produkt- und Servicekonzepte, analysieren und Gestaltungsempfehlungen für deren Design ableiten (Briggs et al. 2009; Vreede/Briggs 2005). Um alle Aspekte, die das Design einer kollaborativen Aufgabe beeinflussen, zu erfassen, wird im vorliegenden Fall das 6-Ebenen-Modell ([Abbildung 2](#)) verwendet, welches eine strukturierte Vorgehensweise zur Konzeption der Zusammenarbeit beschreibt (Nunamaker et al. 2013; Leimeister 2014).

Auf der ersten Ebene („Kollaborationsziele“) wird das angestrebte Ergebnis der Kollaboration festgelegt. Unter Kollaboration wird dabei die gemeinsame Anstrengung verstanden, die eine Gruppe unternimmt, um das Gruppenziel zu erreichen. Alle folgenden Entscheidungen zur Ausgestaltung des Kollaborationsprozesses werden dem vordefinierten Gruppenziel unterstellt und müssen auf diesen abgestimmt werden (Leimeister 2014). Auf der zwei-

Abbildung 2: 6-Ebenen-Modell

ten Ebene („Gruppenprodukte“) werden die angestrebten materiellen und immateriellen Ergebnisse der Zusammenarbeit definiert. Diese Produkte müssen auf Basis der zuvor definierten Ziele sowohl qualitativ als auch quantitativ definiert werden. Die dritte Ebene („Gruppenaktivitäten“) beinhaltet die einzelnen Unteraufgaben, die für die Erstellung der Gruppenprodukte erfüllt werden müssen, um das Gruppenziel erreichen zu können. Die vierte Ebene („Gruppenprozeduren“) umfasst Methoden und Strategien für die Erstellung der Gruppenprodukte. Gruppenprozeduren sind darüber hinaus durch beobachtbare Zustandsveränderungen gekennzeichnet. Mittels Gruppenprozeduren werden die zuvor definierten Gruppenaktivitäten konkretisiert. Der vierten Ebene sind zudem Kollaborationstechniken zugeordnet, die eine erwünschte Interaktion zwischen Gruppenmitgliedern zum Zwecke der Gruppenzielerreichung fördern. Auf der fünften Ebene („Kollaborationswerkzeuge“) werden Werkzeuge identifiziert, mittels derer der Arbeitsvorgang zur Gruppenzielerreichung durchgeführt und unterstützt werden kann. Die sechste Ebene („Kollaborationsverhalten“) beinhaltet die Aussagen und Handlungen der Teilnehmer mit den verwendeten Werkzeugen, die auf die Erreichung des Ziels gerichtet sind.

Das 6-Ebenen-Kollaborationsmodell hilft dabei den online-basierten Entwicklungsprozess von Cloud-Services so zu gestalten, dass übergeordnete Kollaborationsziele erreicht werden können. Der Einsatz von Kollaborations-

techniken und -werkzeugen ermöglicht es, dabei den Prozess zu strukturieren. Als zentrales Werkzeug zur Entwicklung und Ausgestaltung von Cloud-Services soll das Business Model Canvas (Osterwalder/Pigneur 2011) Anwendung finden. Das Business Model Canvas wird im Folgenden vorgestellt, da es einen zentralen Bestandteil der zu entwickelnden Lösung darstellt.

7.3.1.2 Business Model Canvas

Das Business Model Canvas (BMC) ist ein design- und innovationsbasiertes Tool zur Visualisierung und Entwicklung von Geschäftsmodellen (Simmert et al. 2013). Das BMC besteht aus neun verschiedenen Bausteinen: Kundensegmente, Wertangebote, Kanäle, Kundenbeziehungen, Einnahmequellen, Schlüsselressourcen, Schlüsselaktivitäten und Schlüsselpartnerschaften. Die Erstellung eines Geschäftsmodells mittels BMC erfolgt in fünf Phasen (Osterwalder/Pigneur 2011).

In der ersten Phase („Mobilisieren“) werden die Voraussetzungen für die Geschäftsmodellentwicklung geschaffen. Diese sind u.a. der Aufbau eines gemeinsamen Verständnisses zur Entwicklung eines neuen Geschäftsmodells sowie das Zusammentragen aller zur Ausarbeitung des Geschäftsmodells notwendigen Elemente. In der zweiten Phase („Verstehen“) werden u.a. die Bedürfnisse der betreffenden Kundengruppen ermittelt. Die dritte Phase („Gestalten“) beinhaltet Aufbau, Erprobung und Auswahl von Geschäftsmodellprototypen. In der vierten Phase („Implementieren“) werden die Geschäftsmodellprototypen in die Praxis umgesetzt. In der letzten Phase („Durchführen“) wird das Geschäftsmodell gesteuert und, falls nötig, im Hinblick auf Marktreaktionen modifiziert.

Das BMC konnte sich in den letzten Jahren als Werkzeug zur Geschäftsmodellentwicklung etablieren und stellt für den Entwicklungsprozess neuer Cloud-Services ein Kernwerkzeug dar, mittels dem ein vollständiges Geschäftsmodell durch den Einbezug verschiedener Stakeholder ausgearbeitet werden kann.

7.3.2 Anforderungen an die Online-Community

Allgemeine Erfolgskriterien für eine Online-Community sind Usability und Sociability (Preece 2001). Usability bezeichnet die Benutzerfreundlichkeit

und beschreibt somit die Intuitivität der Online-Community-Plattform (Ebner 2008). Der Aspekt der Sociability beschreibt die Nutzbarkeit der Plattform für soziale Zwecke, die sich wiederum in Regeln, Funktionalitäten und Handlungsmöglichkeiten zur Unterstützung der Interaktion widerspiegeln. Eine spezifischere Ausarbeitung von Charakteristika solcher Plattformen erfolgte nach Preece (2000) und Janzik (2012). Zusammengefasst können aus der Literatur acht zentrale Charakteristika identifiziert werden, die zur Beschreibung einer Community und ihrer Anforderungen herangezogen werden können. Dazu zählen *Mitglieder*, *virtueller Treffpunkt im Internet*, *gemeinsame Ziele und/oder Interessen*, *Inhalte*, *Kommunikation über technische Plattform im Internet*, *Vertrauen der Mitglieder*, *Regeln* und *Community-Kultur* sowie das *Geschäftsmodell*.

Mitglieder von Online-Communities bilden meist eine heterogene Gruppe (Janzik 2012). Sie sind der zentrale Faktor für den Erfolg einer Online-Community, da sie Inhalte beisteuern, damit die Ausrichtung der Community festlegen und zu deren Weiterentwicklung beitragen. Kritisch für den Erfolg einer Online-Community sind vor allem die Mitgliedstypen „Innovator“ (veröffentlicht eigene Ideen und Entwicklung, ist aber nicht unbedingt permanent aktiv) und „Aktivist“ (gibt Feedback zu Innovationsprojekten, kollaboriert und verfasst Beiträge; ist regelmäßig aktiv) (Janzik 2012). Für die Entwicklung eines Geschäftsmodells mittels Online-Communities sollten sich die angestrebten Kundensegmente auch in der Mitgliederstruktur der Community wiederfinden. So wird sichergestellt, dass potenzielle Marktbedürfnisse des spezifischen Kundensegments bei der Konzeption des Geschäftsmodells berücksichtigt werden.

Ein weiteres wesentliches Kennzeichen von Online Communities ist die Interaktion über eine *virtuelle Plattform im Internet* (Janzik 2012). Zusätzliche reale Treffen sind allerdings nicht ausgeschlossen.

Die Mitglieder einer Online-Community haben ein Mindestmaß an *gemeinsamen Zielen und/oder Interessen* (Janzik 2012). Die Interessen der Mitglieder sind dabei nicht vollständig homogen. So bestehen auch individuelle, etwa soziale, psychologische oder inhaltliche Interessen. Die Interessen der Mitglieder können mit den Interessen der Betreiber der Online-Community übereinstimmen oder (teilweise) von diesen abweichen. Der Hauptbeweg-

grund für die Teilnahme innerhalb einer Online-Community sollte in einem gemeinsamen Interesse an dem Thema der Community liegen. Der Teilnahme entgegenstehende Hemmungen (wie etwa mangelnde technische Kompatibilität oder Kosten für die Teilnahme) sollten weitestgehend beseitigt werden. Die Betreiber der Online-Community können Anreize setzen, um die Übereinstimmung der Ziele der Mitglieder mit den Kollaborationszielen zu erhöhen und eine rege Beteiligung der Mitglieder sicherzustellen. Dazu können die Betreiber Strukturen schaffen, die die intrinsische Motivation der Mitglieder stärken und zusätzliche extrinsische Anreize setzen. Beispielsweise kann die Motivation der Innovatoren mithilfe von Ideenwettbewerben gesteigert werden. Der Anreiz liegt hier neben möglichen Sach- oder Geldpreisen auch in dem Zugewinn an sozialer Anerkennung, der aus dem Beitrag einer guten Idee resultieren kann. Ein Ideenwettbewerb kann auch eingesetzt werden, um einzelne Gruppenprodukte zu generieren.

Die *Inhalte* einer Online-Community umfassen die Informationen und die Medien, die innerhalb der Community geteilt und diskutiert werden (Janzik 2012). Sie werden häufig von den Mitgliedern selbst generiert. Ein Austauschprozess zwischen den Mitgliedern, in dem die erstellten Inhalte um individuelles Wissen und individuelle Fähigkeiten sowie Meinungen von Mitgliedern angereichert werden, führt zu einem ständig wachsenden Pool an Erfahrungen, Informationen und Wissen und zu einer kontinuierlichen qualitativen Verbesserung der erstellten Inhalte. Die Inhalte, die in einer Ideen-Community generiert werden, bestehen aus (Teil-) Lösungsvorschlägen der Mitglieder und den daraus ableitbaren Bedürfnisinformationen. Insbesondere die Innovatoren und teilweise auch die Aktivisten sollten zur Inhaltserzeugung mit Informationen versorgt werden, die über die am Markt verfügbaren Informationen hinausgehen (Janzik 2012). Die erzeugten Inhalte unterliegen durch die Möglichkeit zur Kommentierung einem kontinuierlichen Verbesserungsprozess. Mit Blick auf die Konzeption eines Geschäftsmodells werden die Inhalte vor allem in der dritten Phase („Gestalten“) erzeugt. Es steht hier der Baustein des Wertangebots im Vordergrund, da insbesondere die Innovatoren mit ihrer gleichzeitigen Eigenschaft als Kunden, Ideen entwickeln können, wie ein Mehrwert für Kunden geschaffen werden kann. Um den Innovatoren die Entwicklung komplexer Inhalte und detaillierter Lösungsangebote

zu ermöglichen, können unterschiedliche Kollaborationswerkzeuge bereitgestellt werden.

Die *Kommunikation* zwischen den Mitgliedern erfolgt überwiegend unterstützt durch elektronische Wege im Internet (Janzik 2012). Dabei können verschiedene Kommunikationskanäle, wie etwa Instant Messaging, E-Mail, VoIP, Chat, Blogs, Foren und Bulletin Boards zum Einsatz kommen. Die technische Plattform im Internet sollte so gestaltet sein, dass Innovatoren ihre Ideen klar und verständlich vermitteln können. Die Plattform sollte dazu übersichtlich und intuitiv gestaltet sein und auch die Erzeugung und/oder die Veröffentlichung multimedialer Inhalte ermöglichen. Vor allem die Möglichkeit zur Überarbeitung und zur Kommentierung der Lösungen erscheint notwendig, um einen kontinuierlichen Verbesserungsprozess zu ermöglichen. Die virtuelle Kommunikation ermöglicht die kontinuierliche Beobachtung der Kommunikation, sodass die Gruppenaktivitäten, die Gruppenprozeduren und das Kollaborationsverhalten festgehalten und analysiert werden können. Hieraus können beispielsweise Lösungsentwürfe, mögliche Bedürfnisse und ein zusätzlicher Informationsbedarf abgeleitet werden.

Für die Interaktion in einer Online-Community bestehen verschiedene *Regeln* (Janzik 2012). Aus technischer Perspektive gibt es beispielsweise Regeln zu Administrationsrechten und Zugangsbeschränkungen. Auch das Verhalten der Community-Mitglieder untereinander ist implizit und/oder explizit durch die so genannte „Netiquette“ geregelt. Die Netiquette stellt die Basis für die Entwicklung einer Online-Community dar. Regeln zu allgemeinen Umgangsformen in der Community stellen eine wesentliche Voraussetzung für den Erfolg der Community dar. Mit Blick auf Online Communities sind insbesondere Regeln relevant, die sicherstellen, dass ein Umfeld entsteht, in dem Mitglieder bereit sind, eigene kreative und innovative Ideen zu veröffentlichen, ohne dabei dem Risiko ausgesetzt zu sein, dass die Ideen diskreditiert und/oder „geklaut“ werden. Ein (kosten-)freier Zugang zu der Online-Community stellt eine wesentliche Voraussetzung für das Erreichen einer großen Anzahl von Mitgliedern dar.

Das *Vertrauen* in den Erfolg der Online-Community stellt einen wichtigen sozialen Anreiz für die Mitglieder dar (Janzik 2012). Für eine Online-Community ist dabei vor allem wichtig, dass die Mitglieder darauf vertrauen,

dass ihnen alle für den Innovationsprozess kritischen Informationen mitgeteilt werden und dass Ideen und Vorschläge gewürdigt werden und tatsächlich in den Innovationsprozess einfließen. Eine regelmäßige Information über den Stand einer Innovationsaktivität erscheint hier sinnvoll. Die Wertschätzung für Innovationsvorschläge kann beispielsweise durch Sachpreise bei Ideenwettbewerben oder auch durch Beiträge und Kommentare von Mitarbeitern des Unternehmens illustriert werden. Da die Mitglieder der Community einen unterschiedlichen Informationsbedarf haben, können beispielsweise Innovatoren mit zusätzlichen, detaillierten Informationen versorgt werden.

Neben Möglichkeiten zur direkten Umsatzgenerierung (z.B. Mitgliederbeiträge, Transaktionsgebühren oder Platzierung von Werbung) kann die Wertschöpfung mittels Online-Community über indirekte Umsatzgenerierung (z.B. thematische Nähe zu bestimmten Produktshops) erfolgen (Janzik 2012). Auch wenn viele Online Communities nicht profitorientiert sind, werden häufig einfache Formen der Werbeintegration genutzt, um die Betriebskosten (zumindest teilweise) zu decken. Die Wertschöpfung der Online-Community kann bereits dadurch erfolgen, dass Lösungsvorschläge und Bedürfnisse in den Innovationsprozess einfließen, ohne durch die eigene Forschung und Entwicklung bzw. Marktforschung generiert zu werden. Weitere Formen der Umsatzgenerierung können sich teilweise negativ auf die Anreizstruktur auswirken. So können beispielsweise Mitgliederbeiträge eine Hemmschwelle für die Beteiligung an einer Online-Community darstellen (Janzik 2012). Auch die Integration von Werbung kann sich negativ auf die Anreizstruktur auswirken, da sie für Mitglieder möglicherweise den Anschein erweckt, dass der Hauptzweck der Community nicht in der Innovationsentwicklung, sondern in der Umsatzgenerierung liegt. Die Werbeintegration kann so das Vertrauen in die Community senken. Transparenz stellt hier einen zentralen Faktor dar – so könnte der Betreiber der Online-Community beispielsweise darauf aufmerksam machen, dass die integrierte Werbung lediglich der Deckung der Betriebskosten und nicht der Umsatzgenerierung dient.

7.4 Schlussbetrachtung

In diesem Kapitel konnten literaturbasierte Anforderungen an eine Online-Community abgeleitet werden. Eine Umsetzung dieser erfolgt im Kapitel 14, in dem eine ‚Open Service Innovation‘-Online-Community entwickelt wird, die eine Ausarbeitung von Ideen bis hin zu vollständigen Geschäftsmodellen ermöglichen soll.

Weitere Erkenntnisse hinsichtlich der Anforderungserhebung an eine Online-Community und die zu verwendenden Werkzeuge und Methoden konnten aus der Durchführung von Offline-Workshops gezogen werden. In den durchgeführten – insgesamt drei – Workshops konnten relevante Anforderungen für den Umgang und die Anwendung des Business Model Canvas, aber auch den kollaborativen Prozess selbst generiert werden. Die Durchführung der Workshops erfolgte in enger Zusammenarbeit mit einem IT-Service-Provider. Durch die direkte Einbindung der Kunden des Providers in den Workshop wurden im Hinblick auf die Anforderungserhebung vor allem zwei wesentliche Ziele adressiert:

- Testen von Werkzeugen und Methoden zur Durchführung und Umsetzung von Open-Innovation-Ansätzen im realweltlichen Szenario zur Entwicklung innovativer und nutzergerechter Cloud-Services.
- Anforderungserhebung (Beobachtung und Fragebogen) hinsichtlich der Umsetzung und Gestaltung des Entwicklungsprozesses von innovativen und nutzergerechten Cloud-Services innerhalb einer onlinebasierten Ideen-Community.

Basierend auf diesen Zielsetzungen sowie den Evaluationsergebnissen aus den Workshops mit Kunden des IT-Service-Providers wurde das Workshop-Design weiterentwickelt, methodisch aufgearbeitet und neu strukturiert. Insgesamt hat sich gezeigt, dass der Ausarbeitung des Wertbeitrages und der Kundensegmente eine deutlich größere Bedeutung zukommen muss. Auch sollen zukünftig weitere Präsenz-Workshops dabei helfen, die Anforderungen weiter auszuarbeiten und kontinuierlich neu aufkommende Anforderungen zu sammeln, um eine funktionstüchtige und produktive Online-Communi-

nity-Plattform bezogen auf das Themenfeld des Cloud-Computings bereitstellen zu können.

7.5 Literaturverzeichnis

- Ahuja, G.; Katila, R. (2001):** Technological acquisitions and the innovation performance of acquiring firms: a longitudinal study. In: *Strategic Management Journal*, Vol. 22 (2001) No. 3, S. 197-220.
- Blohm, I.; Köroglu, O.; Leimeister, J.M.; Krcmar, H. (2011):** Absorptive capacity for open innovation communities-learnings from theory and practice. Präsentiert auf dem 74th Academy of Management Annual Meeting, San Antonio, USA.
- Bretschneider, U. (2012):** Die Ideen-Community zur Integration von Kunden in den Innovationsprozess – Empirische Analysen und Implikationen, Springer Gabler, Wiesbaden 2012.
- Briggs, R.O.; Kolfschoten, G.L.; de Vreede, G.-J.; Albrecht, C.; Dean, D.R.; Lukosch, S. (2009):** A Six Layer Model of Collaboration for Designers of Collaboration Systems. In: *Advances in Collaboration Systems*. Nunamaker, J.F.; Briggs, R.O.; Romano, N.C. (Hrsg.). Armonk, NY 2009.
- Chesbrough, H.W. (2003):** Open Innovation: The New Imperative for Creating and Profiting from Technology, Harvard Business School Press 2003.
- Ebel, P.; Bretschneider, U.; Leimeister, J.M. (2012):** Erarbeitung eines Workshopdesigns zur weiteren Ausarbeitung der Ergebnisse einer virtuellen Ideencommunity. Präsentiert auf der Proceedings zum Workshop Gemeinschaft in Neuen Medien (GeNeMe 12), Dresden, Deutschland.
- Ebner, W. (2008):** Community Building for Innovations – Der Ideenwettbewerb als Methode für die Entwicklung und Einführung einer virtuellen Innovations-Gemeinschaft, Technische Universität München 2008.
- Ebner, W.; Leimeister, J.M.; Krcmar, H. (2009):** Community engineering for innovations: the ideas competition as a method to nurture a virtual community for innovations. In: *R&D Management*, Vol. 39 (2009) No. 4, S. 342-356.
- Faltings Business Development (2014):** Business Model Canvas Poster auf Deutsch. Abgerufen am: 15.11.2014; URL: <http://faltings.de/geschaeftsmodell-canvas/>.
- Kunz, M.; Söllner, M.; Leimeister, J.M. (2014):** Successfully funded! – Welche Geschäftsmodelle machen crowdfinanzierte Cloud-Startups erfolgreich? Präsentiert auf der Multikonferenz Wirtschaftsinformatik, Paderborn, Deutschland.
- Janzik, L. (2012):** Motivanalyse zu Anwenderinnovationen in Online-Communities, Springer Gabler, Wiesbaden, Deutschland 2012.
- Leimeister, J.M. (2012):** Dienstleistungengineering und -management, Springer, Heidelberg, Deutschland 2012.
- Leimeister, J.M. (2014):** Collaboration Engineering – IT-gestützte Zusammenarbeitsprozesse systematisch entwickeln und durchführen, Springer Gabler, Wiesbaden, Deutschland 2014.

- Leimeister, J.M.; Ebner, W.; Krcmar, H. (2005):** Design, Implementation, and Evaluation of Trust-Supporting Components in Virtual Communities for Patients. In: *Journal of Management Information Systems*, Vol. 21 (2005) No. 4, S. 101-135.
- Leimeister, J.M.; Huber, M.; Bretschneider, U.; Krcmar, H. (2009):** Leveraging Crowdsourcing: Activation-Supporting Components for IT-Based Ideas Competition. In: *J. Manage. Inf. Syst.*, Vol. 26 (2009) No. 1, S. 197-224.
- Leimeister, J.M.; Krcmar, H. (2004):** Revisiting the Virtual Community Business Model. Präsentiert auf der 10th Americas Conference on Information Systems, New York, USA.
- Möslein, K.M.; Neyer, A.K. (2009):** Open Innovation – Grundlagen, Herausforderungen und Spannungsfelder, Kommunikation als Erfolgsfaktor im Innovationsmanagement. In: *Open Innovation*. Zerfaß, A.; Möslein, K.M. (Hrsg.). Gabler, Wiesbaden, Deutschland 2009, S. 85-103.
- Nunamaker, J.F.; Romano, N.C.; Briggs, R.O. (2013):** Collaborations Systems: Concept, Value, and Use, M.E.Sharpe, Armonk, New York, USA 2013.
- Oesterwalder, A.; Pigneur, Y. (2011):** Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer, Campus Verlag, Frankfurt a.M., Deutschland 2011.
- Panten, G. (2005):** Internet-Geschäftsmodell Virtuelle Community: Analyse zentraler Erfolgsfaktoren unter Verwendung des Partial-Least-Squares (PLS)-Ansatzes, Deutscher Universitätsverlag, Wiesbaden, Deutschland 2005.
- Preece, J. (2000):** Online communities: designing usability, supporting sociability, John Wiley, USA 2000.
- Preece, J. (2001):** Sociability and usability in online communities: Determining and measuring success. In: *Behaviour & Information Technology*, Vol. 20 (2001) No. 5, S. 347-356.
- Reichwald, R.; Piller, F.T. (2006):** Interaktive Wertschöpfung, Gabler, Wiesbaden, Deutschland, 2006.
- Schaffert, S.; Wieden-Bischof, D. (2009):** Erfolgreicher Aufbau von Online Communities – Konzepte, Szenarien und Handlungsempfehlungen, Salzburg Research Forschungsgesellschaft, Salzburg, Österreich, 2009.
- Simmert, B.; Ebel, P.; Bretschneider, U. (2013):** Empirische Erkenntnisse zur Nutzung des Business Model Canvas, In: *Working Paper Series*, Nr. 5, Kassel, Deutschland 2013.
- Szulanski, G. (1996):** Exploring Internal Stickiness: Impediments to the Transfer of Best Practice Within the Firm. In: *Strategic Management Journal*, Vol. 17 (1996), S. 27-43.
- Vreede, G.-J.d.; Briggs, R.O. (2005):** Collaboration Engineering: Designing Repeatable Processes for High-Value Collaborative Tasks. Präsentiert auf der 38th Annual Hawaii International Conference on System Sciences, Waikoloa, Hawaii.

8 Relevante Rechtsfragen des Cloud-Computing

S. Jandt, S. Kroschwald, A. Roßnagel, M. Wicker

Rechtsfragen des Cloud-Computing können sich aus dem gesamten Spektrum des Rechts ergeben. Sie resultieren aus Rechtsverhältnissen zwischen Bürgern untereinander ebenso wie zwischen Bürgern und Staat.

8.1 Privatrechtliche Beziehung zwischen Cloud-Anbieter und Cloud-Nutzer

Cloud-bezogene Rechtsfragen entspringen beispielsweise dem privatrechtlich geprägten Verhältnis zwischen einem Cloud-Anbieter und einem Cloud-Nutzer. Diese stehen meist in einer gegenseitigen Rechtsbeziehung zum Austausch von IT-Leistungen. Rechtsfragen können aber auch in einem privatrechtlichen Dreiecksverhältnis zwischen Cloud-Nutzer, Cloud-Anbieter und einem Dritten, beispielsweise einem Unterauftragnehmer oder einem von der Cloud-Nutzung Betroffenen, entstehen. Diese privatrechtlichen Verhältnisse haben häufig vertragliche Grundlagen, sodass das Vertragsrecht von Relevanz ist.¹ Erforderlich ist daher, Cloud-Angebote vertragstypologisch einzuordnen und vor allem Gestaltungsanforderungen zu entwickeln, die in einer vertraglichen Beziehung im Cloud-Kontext berücksichtigt werden müssen.

8.2 Öffentlich-rechtliche Beziehung zwischen Cloud-Anbieter und Cloud-Nutzer

Öffentlich-rechtliche Rechtsfragen entstehen insbesondere dort, wo der Staat in das Verhältnis zwischen den Beteiligten schützend oder fördernd eingreift. Von besonderer Bedeutung sind solche öffentlich-rechtlichen Aktivitäten, die sich auf grundrechtlich geschützte Rechtsgüter wie etwa das Persönlichkeitsrecht des Einzelnen beziehen.

1 S. hierzu Kapitel 16 zur Vertragsgestaltung beim Cloud-Computing.

8.3 Datenschutzrecht

Wesentliche öffentlich-rechtliche Fragen ergeben sich für das Cloud-Computing beispielsweise im Bereich des Datenschutzrechts.² Von Bedeutung ist, unter welchen Voraussetzungen eine Datenverarbeitung in der Cloud zulässig ist. Hierfür ist zum einen danach zu fragen, wer in welchen Geschäftsmodellen für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ist. Zum anderen ist zu untersuchen, ob sich die Voraussetzungen für den rechtmäßigen Umgang mit Daten über Geschäfts- und Betriebsgeheimnisse einerseits und personenbezogene Daten der Kunden, Vertragspartner und Mitarbeiter andererseits unterscheiden. Schließlich ist danach zu differenzieren, welche Auswirkungen die territoriale Zuordnung der Cloud für die Zulässigkeit der Datenverarbeitung hat. Die Rechte und Pflichten der Cloud-Nutzer und Cloud-Anbieter aus dem Datenschutzrecht werden anhand der Regelungen des Bundesdatenschutzgesetzes dargestellt. Hierauf aufbauend können Gestaltungsvorschläge zur Nutzer- und Anbieterunterstützung entwickelt werden.

8.4 Materielles und prozessuales Strafrecht

Neben dem öffentlich-rechtlichen Datenschutz- und dem privatrechtlichen Vertragsrecht kann im Rahmen des Cloud-Computing auch das Strafrecht und Strafprozessrecht relevant sein. Die Cloud-Nutzung kann einerseits bereits selbst eine strafbare Handlung sein und einen Straftatbestand verwirklichen, wenn dadurch z.B. Geheimnisse preisgegeben werden. Insofern sind Risiken einer Strafbarkeit für die Cloud-Akteure zu untersuchen.³ Neben dem Strafgesetzbuch werden dabei unter anderem die Strafvorschriften aus dem Bundesdatenschutzgesetz berücksichtigt.

Andererseits erstreckt sich die Untersuchung auf neue Möglichkeiten und Schwierigkeiten, denen der Staat im Rahmen der Strafverfolgung durch das Cloud-Computing begegnet. Schwerpunkt bildet die Frage, ob und inwiefern die Ermittlungsmöglichkeiten im Strafprozess durch Cloud-Nutzung verbes-

2 S. hierzu Kapitel 15 zum Datenschutzrecht beim Cloud-Computing.

3 S. hierzu Kapitel 17 zu den Strafbarkeitsrisiken beim Cloud-Computing.

sert oder verschlechtert werden.⁴ Dabei wird besonders berücksichtigt, ob der von den strafprozessualen Ermittlungen betroffene Cloud-Nutzer mit rechtlichen Nachteilen zu rechnen hat, wenn er sich für die Nutzung von IT aus der Cloud entscheidet. Auch die Rolle des Cloud-Anbieters im Strafprozess wird beleuchtet, insbesondere wird hier die Frage beantwortet, unter welchen Umständen der Cloud-Anbieter zur Kooperation mit den Ermittlungsbehörden verpflichtet ist.

4 S. hierzu Kapitel 18 zu den strafprozessualen Ermittlungsmöglichkeiten beim Cloud-Computing.

Teil E:
Die Value4Cloud-
Mehrwertdienste

9 Service-Auswahl – Entwicklung von Merkmalskatalog und Klassifizierungssystem

P. Hoberg, H. Krcmar

9.1 Einleitung

Es ist eine große Herausforderung für Unternehmen, die für die Auswahl eines Cloud-Service notwendigen Informationen zu sammeln. Zunächst muss im eigenen Unternehmen der Bedarf spezifiziert und dann das Angebot dem Bedarf gegenübergestellt werden. Während einige Cloud-Service-Anbieter Kundenberater einsetzen und potenziellen Unternehmenskunden so die Möglichkeit bieten, sich Informationen über einen persönlichen Kontakt zum Anbieter zu beschaffen, setzen viele darauf, dass sich potenzielle Kunden Informationen zu Service-Angeboten selbstständig beschaffen (z. B. über im Internet verfügbare Dokumente und häufig gestellte Fragen (FAQ)). Die Informationen, auf deren Basis die Auswahl eines Cloud-Service getroffen wird, müssen vom Kunden häufig in Eigenregie beschafft werden. Leicht bleiben dabei entscheidungsrelevante Informationen unbeachtet.

Für viele kleine und mittlere Unternehmen ist die Beauftragung eines spezialisierten Dienstleisters, der die Erhebung der für die Auswahlentscheidung notwendigen Informationen übernimmt und eine Bewertung alternativer Serviceangebote vornimmt, nicht effizient. Oft stehen die Kosten für die Beauftragung eines Spezialisten in keinem Verhältnis zu den Kosten für den Bezug einer Cloud-Lösung.

Die Informationsbeschaffung zur Vorbereitung einer Auswahlentscheidung erfordert ein strukturiertes Vorgehen in Form der Beschreibung und des Vergleichs einzelner Lösungen anhand einheitlicher Kriterien (Wollersheim/Krcmar 2013). Ein Kriterienkatalog hilft bei der systematischen Erfassung von Service-Eigenschaften und stellt damit die Basis einer objektiven Bewertung dar. Auf diese Weise können Lücken in den Angebotsbeschreibungen von Cloud-Service-Anbietern aufgedeckt werden.

Bestehende Kriterienkataloge zur Beschreibung von IT-Services im Allgemeinen und Cloud-Services im Besonderen fokussieren auf die funktionalen Aspekte einer Lösung (siehe Hoefer/Karagiannis 2010) oder auf einen bestimmten Typ von Services (siehe Repschläger et al. 2011; Repschläger et al. 2012; Rimal et al. 2009). In diesem Kapitel wird ein Kriterienkatalog vorgestellt, der das fragmentierte Bild bestehender Kriterienkataloge integriert und aus Perspektive der unterschiedlichen Anspruchsgruppen im Cloud-Kundenunternehmen (z. B. Service-Nutzer, Mitarbeiter im Einkauf, IT-Abteilung) strukturiert.

Ziel ist es, den an einer Nutzung von Cloud-Services interessierten Unternehmen eine Orientierung bei der Frage zu bieten, welche Informationen für die Entscheidung für ein Service-Angebot relevant sein können. Der hier beschriebene Kriterienkatalog für Cloud-Services kann wie eine Checkliste eingesetzt werden. Die Liste hilft bei der Identifikation relevanter Auswahlkriterien. Sie stellt damit eine Grundlage für die Bewertung von Cloud-Services dar, um Cloud-Kundenunternehmen eine informierte Entscheidung für ein Service-Angebot zu ermöglichen.

9.2 Stand der Forschung

Im Forschungsbereich Cloud-Computing haben sich bereits verschiedene Publikationen mit der Klassifizierung von Cloud-Services beschäftigt. Zu den bekanntesten gehört der Service Measurement Index (SMI) der Carnegie Mellon University. Der SMI beschreibt Cloud-Services unter Qualitätsgesichtspunkten anhand einer Reihe geschäftsrelevanter Leistungskennzahlen, die in die folgenden sieben Gruppen gegliedert sind: Benutzerfreundlichkeit, Agilität, Leistungsgarantie, Sicherheit und Datenschutz, Verantwortlichkeiten, Leistungsfähigkeit und Kosten. Der SMI soll Kunden helfen, interne IT-Services und Cloud-Services zu bewerten und zu vergleichen.

Basierend auf einer internationalen Literatur- und Angebotsanalyse sowie Experteninterviews entwickeln Repschläger et al. (2011; 2012) einen Klassifikationsrahmen für die Auswahl von Cloud-Service-Angeboten. Die Autoren fokussieren mit der Untersuchung von Infrastrukturangeboten (IaaS) auf die unterste Ebene im Layer-Modell nach Youseff et al. (2008) (siehe Kapitel

2) und identifizieren sechs Perspektiven, aus denen Cloud-Infrastruktur-Services betrachtet und beschrieben werden können: Flexibilität des Angebots, Verlässlichkeit und Vertrauenswürdigkeit des Angebots, IT-Sicherheit und Compliance, Funktions- und Leistungsumfang, Service-Management und Kosten.

Im Gegensatz zu Repschläger et al. (2011; 2012) fokussieren Rimal et al. (2009) genauso wie Hilley (2009) ausschließlich auf die technischen Unterscheidungsmerkmale von IaaS-Angeboten. Anhand des Vergleichs von vier Infrastrukturservices (Amazon Web Services, GoGrid, Flexiscale, Mosso) geben Rimal et al. (2009) Einblick in die technischen Unterschiede und Gemeinsamkeiten von IaaS in Bezug auf neun Merkmale, von der Servicearchitektur über die Umsetzung des Lastausgleichsverfahrens bis hin zu den eingesetzten Sicherheitsmechanismen. An diese technische Charakterisierung anknüpfend, evaluieren und identifizieren Li et al. (2011) Metriken für den Vergleich der Performance von IaaS- und PaaS-Angeboten. Prodan und Ostermann (2009) erweitern diese technische Betrachtung um eine Analyse und Beschreibung der unterschiedlichen Geschäftsmodelle von IaaS-Anbietern.

Bisher hat sich lediglich eine Veröffentlichung der Klassifikation von Cloud-Services aller drei von Youseff et al. (2008) beschriebenen Service Layer gewidmet. Hoefner und Karagiannis (2010) unterscheiden zwischen Service-Typ unabhängigen und Service-Typ abhängigen Klassifikationskriterien. Am Beispiel von Google Cloud Services entwickeln die Autoren ein Klassifizierungssystem für SaaS, PaaS und IaaS. Gegenüber den auf nur einen Layer beschränkten Klassifikationen von Rimal et al. (2009) oder Hilley (2009) fällt jedoch der höhere Abstraktionsgrad auf. Diese Lücke soll mit Hilfe des in diesem Kapitel vorgestellten neuen Kriterienkatalogs geschlossen werden.

9.3 Der Value4Cloud-Kriterienkatalog

Bestehende Definitionen des Begriffs Cloud-Computing geben enge Grenzen bezüglich der Eigenschaften vor, die einen Cloud-Service ausmachen. Diese decken sich jedoch nicht immer mit den Anforderungen der Anwender. So wird als Preismodell für Cloud-Services allgemein eine nutzungsabhängige Abrechnung vorausgesetzt. Dies geht, Koehler et al. (2010, S. 2) folgend, jedoch an der Realität vorbei, da zumindest für fachliche Services¹ Festpreistarife dominieren. Für die Klassifikation von Cloud-Services ist eine starre Definition, die Einordnung in Schwarz oder Weiß, daher nicht zweckmäßig. Vielmehr müssen ein Kriterienkatalog und die darin definierten Service-Kriterien ein Kontinuum widerspiegeln, das den vielfältigen Realisierungsformen von Cloud-Services Rechnung trägt.

Wie weiter oben bereits angemerkt wurde, sollte die Basis für die Auswahl eines Cloud-Service, wie üblich bei der Auswahl von IT-Lösungen, eine umfassende Anforderungsanalyse sein, die fachliche und technische Aspekte vereint. Hierzu sind die Anforderungen aller unternehmensinternen Anspruchsgruppen an die zu beschaffende Lösung zunächst zu sammeln und zu systematisieren. Als Ordnungsrahmen für die Systematisierung der Anforderungsanalyse wurde eine zielgruppenspezifische Strukturierung von Eigenschaften in fünf Sichten gewählt (siehe [Abbildung 1](#)), die im Folgenden näher beschrieben werden sollen.

Die Reihenfolge der in den unterschiedlichen Sichten zusammengefassten Kriterien stellt keine Hierarchie dar, so dass diese frei kombiniert werden können. Eine Gewichtung der Kriterien erfolgt in Abhängigkeit von den individuellen Anforderungen eines Unternehmens.

1 Anm.: Services, die den Geschäftsbetrieb direkt unterstützen.

Abbildung 1: Die fünf Sichten des Value4Cloud-Kriterienkatalogs (Hoberg et al. 2014, S. 5; in Anlehnung an Hoberg et al. 2012)

9.3.1 Basissicht

Die Basis-Sicht erfasst die zentralen Kriterien, die für die Auswahlentscheidung aus einer Management-Perspektive relevant sein können.

9.3.1.1 Service-Level-Agreement

Das Service-Level-Agreement (SLA) stellt ein Werkzeug für die Steuerung von Leistungserstellungsprozessen, hier der IT, dar. Krcmar (2010, S. 490) definiert SLA als „[...] kennzahlenbasierte Vereinbarungen eines Dienstleistungsanbieters mit seinen Kunden bezüglich der zu gewährleistenden Servicequalität [...]. Dabei wird der Grad der Leistungsqualität (Service-Level oder kurz SL) anhand der Definition der Leistung, der Darstellbarkeit der Leistung als Kennzahl, der Messmethode, dem Ersteller sowie dem Empfänger der Leistung, als auch anhand der Erstellungsfrequenz und des Leistungsniveaus beschrieben [...]“. Es handelt sich damit um eine Gütevereinbarung, die zwischen einem Cloud-Service-Anbieter und seinen Kunden geschlossen wird.

Ein SLA setzt sich aus einer Reihe von Service-Level-Zielpunkten zusammen. Neben den Zielpunkten Verfügbarkeit und Performance werden im Folgenden die Bereitstellungszeit und Skalierbarkeit betrachtet.

Zugesicherte Verfügbarkeit

Verfügbarkeit ist ein Maß für den Grad, in dem der Cloud-Anbieter die festgelegten Anforderungen an einen vom Cloud-Nutzer beauftragten Cloud-Service innerhalb eines vertraglich vereinbarten Messzeitraums erfüllt.

Der Messzeitraum lässt sich anhand von Tagen, Wochen oder Monaten definieren. Für einen festgelegten Messzeitraum wird üblicherweise eine prozentuale Verfügbarkeit des Cloud-Service festgelegt (Bsp.: 98 % bis 99,5 % oder $\geq 99,5$ %). Neben einem oder mehreren alternativen, nicht verhandelbaren und damit für jeden Kunden gleich definierten Zielpunkten bieten manche Anbieter auch eine individuell verhandelbare Verfügbarkeit an. Damit einhergehen kann eine individuelle Aushandlung von Sanktionsmechanismen für den Fall einer Nichterfüllung der im SLA vereinbarten Leistung durch den Anbieter.

Für Cloud-Nutzer ist eine zugesicherte hohe Verfügbarkeit dann von besonderer Relevanz, wenn ein Cloud-Service zur Unterstützung geschäftskritischer Aktivitäten eingesetzt wird. „So kann bspw. der Gefährdung der Verfügbarkeit des Produktionssteuerungssystems typischerweise eine höhere betriebswirtschaftliche Relevanz zugeordnet werden als der mangelnden Verfügbarkeit eines personalwirtschaftlichen Anwendungssystems.“ (Krcmar 2010, S. 578) Sollte dies geplant sein, empfiehlt sich zusätzlich die Prüfung von Verfügbarkeitsvereinbarungen bzgl. der intermediären Infrastruktur.

Performance

Performance kennzeichnet die Fähigkeit von IT-Services, bestimmte Leistungsanforderungen des Kunden erfüllen zu können. Eine niedrige Performance von für den Geschäftsbetrieb kritischen Cloud-Services kann nicht nur zu Produktivitätseinbußen beim Kunden führen, sondern auch die Zufriedenheit der Nutzer des Services und damit deren Nutzungsakzeptanz negativ beeinflussen.

Je nach Art des Cloud-Services können für Cloud-Nutzer unterschiedliche Performancekriterien relevant sein. Während bspw. für Storage-Services der Datendurchsatz eine bestimmende Rolle für die Wahrnehmung der Performance spielt, ist es bei Software-Services eher die Antwortzeit. Für den Kunden ist damit von Bedeutung, auf Basis welcher Kriterien die Zusicherung der Performance des Cloud-Services durch den Service-Anbieter erfolgt.

Bereitstellungszeit

Die Bereitstellungszeit eines Cloud-Services gibt an, wie viel Zeit der Anbieter benötigt, um einen Service nach Erstbeauftragung durch den Kunden bereit zu stellen. Eine niedrige Bereitstellungszeit ist dann von Relevanz, wenn eine kurzfristige technische Unterstützung für ein fachliches Problem des Kunden benötigt wird. Für den Kunden kann es daher relevant sein zu wissen, wie viel Zeit der Cloud-Service-Anbieter für die initiale Bereitstellung des Services benötigt.

Skalierbarkeit

Die Skalierbarkeit eines Cloud-Services bezieht sich auf die Anpassung der für die Service-Erbringung zur Verfügung stehenden Ressourcen (z. B. Rechenleistung, Speicherplatz) an den aktuellen Bedarf des Kunden. Ist der Ressourcenbedarf des Kunden starken, kurzfristigen Schwankungen unterworfen, kann es von Vorteil sein, wenn der Service-Anbieter eine ebenso kurzfristige Bereitstellung zusätzlicher Kapazitäten ermöglicht. Andernfalls sind durch den Kunden Voraussagen über den zukünftigen Bedarf an Rechen-, Speicher- und Netzwerkressourcen anzustellen, um frühzeitig zusätzliche Ressourcen buchen zu können. Ist dies nicht oder nur unzureichend möglich, sind Pufferressourcen als Sicherheit aufzubauen, die zusätzliche Kosten verursachen.

9.3.1.2 Serviceleistungen

Neben Angaben zur Dienstgüte können für Kunden Informationen über die Möglichkeiten der Lokalisierung des Serviceangebots, den Umfang der Ser-

vice-Leistungen und die Kommunikationskanäle zum Anbieter, d.h. ergänzende Service-Leistungen, relevant sein.

Kundendienst

Der Kundendienst nimmt Probleme, die Cloud-Nutzer dem Cloud-Anbieter melden, entgegen, sammelt sie und hilft bei der Problemlösung entweder durch den Verweis auf bzw. die Bereitstellung von Lösungsinformationen (Bsp.: Benutzerhandbuch) oder durch die Vermittlung eines Experten, der persönlich bei der Problemlösung hilft.

Es kann zwischen einem nicht-technischen und einem technischen Kundendienst unterschieden werden. Der nicht-technische Kundendienst hat die Aufgabe, Nutzeranfragen zu fachlichen Problemen (Bsp.: Anlegen eines neuen Nutzers über die Nutzerverwaltung des Cloud-Services) zu registrieren und zu beantworten. Im Gegensatz dazu hat der technische Kundendienst die Aufgabe, Störungsdiagnosen zu erstellen und Störungen zu beheben. Sowohl der nicht-technische als auch der technische Kundendienst können darüber hinaus Schulungen für die Service-Nutzer anbieten.

Im Markt für Cloud-Services bieten viele neue und kleine Anbieter Cloud-Leistungen an. Diese Cloud-Anbieter haben unter Umständen nicht die notwendigen personellen und finanziellen Ressourcen für den Aufbau und den Betrieb eines dedizierten Kundendienstes.

Der Kundendienst ist für die erfolgreiche Einführung eines Cloud-Services wichtig. Insbesondere dann, wenn die funktionale und technische Komplexität eines Cloud-Service hoch ist, kommt auch dem Kundendienst eine hohe Bedeutung zu. Leicht werden die Hürden unterschätzt, die einer reibungslosen Einführung und Integration neuer IT-Services in Unternehmen entgegenstehen. Insofern sollten potenzielle Cloud-Service-Nutzer prüfen, ob der Cloud-Service-Anbieter einen Kundendienst anbietet, welche Leistungen dieser Kundendienst bereitstellt und zu welchen Konditionen dies geschieht.

Kommunikationskanäle

Das Vorhandensein eines Kundendienstes an sich ist kein Garant dafür, dass auftretende Probleme beim Cloud-Nutzer auch effektiv gelöst werden kön-

nen. Kommunikationskanäle repräsentieren ein Instrument zur Anbieter-Nutzer-Kommunikation.

Während manche Cloud-Anbieter gänzlich auf einen synchronen Support (z. B. über Telefon oder Chat) verzichten, bieten andere neben synchronen auch asynchrone Kommunikationskanäle (z. B. Email) sowie einen Vor-Ort-Service oder Hilfestellung per Fernwartung an.

Potenzielle Kunden sollten sich informieren, welche Kommunikationskanäle ihnen zum Anbieter nach Vertragsabschluss zur Verfügung stehen. Darüber hinaus sollten Informationen über die Qualität des Supports und die Kosten für die Nutzung der jeweiligen Kommunikationskanäle eingeholt werden. Als Informationsquellen hierfür können bspw. Nutzerbewertungen auf Cloud-Service-Portalen dienen.

Reaktionszeit auf Kundenanfragen

Im laufenden Betrieb auftretende fachliche und technische Probleme sollten schnell vom Anbieter gelöst werden. Die von einem Cloud-Anbieter zugesicherte Reaktionszeit spezifiziert die Zeitspanne, die dieser benötigt, um auf Kundendienst-Anfragen zu reagieren. Manche Anbieter bieten dem Kunden bei Vertragsschluss die Möglichkeit, einen gewünschten Reaktionszeitraum anzugeben.

Internationalität des Kundendienstes

Die Internationalität von Serviceleistungen ist aufgrund der Globalisierung nicht nur für multinationale Großkonzerne ein entscheidendes Auswahlkriterium, sondern ebenso für KMUs. Für Kunden mit multi-nationalen Projektteams stellt sich die Frage, inwieweit die Internationalität des Teams durch den Kundendienst des Anbieters in Form der Unterstützung unterschiedlicher Sprachen abgebildet wird. Leicht können kulturelle Unterschiede in der Kommunikation die Problemlösung behindern. Insofern kann es von Vorteil sein, wenn der Kundendienst des Cloud-Anbieters in Form nationaler Kundendienstzentren organisiert ist.

9.3.1.3 Preiskalkulation

Unterschiede bei Cloud-Services bestehen nicht nur hinsichtlich ihrer funktionalen Eigenschaften, sondern auch in Bezug auf das Preismodell, die Preisstabilität, die Kostentransparenz sowie die Zahlungsabwicklung und die Zahlungsbedingungen.

Preismodell

Das Preismodell bezieht sich auf die Art und Weise, in der die Nutzung der Leistungen eines Cloud-Anbieters dem Cloud-Nutzer berechnet wird. Denkbar sind neben dem so genannten Pay-per-use-Modell, bei dem z. B. pro Rechenzeiteinheit abgerechnet werden kann, auch Zahlungsmodelle mit einem Fixpreis, bei denen z. B. pro Nutzer und Monat abgerechnet wird. In Mischmodellen können das Pay-per-use- und das Fixpreis-Modell auch kombiniert werden.

Wie im Mobilfunkmarkt ebenfalls üblich, wird in einem solchen Modell ein über die Nutzungszeit fester Grundbetrag mit einer nutzungsabhängigen Abrechnung kombiniert. Während für Kunden, deren Ressourcenbedarf über das Geschäftsjahr verteilt relativ konstant bleibt, ein Festpreismodell von Vorteil sein kann, bieten sich bspw. Pay-per-use-Modelle vor allem für Kunden an, deren Bedarf z. B. saisonalen Schwankungen unterworfen ist.

Preisstabilität

Die Preisstabilität bezieht sich auf die Konstanz des Preises für einen bezogenen Cloud-Service über einen bestimmten Zeitraum hinweg. Für den Kunden ist es vor dem Hintergrund einer nachhaltigen Bindung an den Service-Anbieter relevant zu wissen, über welchen Zeitraum Preisstabilität durch den Cloud-Service-Anbieter gewährleistet wird. Dies ist vor allem für kostenlose Services relevant, da manche Anbieter ihre Services nur zeitweise kostenlos anbieten, um möglichst viele Nutzer zu gewinnen. Ist eine entsprechende Nutzerzahl erreicht, werden neue Funktionen des Service nur gegen Bezahlung freigeschaltet oder bestehende Funktionen nachträglich kostenpflichtig. Ein Wechsel zu einem anderen Cloud-Anbieter kann zu diesem Zeitpunkt

jedoch, bspw. aufgrund einer tiefen Integration des Cloud-Service in die Infrastruktur des Cloud-Nutzers, schwer umzusetzen sein.

Kostentransparenz

Die Abschätzung der Nutzungskosten für einen Cloud-Service kann für den Kunden unter Umständen sehr schwierig sein, da die tatsächlich anfallenden Kosten stark vom Nutzungsverhalten des Kunden abhängen können. Kostentransparenz bezeichnet den Grad der Nachvollziehbarkeit der Kostenberechnung eines Cloud-Service.

Zur Bestimmung der Kostentransparenz kann die Anzahl der auf den Preis wirkenden Einflussfaktoren herangezogen werden. Einflussfaktoren können bspw. die Anzahl der Nutzer, der genutzte Speicherplatz, die Anzahl der Speichervorgänge, die belegte Rechenzeit, der Zeitpunkt der Service-Nutzung (z. B. Werktag oder Wochenende) oder eine ergänzende Leistung wie der Kundendienst sein. Um das Risiko des Anfallens ungeplanter Kosten zu vermeiden, sollten sich potenzielle Kunden informieren, welche und wie viele Einflussfaktoren für die Berechnung des Nutzungsentgeltes vom Anbieter herangezogen werden, und diese vor dem Hintergrund des eigenen Nutzungsprofils betrachten.

9.3.1.4 Allgemeine Geschäftsbedingungen

Die Allgemeinen Geschäftsbedingungen umfassen grundsätzliche Regelungen des Verhältnisses zwischen dem Anbieter und seinen Kunden. Dazu gehören Aspekte wie der Ort der Leistungserbringung, die Vertragslaufzeit bzw. -bindung, die Nennung von Auftragnehmern und Unterauftragnehmern, die Zusicherung von Mandantentrennung, sowie Regelungen über die Datenlöschung nach Vertragsende.

Ort der Leistungserbringung

Aus rechtlichen Gründen kann es für Kundenunternehmen sinnvoll sein, einen Cloud-Service-Anbieter zu wählen, der seine Rechenzentren und/oder seinen Firmensitz in Deutschland oder Europa vorhält (vgl. Kapitel 15-18 zu rechtlichen Fragestellungen). Zur Absicherung, etwa im Katastrophenfall

(z. B. Feuer, Erdbeben, etc.), können darüber hinaus geographisch verteilte Rechenzentren von Vorteil sein.

Vertragslaufzeit bzw. -bindung

Die Vertragslaufzeit bzw. -bindung bezeichnet den Zeitraum, für den die Vertragsbedingungen für beide Parteien als verbindlich gelten. Denkbar sind Vertragslaufzeiten zwischen einem Tag bis hin zu einigen Monaten oder Jahren. Aufgrund sich verändernder Kundenanforderungen (z. B. bei starkem Unternehmenswachstum) kann eine kurzfristige Vertragsbindung anzustreben sein.

Auftragnehmer/Unterauftragnehmer

Ein Cloud-Service-Anbieter kann zur Erbringung seines Service auf die Cloud-Services anderer Anbieter zurückgreifen. Die Kenntnis solcher Unterauftragnehmer-Verhältnisse ist für den Kunden nicht nur unter rechtlichen (vgl. Kapitel 15-18), sondern auch unter sicherheitstechnischen Gesichtspunkten relevant (Hoberg et al. 2012). Für den Kunden stellt sich entsprechend die Frage, ob der Cloud-Service-Anbieter im Rahmen der Leistungserstellung Unterauftragnehmer beauftragt, die ggf. einer gesonderten Bewertung unterzogen werden müssen.

Mandantentrennung

Der Begriff der Mandantentrennung bezeichnet IT-Architekturen, bei denen es verschiedenen Nutzern möglich ist, IT-Ressourcen gemeinsam zu nutzen, ohne dass die gespeicherten und/oder verarbeiteten Daten durch andere Nutzer der Ressource eingesehen oder genutzt werden können. Durch Mandantentrennung erfolgt eine virtuelle, jedoch keine physische Separierung der Ressourcen des Anbieters, die gleichzeitig durch mehrere Kunden genutzt werden. Wird durch den Anbieter keine ausreichende Trennung von Mandanten gewährleistet, besteht die Gefahr, dass Unbefugte Zugriff auf die Daten des Cloud-Nutzers erlangen.

Mandantentrennung muss auf allen Ebenen einer Cloud-Infrastruktur realisiert werden. Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) folgend, gehören dazu die Anwendungs-, Plattform-, Betriebssystem-, virtuelle Server-, Speicher- und Netzebene (BSI 2013). Potenzielle Kunden sollten sich Informationen über die vom Cloud-Anbieter ergriffenen Maßnahmen zur Mandantentrennung beschaffen und diese mit dem Maßnahmenkatalog zur Mandantentrennung des BSI abgleichen (BSI 2013).

Irreversible Datenlöschung

Cloud-Services speichern und verarbeiten unter Umständen sensitive Daten. Aus verschiedenen Gründen kann ein irreversibles und vollständiges Löschen von Daten des Cloud-Nutzers notwendig sein. Dazu gehören der Wechsel des Anbieters oder die Rückholung der ausgelagerten Funktionen in das eigene Unternehmen, das Ende einer Aufbewahrungspflicht oder außerordentliche Anforderungen (BSI 2013). Kundenunternehmen sollten sowohl aus rechtlichen wie auch aus wettbewerblichen Gründen darauf achten, dass eindeutige und transparente Regelungen über die Löschung von Daten nach Vertragsende bestehen und der Cloud-Anbieter zu deren Umsetzung in der Lage ist. Dazu gehören Termine, Fristen und Vorgehensweisen für die irreversible und vollständige Löschung der Daten².

9.3.1.5 Referenzen

Referenzen beziehen sich auf die subjektive Einschätzung oder Empfehlung Dritter hinsichtlich der qualitativen Eigenschaften eines Cloud-Anbieters oder der durch ihn angebotenen Cloud-Services. Es können Kundenreferenzen, Expertenmeinungen und Nutzermeinungen unterschieden werden. Meinungen und Referenzen dienen dazu, sich bereits vor der Nutzung eines Cloud-Services einen Eindruck von dessen zu erwartender Qualität zu verschaffen.

2 Für nähere Informationen hierzu siehe (BSI 2013).

Kundenreferenzen

Kundenreferenzen beziehen sich auf die Bewertung der Qualität eines Cloud-Services und des Cloud-Anbieters durch Bestandskunden. Kundenreferenzen werden häufig in Form von Erfolgsgeschichten publiziert und geben einen Einblick in das Potenzial und die Herausforderungen der Nutzung eines Cloud-Services aus Sicht eines Anwenderunternehmens. Ein solcher Einblick bietet potenziellen Service-Nutzern die Möglichkeit zu einer ersten Einschätzung der Leistungsfähigkeit eines Cloud-Services. Da Kundenreferenzen nicht notwendigerweise unabhängig und objektiv sind, sollten zusätzliche Meinungen wie die von Experten und anderen Nutzern eingeholt werden.

Expertenmeinungen

Expertenmeinungen beziehen sich auf Einschätzungen von unabhängigen Personen mit entsprechendem Fachwissen. Auf Expertenmeinungen kann mithilfe von Cloud-Service-Reviews oder -Rankings zurückgegriffen werden, die in einschlägigen Print- oder Onlinemedien veröffentlicht werden. Expertenmeinungen vermitteln ein umfassenderes Bild der Eigenschaften eines Cloud-Services als Kundenreferenzen und Nutzermeinungen. Damit einher geht jedoch häufig ein höherer Abstraktionsgrad, der die spezifischen Fragestellungen eines potenziellen Kunden unbeantwortet lassen kann.

Nutzermeinungen

Nutzermeinungen sind teilstandardisierte Qualitätsbewertungen, die es potenziellen Kunden erlauben, sich ein Bild der Qualität von Cloud-Service und Anbieter aus Nutzersicht zu verschaffen. Nutzermeinungen sind häufig auf die spezielle Sicht- und Nutzungsweise des Rezensenten beschränkt, bieten jedoch möglicherweise tiefere Einblicke in Aspekte wie die Handhabung oder den Kontakt zum Anbieter, als dies Expertenmeinungen tun. Ihre besondere Stärke liegt darin, dass in sie die Langzeiterfahrungen der Nutzer einfließen. Eine große Schwäche ist jedoch, dass die Aussagekraft der Be-

wertung von der Expertise des Rezensenten abhängt, die sich nicht oder nur schwer verifizieren lässt.

9.3.1.6 Anbieterprofil

Das Anbieterprofil beschreibt die wesentlichen, den Cloud-Service-Anbieter charakterisierenden Eigenschaften, die für die Auswahlentscheidung aus Kundensicht von Relevanz sind.

Stabilität des Anbieters

Die Stabilität des Service-Anbieters ist ein Indikator für die Wahrscheinlichkeit, dass das Cloud-Angebot dieses Cloud-Anbieters während der Vertragslaufzeit bestehen bleibt und der Cloud-Anbieter seine vertraglichen Verpflichtungen erfüllen kann. Als Stabilitätsindikatoren können neben dem Alter des Anbieterunternehmens auch Informationen über den Marktanteil eines Cloud-Service herangezogen werden. Der Marktanteil ist ein Maßstab für die Bedeutung, die dieser Service in einem bestimmten Marktsegment hat und stellt eine wesentliche Einflussgröße für den langfristigen Erfolg des Produktes dar.

Anzahl der Unternehmenskunden

Die Anzahl der Unternehmenskunden kann als Reputationskriterium für den Cloud-Service-Anbieter herangezogen werden, da mit einer steigenden Anzahl an Kunden eine allgemeine Zufriedenheit mit dem Leistungsportfolio des Cloud-Service-Anbieters in Zusammenhang stehen kann. Potenzielle Kunden sollten sich informieren, wie etabliert der Cloud-Service des Anbieters in der Unternehmenspraxis im Vergleich zu anderen Services ist. Diese Information kann jedoch nur als ein grober Indikator für die Qualität des Service angesehen werden. Eine Fokussierung auf diese Information alleine birgt für interessierte Kunden das Risiko, neue Cloud-Services oder Nischen-Services außer Acht zu lassen, die im konkreten Kundenkontext einen höheren Nutzen bieten können.

Corporate-Social-Responsibility

Corporate-Social-Responsibility bezeichnet die freiwillige, über die rechtlichen Verpflichtungen hinausgehende Übernahme gesellschaftlicher Verantwortung durch Unternehmen (Münstermann 2007, S. 16). Bedingt durch größere Transparenz und einen Wertewandel in der Gesellschaft werden Fragen der Gesellschaftsverantwortung für Kundenunternehmen immer wichtiger. Neben einer Selbstverpflichtung des Anbieters bei Arbeitsstandards können Selbstverpflichtungen in den Bereichen Umweltstandards und Lieferantenmanagement sowie in Bezug auf den Einsatz für den Datenschutz auf politischer Ebene relevant sein.

9.3.2 Technische Sicht

Die Merkmale der technischen Sicht sollen die Frage beantworten, ob der zu beziehende Cloud-Service alle technischen und organisatorischen Anforderungen, die das Kundenunternehmen und der Gesetzgeber stellen erfüllt werden. Zur Beantwortung dieser Frage sind die Einzelkriterien innerhalb der Dimensionen Sicherheit & Datenschutz, Interoperabilität & Performance sowie Features zu prüfen.

9.3.2.1 Datensicherheit

Eine hohe Datensicherheit ist nicht nur aus wirtschaftlicher oder wettbewerbllicher Sicht, sondern auch aus rechtlicher Sicht relevant (siehe § 9 BDSG). Insbesondere dann, wenn personenbezogene Daten verarbeitet oder gespeichert werden sollen, muss gewährleistet sein, dass die Anforderungen, die das BDSG an die Datensicherheit formuliert, erfüllt sind (vgl. Kapitel 15-18). Zu diesen Anforderungen gehören neben technischen auch organisatorische Sicherheitsmaßnahmen³.

Technische Sicherheitsmaßnahmen wie z. B. Verschlüsselungsverfahren, Alarmanlagen oder Videoüberwachung zielen darauf ab, physische Gefahrenquellen zu eliminieren. Zu diesen Gefahrenquellen gehören u. a. Feuer, Wasser und unerwünschte Fremdzugriffe. Organisatorische Sicherheitsmaß-

3 [www.bfdi.bund.de/bfdi_wiki/index.php/Technische_und_organisatorische_Maßnahmen](http://www.bfdi.bund.de/bfdi_wiki/index.php/Technische_und_organisatorische_Ma%C3%9Fnahmen), zugegriffen am 19.06.2014.

nahmen umfassen hingegen alle nicht-technischen Maßnahmen in Form von Handlungsanweisungen, Verfahren- und Vorgehensweisen⁴.

Sicherheitsmaßnahmen sind für insgesamt acht Bereiche zu ergreifen. Dazu gehören: (1) die Zutrittskontrolle, (2) die Zugangskontrolle, (3) die Zugriffskontrolle, (4) die Weitergabekontrolle, (5) die Eingabekontrolle, (6) die Auftragskontrolle, (7) die Verfügbarkeitskontrolle und (8) die Datentrennung⁵.

Kunden, die den Einsatz eines Cloud-Service für die Speicherung und Verarbeitung geschäftskritischer Daten und/oder personenbezogener Daten planen, sollten sich informieren, inwieweit der Cloud-Service-Anbieter eine datenschutzrechtlich konforme Verarbeitung und/oder Speicherung solcher Daten gewährleisten kann. Anhaltspunkte hierfür bieten die Kataloge des BSI-IT-Grundschutz⁶. Ob die vom Anbieter ergriffenen Maßnahmen jedoch ausreichend sind, ist jeweils vom Einzelfall abhängig.

Zertifikate staatlicher Organisationen und akkreditierter Prüfer

Zertifikate staatlicher Organisationen und akkreditierter Prüfer können dem Kunden Aufschluss über die Vertrauenswürdigkeit und Leistungsfähigkeit eines Cloud-Anbieters geben. Insbesondere dann, wenn der Kunde nicht die Möglichkeit hat, ein Audit beim Anbieter durchzuführen, können Zertifikate für Vertrauen in den Anbieter sorgen. Der Kunde sollte entsprechend analysieren, ob der Cloud-Anbieter über Zertifikate verfügt und über welche er verfügt.

4 [www.bfdi.bund.de/bfdi_wiki/index.php/Technische_und_organisatorische_Maßnahmen](http://www.bfdi.bund.de/bfdi_wiki/index.php/Technische_und_organisatorische_Ma%C3%9Fnahmen), zugegriffen am 19.06.2014.

5 www.gesetze-im-internet.de/bdsg_1990/anlage_79.html, zugegriffen am 19.06.2014.

6 www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node, zugegriffen am 19.06.2014.

Auditierbarkeit des Anbieters

Die Auditierung eines Cloud-Anbieters ermöglicht es dem Kunden, den Leistungserstellungsprozess des Anbieters in Bezug auf die Einhaltung von Anforderungen und Richtlinien, wie sie bspw. das BSI definiert (BSI 2013), zu evaluieren. Die Möglichkeit eines Audits hat Signalwirkung für den Kunden, jedoch bietet nicht jeder Anbieter diese Möglichkeit an.

Infrastruktur-Redundanz

Um Ausfallzeiten zu verringern, werden moderne Rechenzentren redundant aufgebaut. So kann der Ausfall kritischer Systemkomponenten kompensiert oder Systemkomponenten ohne Beeinträchtigung des laufenden Betriebs gewartet werden.

Für Kunden stellt sich die Frage, ob und in welchen Bereichen von Seiten des Cloud-Service-Anbieters Zusicherungen hinsichtlich der Infrastruktur-Redundanz bestehen. Relevante Infrastrukturkomponenten sind bspw. die Netzwerkanbindung, die Stromversorgung, die Klimatisierung oder sogar das komplette Rechenzentrum selbst.

9.3.2.2 Interoperabilität

Der Begriff der Interoperabilität stellt auf den Grad der technischen Kopplung zwischen zwei Cloud-Services oder zwischen einem Cloud-Service und den IT-Systemen des nutzenden Unternehmens ab. Die Kopplung beeinflusst den Umfang der Änderungen, die an der technischen Realisierung des aufrufenden Service vorgenommen werden müssen, wenn sich an der technischen Realisierung des aufgerufenen Service etwas ändert. Bei geringem Kopplungsgrad sind wenige, bei hohem Kopplungsgrad dagegen umfangreiche Änderungen notwendig. Die Nutzung einheitlicher Schnittstellen- und Kommunikationsstandards stellt eine Grundvoraussetzung für eine hohe Interoperabilität dar.

Datenexportfunktion zwischen verschiedenen Systemen

Insbesondere für den Fall eines notwendigen Wechsels des Cloud-Anbieters ist sicherzustellen, dass die vom Cloud-Service gehaltenen Daten bei Beendigung des Auftragsverhältnisses exportiert werden können. Das Fehlen einer solchen Funktion kann erhebliche Wechselkosten verursachen und damit die einseitige Abhängigkeit vom Cloud-Anbieter erhöhen. Kunden sollten sich informieren, ob der zu beziehende Cloud-Service über eine Datenexportfunktion verfügt.

Datenexportfunktion hinsichtlich der Datenformate

Ist die Möglichkeit für einen Datenexport gegeben, sollten Kunden prüfen, ob die Daten nach ihrem Export in einem für alternative Cloud-Services oder eine unternehmensinterne Softwarelösung verarbeitbaren Format vorliegen. Dies ist nicht nur für den Fall eines Anbieterwechsels relevant, sondern auch dann, wenn der Cloud-Anbieter selbst keine Backup-Funktion für die von ihm gehaltenen Kundendaten anbietet.

Datenimportfunktion zwischen verschiedenen Systemen

Um eine fehlerbehaftete händische Eingabe von Daten zu vermeiden, ist es für den Kunden wichtig zu erfahren, ob der Cloud-Anbieter eine Datenimportfunktion anbietet. Über eine solche Funktion lassen sich, soweit notwendig, Daten aus den Systemen des Kunden automatisiert zum Anbieter übertragen.

Datenimportfunktion hinsichtlich der Datenformate

Um eine aufwendige Datentransformation zu vermeiden oder deren Aufwand zu reduzieren, sollte der Datenimport ein für den Kunden kompatibles Format anbieten. Kunden sollten sich entsprechend informieren, in welchen Formaten Daten vorliegen müssen, um beim Cloud-Anbieter importiert werden zu können.

Unterstützte Schnittstellen

Durch eine medienbruchfreie Integration eines Cloud-Service in die Applikationslandschaft des Kunden (oder mit den Angeboten anderer Cloud-Anbieter) können Automatisierungspotenziale auf Geschäftsprozessebene ausgenutzt werden. Aufgrund von inkompatiblen Schnittstellen lässt sich allerdings u. U. nicht jeder Cloud-Service mit den im Kundenunternehmen eingesetzten IT-Systemen ohne größeren Aufwand integrieren. Kunden sollten sich darüber informieren, welche Schnittstellen zu den im Kundenunternehmen eingesetzten lokalen Software-Lösungen und Produkten von dem zu beziehenden Cloud-Service unterstützt werden.

9.3.2.3 Features

Unter Software-Features sind Unterscheidungsmerkmale einer Software im Sinne des Funktionsumfanges zu verstehen.

Zugriffsmöglichkeiten

Zugriffsmöglichkeiten umfassen die vom Cloud-Anbieter unterstützten Netzwerkprotokolle zum Fernzugriff. Während für einzelne, weniger komplexe Services ein Zugriff über eine Weboberfläche ausreichend sein kann, werden für andere Cloud-Services ggf. Zugriffsmöglichkeiten über Netzwerkprotokolle wie SSH oder SFTP benötigt.

Identitäts- und Rechtemanagement

Das Identitäts- und Rechtemanagement dient der Kontrolle des Zugriffs von Personen auf einen Cloud-Service und auf die von diesem gehaltenen Daten. Ziel ist es, den Zugriff auf den Service und die Daten durch unbefugte Personen zu verhindern. Ein Cloud-Anbieter sollte selbst ein Identitäts- und Rechtemanagement oder Schnittstellen zu externen Management-Lösungen anbieten (BSI 2012). Das Bundesamt für Sicherheit in der Informationstechnik definiert unterschiedliche Sicherheitsstufen für das Identitäts- und Rechtemanagement bei Cloud-Services sowie deren Ausgestaltung in Form organisatorischer, personeller und technischer Maßnahmen (BSI 2012). Der Kunde

sollte nicht nur prüfen, welche Sicherheitsmaßnahmen er benötigt, sondern auch inwieweit die vom Cloud-Anbieter bereitgestellte Management-Lösung funktionell seinen zukünftigen Anforderungen entspricht. Insbesondere dann, wenn ein Unternehmen schnell wächst, können der Aufbau eines eigenen Identitäts- und Rechtemanagements und die Anbindung des Cloud-Services an diese Management-Lösung aus Gründen der Komplexitätsbeherrschung sinnvoll sein. Dies gelingt jedoch nur, wenn der Cloud-Anbieter Schnittstellen zu externen Management-Lösungen anbietet. Anderenfalls sehen sich Kunden, die einen weitgehenden Bezug von IT-Services aus der Cloud planen, u. U. mit verschiedenen, parallel zu betreibenden Management-Lösungen konfrontiert.

Update-Management

Das Update-Management umfasst die vom Cloud-Anbieter zur Verfügung gestellten Maßnahmen zur Aktualisierung von Software oder Daten. Updates können zu einer temporär geringeren Performance des Cloud-Service führen oder die Erreichbarkeit des Service einschränken. Vor allem für Services, die geschäftskritische Prozesse unterstützen, sollten sich Kunden informieren, in welcher Form das Update-Management vom Cloud-Service-Anbieter realisiert wird. Neben einer automatischen Durchführung von Updates ist auch eine Terminierungsmöglichkeit von Updates durch den Kunden oder sogar eine Steuerungsmöglichkeit von Updates durch den Kunden denkbar.

9.3.3 Funktionale Sicht

Funktionale Merkmale von IT-Dienstleistungen werden zumeist hierarchisch angeordnet, um die Funktionalität sukzessive zu präzisieren. Im Kontext von Cloud-Services kann zunächst nach dem Service-Modell (Infrastruktur-Service, Plattform-Service oder Software-Service) unterschieden werden.

Innerhalb der drei Service-Modelle variiert die gewünschte Funktionalität jedoch sehr stark und hängt vom Unterstützungsbedarf ab, den ein Unternehmen hat. Zur Spezifikation der Anforderungen auf funktionaler Ebene ist eine gesonderte, dem gewünschten Dienstleistungsumfang entsprechende, funktionale Anforderungsanalyse vorzunehmen. Eine solche Analyse ist auf-

grund unterschiedlicher fachlicher, technischer und rechtlicher Anforderungen stets individuell für ein Unternehmen vorzunehmen. Dies kann eine Checkliste, die sich an kleine und mittlere Unternehmen im Allgemeinen richtet, nicht leisten. Daher wird an dieser Stelle nicht weiter auf mögliche funktionale Ausprägungen eingegangen.

9.3.4 *Operative Sicht*

Für Anwender ist es wichtig zu wissen, wie die bezogene Dienstleistung im operativen Betrieb den eigenen Anforderungen angepasst werden kann, wie von Seiten des Cloud-Anbieters auf Ausfälle reagiert wird und wie die Einhaltung von SLA überprüft werden kann.

9.3.4.1 Service-Management

Im Rahmen der Entscheidung für die Auswahl eines geeigneten Cloud-Service wird nachfolgend auf folgende Charakteristika eingegangen: Konfigurationsmöglichkeiten, Notfallmanagement – Reaktionszeit auf Ausfall, Notfallmanagement – Wiederanlaufzeit nach Serviceausfall, Backup und Self-Service.

Konfigurationsmöglichkeiten

Konfigurationsmöglichkeiten beziehen sich auf das Hinzufügen neuer Funktionalitäten, die über diejenigen der Basisfunktionalität des Cloud-Services hinausgehen. Bisher haben sich für Cloud-Services keine einheitlichen Schnittstellen- und Kommunikationsstandards etablieren können. Ein Grund hierfür ist darin zu sehen, dass manche Anbieter versuchen, mittels proprietärer Formate eigene, abgeschottete Ökosysteme um ihre Services herum aufzubauen. Wie in Kapitel 3 beschrieben, ist diese Strategie vergleichbar mit der der Hersteller von Smartphone-Betriebssystemen, die erst über die in die Betriebssysteme integrierten Stores den Zugriff auf Fremdanbietersoftware ermöglichen. Auf diese Weise können die Basisfunktionen des Mobilbetriebssystems über die Installation von Fremdsoftware um zusätzliche Funktionen erweitert werden. Analog zu den Smartphone-Betriebssystemen stellen einige der großen Cloud-Anbieter Plattformen zur Verfügung, über

die selbstständige Entwickler Cloud-Services anbieten können, welche die Cloud-Services des Plattformanbieters um zusätzliche Funktionen erweitern.

Gerade dann, wenn die zukünftig benötigte Funktionalität noch nicht abschätzbar ist oder ein weitreichender Bezug von IT-Services aus der Cloud für die Zukunft nicht ausgeschlossen wird, sollten sich Kunden über das Ökosystem des Cloud-Anbieters informieren. Relevante Kriterien für die Wahl des Anbieters und seines Ökosystems können sein: die Anzahl verfügbarer Cloud-Services im Ökosystem, die Wachstumsrate des Ökosystems hinsichtlich der Nutzerzahlen und der selbstständigen Service-Entwickler oder die relative Größe des Ökosystems im Vergleich zu anderen Ökosystemen.

Notfallmanagement – Ausfallreaktionszeit

Das Notfallmanagement im Rahmen der Reaktionszeit auf einen Ausfall der Serviceleistung bezieht sich auf die Zeit, die ein Cloud-Anbieter benötigt, um auf Störungen im IT-Betrieb zu reagieren. Zumindest für Services, die der Unterstützung des operativen Geschäftsbetriebs dienen, ist eine geringe Reaktionszeit von hoher Bedeutung. Kunden sollten sich informieren, wie lange der Anbieter des zur Wahl stehenden Cloud-Service benötigt, um auf eine Störung zu reagieren.

Notfallmanagement – Wiederanlaufzeit

Im Rahmen des Notfallmanagements wird unter der Wiederanlaufzeit die Summe aus Reparatur-, Anlauf- und Prüfzeit für die ausgefallene Ressource verstanden. Die Wiederanlaufzeit gibt also an, wie viel Zeit ein Cloud-Anbieter benötigt, um nach der ersten Reaktion auf einen Störfall die vollständige Betriebsfähigkeit des Service für den Kunden wiederherzustellen.

Backup

Ein Backup ist eine Datensicherung, die für den Fall des Auftretens eines Datenverlustes oder von Inkonsistenzen im Datenbestand angefertigt wird, um die Daten zurück in das Produktivsystem spielen zu können. In der Praxis

haben sich unterschiedliche Strategien etabliert, um eine Datensicherung durchzuführen. Die für den Kunden passende Backup-Strategie ist u. a. von speziellen gesetzlichen Anforderungen, denen die Datensicherung unterliegen kann,⁷ oder den Anforderungen des Kunden an die Verfügbarkeit der Daten abhängig. Der Kunde sollte sich in einem ersten Schritt informieren, ob und, wenn ja, welche Strategien zur Datensicherung vom Cloud-Anbieter angeboten werden. Im zweiten Schritt ist dann zu klären, ob die angebotene Backup-Strategie zu den Anforderungen des Kunden passt.

On-demand Self-Service

Unter On-demand Self-Service versteht man die automatische, ohne persönliche Interaktion mit dem Cloud-Service-Anbieter ablaufende Provisionierung von Ressourcen (z. B. Rechenleistung, Speicherplatz). Ein On-demand Self-Service kann es dem Kunden ermöglichen, schnell und flexibel zusätzliche Ressourcen in Anspruch zu nehmen.

9.3.4.2 SLA-Monitoring

Für einen effizienten Servicebetrieb ist die kontinuierliche Überwachung der Einhaltung der vereinbarten Service-Levels notwendig. Kunden sollten sich informieren, ob und in welcher Form (z. B. Erhebungszeiträume, Granularität) der Cloud-Anbieter Informationen über die eigene Einhaltung des SLA bereitstellt.

9.3.5 *Rechtliche Sicht*

Die rechtlichen Chancen und Risiken sind für den Cloud-Nutzer oft schwer abzuschätzen. Der Cloud-Nutzer trägt dennoch meist die rechtliche Verantwortung, insbesondere wenn er Informationen über andere Personen in einer Cloud speichert oder verarbeitet. Dabei spielt die Rechtssicherheit bei der Auswahl des richtigen Cloud-Services eine wesentliche Rolle.

Die rechtliche Sicht auf einen Cloud-Service umfasst Herausforderungen, die insbesondere durch die Virtualisierung von IT-Infrastrukturen bedingt

7 Vergleiche Abschnitt 9.3.5.2 in diesem Kapitel.

sind. Dabei finden sich Herausforderungen in allen Rechtsgebieten, vor allem aber im Datenschutzrecht, bei staatlichen Ermittlungen und bei IT-Compliance. Was im Rahmen der Rechtmäßigkeit zu beachten ist und im Rahmen der vorliegenden Checkliste für den Cloud-Nutzer von Relevanz sein kann, spiegelt sich in den Kapiteln 15-18 wider.

Beim Umgang mit dem Cloud-Computing müssen die Akteure zahlreiche Normen aus verschiedenen Rechtsgebieten beachten. Zwar muss der Cloud-Nutzer auf der einen Seite sicherstellen, dass die Nutzung des von ihm ausgewählten Cloud-Angebots nicht gegen diese Regelungen verstößt. Auf der anderen Seite bestimmen aber meist die Cloud-Anbieter über den Rahmen der Möglichkeiten der Cloud-Nutzung einschließlich einzelner Vertragsbedingungen. Dem Cloud-Nutzer bleibt also nur, bereits bei der Auswahl darauf zu achten, dass die vom Cloud-Anbieter angebotenen Bedingungen den rechtlichen Anforderungen, die er als Cloud-Nutzer beachten muss, entsprechen.

9.3.5.1 Umgang mit personenbezogenen Daten

Soweit die Erhebung, Verarbeitung oder Nutzung von Daten, die auch Dritte betreffen, in der Cloud erfolgen soll, muss der Cloud-Nutzer das Datenschutzrecht beachten.⁸ Der Cloud-Nutzer muss daher für sich die Frage beantworten, ob er personenbezogene Daten (beispielsweise Kunden- oder Mitarbeiterdaten) in der Cloud speichern oder verarbeiten will.

Soweit er für personenbezogene Daten die Cloud nutzen will, kann der Cloud-Nutzer auch aufgrund eines bestimmten Berufes einer zusätzlichen Geheimhaltungsverpflichtung unterliegen.⁹

Viele Cloud-Anbieter befinden sich im Ausland oder greifen auf ausländische Server zurück. Eine Übertragung von Daten außerhalb der EU/EWR ist beim Cloud-Computing in der Regel nicht zulässig.¹⁰ Für den Cloud-Nutzer kann es relevant sein, ob der Cloud-Anbieter Angaben über die mög-

8 Vergleiche dazu ausführlich Kapitel 15.

9 Vergleiche dazu ausführlich Kapitel 17.

10 Vergleiche dazu ausführlich Kapitel 23.

lichen Standorte der Server macht und dabei die Datenspeicherung und -verarbeitung ausschließlich innerhalb der EU/EWR garantiert.

9.3.5.2 Aufbewahrungspflichten

Bestimmte Dokumente unterliegen gesetzlichen Aufbewahrungspflichten und müssen über den im Gesetz bestimmten Zeitraum zuverlässig zugänglich sein. Der Cloud-Nutzer muss für sich die Frage beantworten, ob entsprechende Pflichten auf ihn zutreffen und der Cloud-Anbieter den consequenten Zugriff über viele Jahre garantiert.

9.3.5.3 Staatliche Überwachungs- und Ermittlungsmaßnahmen

Cloud-Angebote ermöglichen vereinfacht den Zugriff von Seiten öffentlicher Institutionen auf digitale Daten, sei es zu polizeilichen Überwachungs- und strafrechtlichen Ermittlungszwecken oder bei Industriespionage insbesondere aus dem Ausland.

Cloud-Anbieter könnten von ihrem ausländischen Staat verpflichtet werden, einen Zugriff auf gespeicherte Daten zu ermöglichen.¹¹ Für den Cloud-Nutzer sollte es von Interesse sein, ob der Cloud-Anbieter in einer rechtlichen Abhängigkeit zu anderen Unternehmen im Ausland steht.

Inländische staatliche Zugriffe unterliegen strengen gesetzlichen Voraussetzungen.¹² Der Cloud-Anbieter kann dabei rechtlich gehindert sein, über einen erfolgten Zugriff von Ermittlungsbehörden zu informieren.¹³ Für den Cloud-Nutzer kann es notwendig sein zu wissen, ob der Cloud-Anbieter die Absicht hat, über die Weitergabe von Daten an Behörden, soweit ihm dies gesetzlich nicht verboten ist, gegenüber dem Cloud-Nutzer Auskunft zu erteilen.

11 Vergleiche dazu ausführlich Kapitel 18.

12 Vergleiche dazu ausführlich Kapitel 18.

13 Vergleiche dazu ausführlich Kapitel 18 und 23.

9.3.5.4 Verschlüsselungstechniken

Viele rechtliche Risiken lassen sich mit Hilfe technischer Mittel, wie der Verschlüsselung, reduzieren. Voraussetzung ist allerdings, dass der Cloud-Nutzer die Daten verschlüsselt und der Cloud-Anbieter den Schlüssel nicht kennt.¹⁴ Daher ist es für den Cloud-Nutzer von besonderer Relevanz zu wissen, ob der Cloud-Anbieter die Speicherung verschlüsselter Daten, die der Cloud-Nutzer vor der Übertragung nach dem neuesten Stand der Technik verschlüsselt hat, erlaubt. Dabei sollte der Cloud-Nutzer zeitgleich wissen, dass eine Datenverarbeitung in der Cloud an verschlüsselten Daten nur bedingt möglich ist.

9.4 Literaturverzeichnis

- BSI (2012):** Sicherheitsempfehlungen für Cloud Computing Anbieter – Mindestanforderungen in der Informationssicherheit. Bonn: Bundesamt für Sicherheit in der Informationstechnik.
- BSI (2013):** Vorabversion Baustein Cloud Management. *IT-Grundschutz*: Bundesamt für Sicherheit in der Informationstechnik.
- Hilley, D. (2009):** Cloud computing: A taxonomy of platform and infrastructure-level offerings. Georgia Institute of Technology, 2009.
- Hoberg, P.; Reidt, A.; Wollersheim, J.; Krcmar, H. (2014):** CloudServiceCheck, Ausgabe 1, 2014.
- Hoberg, P.; Wollersheim, J.; Krcmar, H. (2012):** Service Descriptions for Cloud Services – The Customer's Perspective. Präsentiert auf der ConLife Academic Conference 2012, Köln, Deutschland.
- Hoefer, C.N.; Karagiannis, G. (2010):** Taxonomy of cloud computing services. Präsentiert auf dem IEEE Globecom Workshop on Enabling the Future Service-Oriented Internet.
- Koehler, P.; Anandasivam, A.; Dan, M.; Weinhardt, C. (2010):** Customer Heterogeneity and Tariff Biases in Cloud Computing. Präsentiert auf der 31th International Conference on Information Systems.
- Krcmar, H. (2010):** Informationsmanagement (5. Ausgabe), Springer, Heidelberg, Deutschland 2010.
- Li, A.; Yang, X.; Kandula, S.; Ming, Z. (2011):** Comparing Public-Cloud Providers. In: Internet Computing, IEEE, Vol. 15 (2011) No. 2, S. 50-53.
- Münstermann, M. (2007):** Corporate Social Responsibility – Ausgestaltung und Steuerung von CSR-Aktivitäten (1. Ausgabe), Gabler, Wiesbaden, Deutschland 2007.

14 Vergleiche dazu ausführlich Kapitel 18.

- Prodan, R.; Ostermann, S. (2009):** A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers. Präsentiert auf der 10th IEEE/ACM International Conference on Grid Computing, Las Vegas, USA.
- Repschläger, J.; Wind, S.; Zarnekow, R. (2011):** Klassifikationsrahmen für die Anbietersauswahl in der Cloud. Präsentiert auf der Jahrestagung der Gesellschaft für Informatik / Workshop: Neue Aspekte der zwischenbetrieblichen Integration durch Enterprise 2.0 (IOS 2.0), Berlin, Deutschland.
- Repschläger, J.; Wind, S.; Zarnekow, R.; Turowski, K. (2012):** A Reference Guide to Cloud Computing Dimensions: Infrastructure as a Service Classification Framework. Präsentiert auf der 45th Hawaii International Conference on System Sciences, Maui, Hawaii.
- Rimal, B.P.; Choi, E.; Lumb, I. (2009):** A Taxonomy and Survey of Cloud Computing Systems. Präsentiert auf der 5th International Joint Conference on INC, IMS and IDC, Seoul, Korea.
- Wollersheim, J.; Krcmar, H. (2013):** Purchasing processes for cloud services – An exploratory study of process influencing factors. Präsentiert auf der 22nd Annual IPSERA Conference, Nantes, Frankreich.
- Youseff, L.; Butrico, M.; Da Silva, D. (2008):** Toward a unified ontology of cloud computing. Präsentiert auf dem Grid Computing Environments Workshop, 2008, Austin, USA.

10 Servicebeschreibung – Entwicklung eines domänenspezifischen Vokabulars (eUSDL)

J. Wollersheim, H. Krcmar

In diesem Beitrag werden eine Erweiterung der allgemeinen Servicebeschreibungssprache USDL um domänenspezifisches Vokabular (eUSDL) sowie beispielhafte Sets von Qualitätskriterien zur Unterstützung von Cloud-Service-Kunden bei der einmaligen Qualitätsbewertung während Such- und Beschaffungsaktivitäten (Suche) wie auch bei der kontinuierlichen Qualitätsbewertung während der Servicenutzung (Bewertung) beschrieben.

10.1 Einleitung

Wie im vorhergehenden Kapitel 9 erläutert, ist es eine große Herausforderung für Unternehmen, alle im Beschaffungsprozess relevanten Qualitätsinformationen bezüglich der am Markt verfügbaren und prinzipiell in Frage kommenden Serviceangebote zu eruieren. Der im vorhergehenden Kapitel erläuterte Katalog von Qualitätskriterien kann beschaffende Unternehmen bereits unterstützen. Um den Informationsaustausch zwischen beschaffenden und anbietenden Unternehmen nicht nur inhaltlich zu strukturieren, sondern auch effizienter zu gestalten, ist eine Vereinheitlichung des verwendeten Vokabulars beider Unternehmen notwendig, um Missverständnisse und in Folge Abweichungen zwischen dem Leistungsbedarf auf der einen und der verfügbaren Servicequalität auf der anderen Seite zu vermeiden. Es ist die Frage zu beantworten:

- Welche Vokabulare können die identifizierten Qualitätskriterien von Cloud-Services weiter konkretisieren und beschreiben, etwa um Servicebeschreibungen möglichst vollständig und eindeutig zu verfassen?

Der nachfolgende Abschnitt 10.2 widmet sich der Beantwortung dieser Frage und stellt eine Erweiterung und Konkretisierung der Servicebeschreibungssprache USDL vor. Aus Sicht des beschaffenden Unternehmens ist neben

einem verlässlichen Vokabular auch ein effizienter Beschaffungsprozess wünschenswert. Die Bewertung von Serviceangeboten sollte entsprechend nur die notwendigen Qualitätskriterien umfassen. Hieraus ergibt sich die Frage:

- Lassen sich exemplarisch für einzelne Typen von Cloud-Services Abweichungen bzgl. der Wichtigkeit der einzelnen Qualitätskriterien identifizieren?

Abschnitt 10.3 widmet sich der Beantwortung dieser Frage. Abschließend bleibt zu klären, welche Qualitätsaspekte eines Services im Anschluss an den Beschaffungsvorgang, also während der kontinuierlichen Nutzung von Cloud-Services aus Sicht des Service-nutzenden Unternehmens, von Relevanz sind. Abschnitt 10.4 beschäftigt sich mit der Beantwortung dieser Frage:

- Welche Kriterien sind für die Bewertung der wahrgenommenen Servicequalität von Cloud-Services passend?

10.2 USDL-Erweiterung zur Beschreibung von Cloud-Services (eUSDL)

Cloud-Services werden, wie einleitend in Kapitel 2 dieses Buches beschrieben, per Definition mit vergleichsweise geringer menschlicher Interaktion zwischen Käufer und Verkäufer beschafft und in die bestehende Systemlandschaft integriert (NIST 2011). Interaktion zum Zwecke des Informationsaustauschs während des Beschaffungsprozesses, aus Sicht des beschaffenden Unternehmens, findet im Wesentlichen in elektronischer Form statt, etwa über Marktplätze, Portale oder die Webseite des Service-Anbieters. Um den Austausch von Informationen zwischen Service-Anbieter und Kunde zu erleichtern und auch in Teilen maschinell zu ermöglichen, ist eine entsprechend standardisierte Beschreibung des Service-Angebots notwendig. Diese Service-Beschreibung sollte aus Sicht des beschaffenden Unternehmens nicht nur alle benötigten Informationen enthalten, sondern auch möglichst gut strukturiert und aussagekräftig sein, sowie ein eindeutig definiertes Vokabular verwenden.

Aufbauend auf den im vorhergehenden Kapitel 9 dieses Buchs beschriebenen Qualitätskriterien zur möglichst vollständigen Beschreibung von Cloud-Services aus der Sicht eines beschaffenden Unternehmens, wird nachfolgend versucht, das zur Beschreibung der einzelnen Kriterien verwendete Vokabular zu vereinheitlichen und mit bekannten Vokabularen zu verknüpfen. Zu diesem Zweck wird untersucht, welche der im Qualitätskriterien-Katalog verwendeten Aspekte bereits mittels der universellen Beschreibungssprache für Services (USDL) adressiert werden können. Ergänzend wird aufgezeigt, mittels welcher Vokabulare einzelne Qualitätsaspekte bereits abgebildet werden können und welche Ergänzungen notwendig sind.

10.2.1 Bestehende Herausforderungen

Da die von Cloud-Services erwartete Funktionalität aus Kundensicht stark variiert, werden nachfolgend zunächst nicht-funktionale Aspekte fokussiert. Nicht-funktionale Eigenschaften eines Services sind solche, die beschreiben, wie der Service die Bedürfnisse eines Nutzers erfüllt, also z.B. Erreichbarkeit, Performance und Verfügbarkeit des Services (Robertson 2006). Um das von KMUs benötigte Set an nicht-funktionalen Service-Merkmalen (identifiziert und zusammengefasst in Kapitel 9 dieses Buches) weiter zu strukturieren, verwenden wir die Unified Service Description Language (USDL) als Ausgangspunkt. Die Servicebeschreibungssprache USDL ermöglicht es, die wesentlichen Konzepte und Beziehungen zwischen Qualitätseigenschaften zu modellieren, inklusive etwaiger Schnittstellen und geschäftlicher Details wie etwa der Preisgestaltung (Oberle et al. 2013).

10.2.2 Vorstellung der Servicebeschreibungssprache USDL

Ziel der Servicebeschreibungssprache USDL ist es, Services umfassend und ganzheitlich zu beschreiben (Barros et al. 2011). USDL bringt geschäftliche, operative und technische Informationen in eine einheitliche Sprache. USDL ist die bis heute verbreitetste Service-Beschreibungssprache (Oberle et al. 2013), bei der existierende Schemata zur Servicebeschreibung nach dem Prinzip von „Linked Data“ verbunden wurden, was zur aktuellen Version

Tabelle 1: Module der Linked USDL (Basierend auf Pedrinaci/Leidig 2013)

Modul	Beschreibung
USDL-Core	Wortschatz der Linked USDL-Core bildet den Kern der Linked USDL und deckt die wesentlichen Konzepte wie die Definition eines Services, einer Service-Suite oder einer Service-Komposition sowie deren Beziehungen, Interaktionen und Abhängigkeiten ab. Dabei werden manche Service-Merkmale wie Anbieter oder Agent nicht erneut definiert, sondern stattdessen mit bestehenden Ontologien wie der FOAF-Ontologie verbunden.
USDL-Pricing	Dieses Modul befasst sich mit der Preisgestaltung von Services. Da die Preisgestaltung von Services dem Einsatz des Services oftmals vorausgeht (z.B. weil die exakte Anzahl an Stunden, die der Service in Anspruch genommen wird, noch nicht bekannt ist), müssen Preiskonzepte definiert werden, die es ermöglichen, Kosten an die Service-Nutzung zu binden, den Preis an die angefallenen Kosten anzupassen oder Preisobergrenzen und Flat Rates für bestimmte Zeitperioden zu definieren. Um flexibel und generisch genug zu sein, dass sie mit dieser Komplexität umgehen können, bilden die Klassen PricePlan, PriceComponent und PriceLevel die Basiselemente des Linked USDL-Preismoduls.
USDL-SLA	Dieses Linked USDL-Modul deckt den Wortschatz ab, der sich mit der Definition der Service Level Agreements (SLAs) befasst. SLAs werden für gewöhnlich eingesetzt, um Konditionen wie z.B. eine garantierte Erreichbarkeit eines Services zu spezifizieren. Für Kunden bieten Service-Level nicht nur Information über die Qualität eines Services an, die man erwarten kann, sondern stellen darüber hinaus ein rechtliches Übereinkommen an Strafen und Kompensationen im Falle einer Nichteinhaltung dar.

“Linked USDL” führte (Pedrinaci/Leidig 2013). Der in USDL benutzte Wortschatz ist aufgeteilt in drei Module: “USDL Core”, “USDL Pricing” und “USDL SLA” (siehe [Tabelle 1](#)). Jedes Modul definiert dabei ein Set an Klassen und Eigenschaften, wobei einige mit Ontologien wie GoodRelations (GR) (Hepp 2013) oder FOAF (Brickley 2013) verbunden sind und diese somit das Vokabular zur Servicebeschreibung vorgeben. GoodRelations adressiert Eigenschaften, die für E-Commerce benötigt werden, wohingegen das Vokabular von FOAF auf die Modellierung von sozialen Beziehungen, Netzwerken und deren Akteuren abzielt.

10.2.3 Vorgehen zur Identifikation des benötigten Vokabulars

Zur Identifikation des zur Beschreibung von Cloud-Services aus Anwendersicht benötigten Vokabulars wurde auf einer Vorabversion (Stand 2013) der in Kapitel 9 beschriebenen Sammlung von Qualitätskriterien aufgebaut. Ergänzend wurden Gruppeninterviews mit Praktikern durchgeführt, um domänenspezifisches Wissen und Einblicke in die Eigenschaften von Cloud-Services zu gewinnen, die in der Unternehmenspraxis relevant sind. So konnte die weitestgehend auf Basis von Literaturquellen entstandene Sammlung von Qualitätskriterien verfeinert werden.

Zur Einführung in die Thematik wurde in den mit Praktikern geführten Interviews zunächst der literatur-basierte Katalog von Qualitätsmerkmalen vorgestellt. Im Anschluss daran wurde der Merkmalskatalog detailliert diskutiert. Jedes Gruppenmitglied wurde gebeten, den eigenen Beschaffungsprozess gedanklich durchzugehen und die gegebenen Service-Merkmale nach ihrer Wichtigkeit zu sortieren. Dabei wurden die Teilnehmer dazu ermutigt, ihre Entscheidungen zu diskutieren, so als ob sie diese mit ihren Kollegen innerhalb ihrer Arbeitsumgebung diskutieren würden.

Nach etwa 1,5 Stunden der Diskussion innerhalb jeder Gruppe wurden die Merkmal-Rankings und Notizen eingesammelt. In einem zweiten Schritt wurden die Servicemerkmale, die von einer Service-Beschreibungssprache für Cloud-Services abgedeckt werden sollten, nach den Bedürfnissen der Stakeholder gruppiert. Die Ergebnisse zeigen, dass mehrere Abteilungen an der Beschaffung von Services beteiligt sind. Deshalb bietet es sich an, dass die unterschiedlichen Bedürfnisse dieser Abteilungen auch im Prozess der Entscheidungsfindung abgebildet werden. In Übereinstimmung mit bspw. Hoberg et al. (2012), wurden die Qualitätsmerkmale im Anschluss in die Kategorien „Basis“, „Technische Aspekte“, „Operative Aspekte“ und „Rechtliche Aspekte“ aufgeteilt.

Der Basis-Kategorie konnten Merkmale wie Performance des Services, Internationalität des Supports, Multi-Mandatenfähigkeit, irreversible Datenlöschung nach Vertragsende oder die Bekanntmachung von Bestandskunden und deren Feedback hinzugefügt werden. Bezüglich der technischen Kategorie befanden sich Sicherheitsmaßnahmen, unterstützte Schnittstellen zu Softwarelösungen (Name und Version), unterstützte Schnittstellen zu PaaS-Lö-

sungen (Name und Version), unterstützte Schnittstellen zu IaaS-Lösungen (Name und Version) sowie Möglichkeiten des Zugangs und der Authentifizierung unter den verfeinerten und hinzugefügten Merkmalen. Im operativen Bereich zeigten die Gruppeninterviews, dass Backup und Recovery wesentliche Servicemerkmale sind, die in einer Cloud-Service-Beschreibung vorhanden sein müssen. Des Weiteren zeigten die Workshops, dass eine Qualitätsaussage bezüglich der zugesicherten „Fähigkeit zur Datensicherheit“ ebenfalls Teil der Beschreibung sein sollte.

10.2.4 Ergebnisbeschreibung – eUSDL

Vergleicht man die zusammengefassten Anforderungen an die Inhalte von Cloud-Service-Beschreibungen mit den Möglichkeiten der Service-Beschreibungssprache USDL, so erhält man gemischte Ergebnisse. Auf der einen Seite sind manche Service-Merkmale bereits gut abgedeckt. Bei näherer Betrachtung fällt jedoch auf, dass manche wichtigen Aspekte nur teilweise von USDL abgedeckt werden oder eine sehr undifferenzierte und wenig aussagekräftige Beschreibung erlauben. Zum Beispiel ist es für Unternehmen wichtig, über bestimmte Servicemerkmale, wie z.B. Service-Levels, welche die garantierte Erreichbarkeit und Skalierbarkeit eines Cloud-Services betreffen, gut unterrichtet zu sein. Trotz dieses Bedürfnisses sind diese Servicemerkmale nicht explizit Teil der USDL. Sie könnten zwar in USDL durch den GoodRelations-Wortschatz als multiple Service-Ebenen beschrieben werden (d.h. als qualitative und quantitative Werte), aber die resultierende Beschreibung ist recht verwirrend, da die abgedeckten Eigenschaften von Service zu Service variieren. Ein expliziter Leitfaden zur Beschreibung von Service-Level-Merkmalen, die im Cloud-Service-Ökosystem benötigt werden, könnte diesen Bedarf adressieren und so die Vergleichbarkeit von Services aus Sicht der Kunden verbessern. Des Weiteren ist z.B. das Merkmal Bezahlmethode momentan nicht in der Service-Beschreibungssprache USDL definiert, obwohl es für Kunden im Cloud-Service-Ökosystem notwendig ist und sogar in der GoodRelations-Ontologie enthalten wäre. [Tabelle 2](#) bietet einen detaillierten Überblick des gerade beschriebenen Abgleichs bzgl. der Eigenschaften in der Kategorie „Basis“.

Tabelle 2: Basis-Eigenschaften

Sub-Class	Qualitätseigenschaft	Abgedeckt von USDL	Referenz. Ontologie
SLA-Generisch	Guaranteed service level (state and actions upon preconditions)	ja (SLA)	USDL + GR
SLA-Generisch	Preconditions for service level guarantees	nein	
SLA-Generisch	Guaranteed availability of service (time in %)	generisch	GR
SLA-Generisch	Guaranteed scalability of service (e.g. amount of users changeable)	generisch	GR
SLA-Generisch	Guaranteed performance of service (e.g. amount of parallel users supported)	generisch	GR
SLA-Generisch	Initial provisioning time (hours until the service can be used)	generisch	GR
SLA-Generisch	Elasticity (e.g. hours until more/less users can use the service)	generisch	GR
SLA-Customer Support	Response time of provider (hours) upon customer requests	generisch	GR
SLA-Customer Support	Communication channels for customer requests	generisch	GR
SLA-Customer Support	Coverage and volume of support obligations	generisch	GR
SLA-Customer Support	Internationality of support obligations	generisch	GR
Contract Components – Generisch	Place of service provision (place where data are processed & stored)	nein	
Contract Components – Generisch	Liability and compensation in case of SLA-under-performance	ja (SLA)	USDL + GR

Sub-Class	Qualitätseigenschaft	Abgedeckt von USDL	Referenz. Ontologie
Contract Components – Generisch	Duration of contract and binding-length for customer	nein	
Contract Components – Generisch	Naming of (sub-) contractors	generisch	GR
Contract Components – Generisch	Guaranteed data separation (Multi-tenancy)	nein	
Contract Components – Generisch	Guaranteed deletion of data upon termination of contract	generisch	GR
Contract Components – Pricing	Price plan and components (plan on how a service's price composes)	ja (Pricing)	USDL + GR
Contract Components – Pricing	Guaranteed price stability (amount of days)	nein	
Contract Components – Pricing	Amount of factors involved in price-formation	ja (Pricing)	USDL + GR
Contract Components – Pricing	Payment method	nein	
Contract Components – Pricing	Payment conditions (e.g. monthly, yearly, upon threshold, etc.)	nein	
References	Reference customer(s) (e.g. name)	nein	
References	Service assessment by experts	nein	
References	Service assessment by customers	nein	
Provider Profile	Name and address of provider	ja (Core)	FOAF

Sub-Class	Qualitätseigenschaft	Abgedeckt von USDL	Referenz. Ontologie
Provider Profile	Experience of provider (amount of months)	nein	
Provider Profile	Market share of service (%)	nein	
Provider Profile	Stability of provider (e.g. years since formation)	nein	
Provider Profile	Amount of enterprise customers using service	nein	
Provider Profile	Corporate social responsibility of provider	nein	
Provider Profile	Location (data center, office of provider)	generisch	GR

Ähnlich wie die Aspekte bezüglich der Service-Levels innerhalb des Basis-Bereichs könnten technische Servicemerkmale wie Sicherheit und Datenschutz mit USDL beschrieben werden. Da die notwendigen Aspekte allerdings nicht von USDL vordefiniert sind und daher der Freiheitsgrad sowohl für Anbieter, die ihre Services beschreiben, als auch für Kunden, die die Beschreibungen interpretieren, groß ist, resultiert eine hohe Varianz zwischen den Service-Beschreibungen für ähnliche Services. Da dies den Vergleich zwischen verschiedenen Services erschwert, wurde versucht, die Merkmale stärker zu standardisieren, was allerdings nicht mit Hilfe von USDL realisiert werden konnte. Ähnlich wie die in der Basis-Kategorie zusammengefassten Merkmale (siehe oben), könnten technische Merkmale zwar teilweise mit USDL abgedeckt werden. Da diese Sprache jedoch einen hohen Freiheitsgrad in Bezug darauf hat, wie spezielle Aspekte von Anbietern beschrieben werden, schränkt dies die Vergleichbarkeit von Services ein. So könnte bspw. ein sicherheits- und datenschutzrechtlicher Aspekt wie eine garantiert redundante Infrastruktur mittels dem Service-Level-Beschreibungselement von USDL beschrieben werden. Allerdings ist diese Information nicht verpflichtend und wird so nicht explizit von Anbietern gefordert. Des Weiteren deckt USDL Merkmale bezüglich Interoperabilität und Portabilität von Services wie z.B. Daten-Export-Formate nicht ab. [Tabelle 3](#) fasst diese Ergebnisse zusammen.

Tabelle 3: Technische Aspekte

Sub-Class	Qualitätseigenschaft	Abgedeckt von USDL	Referenz. Ontologie
Security & Data Privacy	Security measures – organizational	generisch	GR
Security & Data Privacy	Security measures – personnel-wise	generisch	GR
Security & Data Privacy	Security measures – infrastructure	generisch	GR
Security & Data Privacy	Security measures – technical	generisch	GR
Security & Data Privacy	Certificates – issued and acknowledged by gov. organizations	generisch	GR
Security & Data Privacy	Certificates – issued by an accredited validator	generisch	GR
Security & Data Privacy	Auditability of provider by customers	nein	
Security & Data Privacy	Redundant infrastructure guaranteed	generisch	GR
Interoperability and Portability	Dependability of service upon other/underlying services	ja (Core)	USDL
Interoperability and Portability	Functionality to export data – available	nein	
Interoperability and Portability	Functionality to export data – formats	nein	
Interoperability and Portability	Functionality to import data – available	nein	
Interoperability and Portability	Functionality to import data - formats	nein	
Interoperability and Portability	Information reg. data export/import	nein	
Interoperability and Portability	Interfaces to applications	ja (Core)	USDL

Sub-Class	Qualitätseigenschaft	Abgedeckt von USDL	Referenz. Ontologie
Interoperability and Portability	Interfaces to PaaS solutions	ja (Core)	USDL
Interoperability and Portability	Interfaces to IaaS solutions	ja (Core)	USDL
Features	Network configuration capabilities	nein	
Features	Service and data access possibilities	nein	
Features	Authentication possibilities	nein	
Features	Network connection – bandwidth and redundancy	nein	

Bezüglich der Servicemerkmale, die operative Aspekte betreffen, wie bspw. SLA-Monitoring oder Service-Management (z.B. der Umgang mit Backup und Recovery), adressiert USDL diese, in unserer empirischen Studie identifizierten Merkmale nicht. Die Feststellung dieser Merkmale, die von Unternehmen in der Unternehmenspraxis angesprochen wurden, und die Identifizierung von passenden Ontologien wird momentan nicht von der USDL unterstützt, wie [Tabelle 4](#) zeigt.

Bezüglich der Servicemerkmale, die rechtliche Aspekte wie Gewährleistungen für bestimmten Privatschutz betreffen, bietet USDL eine generische Lösung basierend auf der GoodRelations-Ontologie an. Wie zuvor allerdings schon angemerkt, ist eine Konkretisierung notwendig, um die Vergleichbarkeit von Services, wie sie von (Kunden-)Unternehmen gefordert wird, zu gewährleisten. [Tabelle 5](#) fasst diese identifizierten Ergebnisse zusammen.

Tabelle 4: Operative Aspekte

Sub-Class	Qualitätseigenschaft	Abgedeckt von USDL	Referenz. Ontologie
Service Management	Service configuration possibilities	nein	
Service Management	Handling of emergencies – response time	nein	
Service Management	Handling of emergencies – duration of restart after failure	nein	
Service Management	Backup possibilities	nein	
Service Management	Recovery possibilities	nein	
Service Management	Self service possibilities	nein	
Service Management	Update-management possibilities	nein	
SLA-Monitoring	SLA-monitoring possibilities	nein	

Tabelle 5: Rechtliche Aspekte

Sub-Class	Qualitätseigenschaft	Abgedeckt von USDL	Referenz. Ontologie
Warranties	Degree of protection sufficient to store & process personal data (§9 BDSG)	generisch	GR
Warranties	Degree of protection sufficient to store & process data subject to §257 HGB	generisch	GR
Warranties	Degree of protection sufficient to store & process data subject to §147 Abgabenordnung	generisch	GR

10.3 Entwicklung von Qualitätskriterien-Sets für variierende Beschaffungsobjekte

Aufbauend auf der bereits im wissenschaftlichen Kontext von Wollersheim et al. (2013) erfolgten Veröffentlichung zum Thema dieses Abschnitts werden nachfolgend die wesentlichen Aspekte kurz zusammengefasst.

10.3.1 Bestehende Herausforderungen

Um einer Organisation die Spezifikation ihres Bedarfs an unternehmensextern zu beschaffenden IT-Services zu erleichtern, können Kriterien-Kataloge wie der in Kapitel 9 dieses Buches vorgestellte Katalog verwendet werden. Typischerweise beeinflusst jedoch der Anwendungsbereich eines Services die Zusammensetzung des Buying Centers (weitere Ausführungen in Kapitel 4 dieses Buches), also der an der Beschaffung beteiligten Personen (Wynstra et al. 2006), und somit die detaillierte Ausgestaltung der Bedarfsspezifikation. Ein Cloud-Service, der IT-Infrastrukturbedarfe adressiert, wird zumeist federführend von Mitarbeitern einer IT-Abteilung beschafft. Services, die demgegenüber der Steuerung von Kundeninteraktionen und Marketingkampagnen dienen, werden hingegen eher von Mitarbeitern einer entsprechenden Fachabteilung beschafft. Um Anbieter von Cloud-Services bei der notwendigen, zielgruppenorientierten Ausformulierung ihrer Servicebeschreibungen zu unterstützen, erscheint entsprechend eine Berücksichtigung des jeweils typischen Service-Einsatzbereiches und des Informationsbedarfs der in diesem Fall federführend tätigen Beschaffer notwendig.

10.3.2 Vorgehen zur Identifikation des Kriterien-Sets

Auf Basis empirischer Erkenntnisse aus Gruppeninterviews mit Praktikern konnte bestätigt werden, dass die in der Servicebeschreibung erwarteten Informationen während des Beschaffungsprozesses in Abhängigkeit vom Anwendungsbereich eines Services variieren. Der Beschaffungsprozess von Unternehmen wird von einer Vielzahl von Aspekten beeinflusst, wie etwa dem Typ des Beschaffungsobjekts. Die Forschung hat gezeigt, dass typischerweise unterschiedliche Personengruppen an der Beschaffung beteiligt sind, in Abhängigkeit vom Typ des Beschaffungsobjekts. Da der persönliche Erfahrungsschatz und fachliche Hintergrund der Beschaffer und somit der

vorherrschende Informationsbedarf variieren, werden im Gleichklang variierende Informationen als Teil einer Cloud-Service-Beschreibung erwartet. In Abhängigkeit vom Typ des zu beschaffenden Cloud-Service wird nachfolgend ein solch variierender Informationsbedarf exemplarisch aufgezeigt.

Um die notwendigen Daten zu sammeln, wurden Interviews mit zwölf Entscheidungsträgern aus kleinen und mittelgroßen Unternehmen geführt. Die Interviews folgten alle einem einheitlichen Muster. Zunächst wurde der in Kapitel 9 dieses Buches dargelegte Katalog von Serviceeigenschaften erläutert und diskutiert. Im Anschluss wurden die Interviewpartner gebeten, sich für ein Beschaffungsszenario zu entscheiden, zu dem sie im weiteren Verlauf des Interviews detailliert befragt werden möchten. Den Interviewpartnern standen die folgenden zwei Szenarien zur Auswahl:

- 1) Beschaffung einer Software-as-a-Service (SaaS) wie etwa CRM oder ERP,
- 2) Beschaffung eines Services, der Plattform- oder Infrastruktur-Leistungen anbietet, etwa kollaborative Speicherlösungen für abteilungsübergreifende Teams.

Typischerweise werden Cloud-Service anhand der drei Servicemodelle SaaS, PaaS und IaaS unterschieden (Durkee 2010; Kaisler/Money 2011; Sarkar/Young 2011), siehe hierzu auch Kapitel 2 dieses Buches. Jedoch ist es aus wissenschaftlicher Sicht nahezu unmöglich, zwischen den Modellen PaaS und IaaS eine klare Trennung vorzunehmen (Armbrust et al. 2010). Um diese Abgrenzungsproblematik in den Interviews nicht thematisieren zu müssen, wurden beide Modelle in Anlehnung an Armbrust et al. (2010) zusammengefasst. Im Anschluss wurden die Interviewpartner gebeten, die zu Beginn des Interviews diskutierten Kriterien anhand ihrer Wichtigkeit zu ordnen, jedoch mit Bezug zum gewählten Beschaffungsobjekt. Somit war es möglich, Unterschiede in der Wichtigkeit der Kriterien zwischen den beiden Servicetypen und ihren Anwendungsbereichen zu identifizieren.

10.3.3 Ergebnisbeschreibung – beispielhaftes Suchprofil

Auf Basis der Interviews konnten einige Unterschiede im Informationsbedarf zwischen den Beschaffungsobjekten SaaS und IaaS/PaaS identifiziert werden.

Tabelle 6: Qualitätseigenschaften nach Cloud-Service-Typen – Suchprofile

Service-Typ	Qualitätseigenschaft
IaaS, PaaS Beschaffungen	<ul style="list-style-type: none"> – Haftung und Verantwortung im Fall von SLA-Verletzungen – Ort der Servicebereitstellung (z.B. der Ort der Datenverarbeitung) – Ort (Gerichtsstand) – Zertifikate – Auditierbarkeit des Anbieters durch den Kunden – Ergänzende Beratungsdienstleistungen
SaaS Beschaffungen	<ul style="list-style-type: none"> – Initiale Bereitstellungszeit – Zugesicherte Kommunikationskanäle für Kundenanfragen – Internationalität in Supportangelegenheiten – Anzahl von Unternehmenskunden, die den Service bereits nutzen – Feedback von Nutzern bzgl. Service – Nutzung und Unterstützung offener Standards – Training – Ort (Rechenzentrum, Büros des Anbieters)

Tabelle 6 fasst die Ergebnisse der Interviews zusammen und verdeutlicht somit die Unterschiede im Informationsbedarf zwischen Software-Services (ERP/CRM-Lösungen) und Infrastrukturdienstleistungen (kollaborative Speicherlösung).

In den im Rahmen des Projektes Value4Cloud entwickelten Software-prototypen hat das Suchprofil ebenfalls Eingang gefunden, wie der Screenshot in [Abbildung 1](#) verdeutlicht. Die in [Tabelle 6](#) genannten Kriterien können auf diese Weise effizient vorausgewählt werden, um die Liste der Qualitätskriterien unternehmensindividuell weiter zu verfeinern.

Neben diesen Unterschieden im Informationsbedarf sind weitere Unterschiede zu vermuten, etwa in Abhängigkeit vom Schutzbedarf der durch den zu beschaffenden Service verarbeiteten Daten und entsprechend zu berücksichtigende, gesetzliche Rahmenbedingungen oder der Kaufanlass. [Abbildung 2](#) visualisiert die im Projekt Value4Cloud identifizierten Aspekte und ihre Ausprägungen.

Abbildung 1: Screenshot – Vorauswahl von Kriterien durch Profile

Werte und Normen am Markt	Beschaffungsgut ist etabliert		Beschaffungsgut ist innovativ und neu	
Gesetzliche Rahmenbedingungen	Beschaffung tangiert Daten mit Personenbezug	Beschaffung tangiert Daten mit gesetzlich festgelegter Aufbewahrungsfrist	Beschaffung tangiert keine Daten mit Personenbezug oder Aufbewahrungsfristen	
Unternehmenssituation des Beschaffers	Start-Up / Gründungsphase	Stabilität	Down-Sizing, Turnaround	
Kaufanlass und Innovationsgrad	Innovative, neue Lösung für experimentellen Einsatz	Innovative, neue Lösung für tagtäglich-lichen Einsatz	Lösung zur Unterstützung des Unternehmenswachstums, Ergänzungsbeschaffung	Lösung zur Effizienzsteigerung, Ersatz einer bestehenden Lösung
Typ des (initialen) Beschaffungsobjekts	Unternehmensweite IT-Infrastruktur	Anwendung, die von einer Abteilung genutzt werden soll	Anwendung, die von mehreren Abteilungen genutzt werden soll	

Abbildung 2: Ergänzende Suchprofile auf Basis identifizierter Einflussfaktoren (aufbauend auf den identifizierten Einflussfaktoren in Wollersheim/ Krcmar 2013)

10.4 Entwicklung von Qualitätskriterien-Sets für die Nutzungsphase von Cloud-Services

Aufbauend auf der bereits im wissenschaftlichen Kontext von Wollersheim/Krcmar (im Erscheinen) erfolgten Veröffentlichung zum Thema dieses Abschnitts werden nachfolgend die wesentlichen Aspekte kurz zusammengefasst.

10.4.1 Bestehende Herausforderungen

Die Prüfung und Überwachung der Servicequalität von Cloud-Services wird aufgrund des „self-service“-Prinzips (siehe auch Kapitel 2 dieses Buches) von dem Unternehmen durchgeführt, das den Service beschafft und nutzt. Die dabei aus Sicht des Unternehmens als wichtig und entscheidend wahrgenommenen Qualitätskriterien können eine Vielzahl von Aspekten umfassen (Kapitel 9 dieses Buches). Des Weiteren variiert die Wichtigkeit einzelner Qualitätskriterien im Beschaffungsprozess in Abhängigkeit vom Typ des zu beschaffenden Service (vorhergehender Abschnitt 10.3). Neben solchen Sets von Qualitätskriterien, die während des Beschaffungsprozesses zur Qualitätsanalyse und Bewertung genutzt werden, also vor der tatsächlichen Servicenutzung eines Services, werden auch Sets von Qualitätskriterien benötigt, um die Qualität während der tatsächlichen Service-Nutzung kontinuierlich zu überwachen.

Es stellt sich somit die Herausforderung, entlang des Lebenszyklus eines Cloud-Services im nutzenden Unternehmen, von der Beschaffung über die Nutzungsphase bis zur Nutzungseinstellung, die relevanten Qualitätsaspekte zu identifizieren und entsprechend zu überwachen. Die nachfolgenden Abschnitte fokussieren, im Gegensatz zum voranstehenden Abschnitt dieses Kapitels, den Zeitraum der Servicenutzung und somit Qualitätskriterien zur kontinuierlichen Leistungsüberwachung.

10.4.2 Vorgehen zur Identifikation des Kriteriensets

Auf Basis einer Literaturanalyse konnten Kriteriensets ermittelt werden, die in ihrer Zusammenstellung einen Fokus auf Qualitätskriterien legen, die bei der Beschaffung von Cloud-Services eine hohe Relevanz besitzen. Ebenso konnten jedoch auch Kriteriensets identifiziert werden, die einen Fokus auf solche Inhalte legen, die bei der kontinuierlichen Qualitätsüberwachung während des Leistungsbezugs relevant werden. Nur wenige Kriterienkataloge umfassen beide Aspekte und ermöglichen eine durchgängige Qualitätsbetrachtung, vom Beschaffungsvorgang bis zur kontinuierlichen Nutzung eines Services. Dies sind die ISO/IEC Norm 25010 (ISO/IEC 25010 2011), der von Siegel/Perdue veröffentlichte Service Measurement Index (SMI 2011; Siegel/Perdue 2012) sowie einzelne stark Praktiker-orientierte Veröffentlichungen. Von den identifizierten Veröffentlichungen unterstützt leider lediglich der Service Measurement Index die Strukturierung und Durchführung der Qualitätsbewertung. Die zugrunde liegenden Schritte sind entsprechend eine wichtige Basis für etwaige Workflows im Bereich Qualitätsbewertung. In Bezug auf die Strukturierung der Kriterien ist jedoch die ISO/IEC-Norm weiter vorangeschritten. Alle enthaltenen Qualitätskriterien sind bereits den Lebenszyklusphasen zugeordnet und somit ein Set von Kriterien für die Beschaffung und ein weiteres Set für die kontinuierliche Qualitätsüberwachung definiert. Die in der Norm ISO/IEC 25010 identifizierten Kriterien zur Qualitätsbewertung zum Zeitpunkt der Service-Nutzung werden entsprechend im nachfolgenden Abschnitt kurz erläutert.

10.4.3 Ergebnisbeschreibung – kontinuierliche Qualitätsbewertung

In der Norm ISO/IEC 25010 werden fünf Qualitätseigenschaften näher betrachtet, die zum Zeitpunkt der Service-Nutzung relevant sind. [Tabelle 7](#) zeigt die enthaltenen Kriterien und die – in der im Rahmen des Projekts entwickelten Plattform enthaltenen – Bewertungsmöglichkeiten auf.

Tabelle 7: Qualitätsbewertung / kontinuierliche Service-Nutzung

Qualitätskriterien	Bewertung	Ergänzende Kommentare
Effektivität Exaktheit und Vollständigkeit, mit denen die an den Service gesteckten Ziele erreicht werden konnten.	>Sterne-Bewertung<	>>Freitext<<
Effizienz Aufgewendete Ressourcen in Relation zu der Exaktheit und Vollständigkeit der erreichten Ziele	>Sterne-Bewertung<	>>Freitext<<
Nützlichkeit Grad, zu dem ein Nutzer mit der wahrgenommenen Zielerreichung zufrieden ist; inkl. dem Ergebnis und der sonstigen Konsequenzen der Service-Nutzung	>Sterne-Bewertung<	>>Freitext<<
Vertrauen Grad, zu dem ein Nutzer oder Interessenvertreter Vertrauen in die bezogene Dienstleistung hat, dass sich diese wie beabsichtigt verhält	>Sterne-Bewertung<	>>Freitext<<
Vergnügen Grad, zu dem ein Nutzer an der Nutzung des Services Vergnügen erzielt hat	>Sterne-Bewertung<	>>Freitext<<
Komfort Grad, zu dem ein Nutzer mit dem Komfort zufrieden ist	>Sterne-Bewertung<	>>Freitext<<
Risikominderung – ökonomisch Grad, zu dem die Dienstleistung das ökonomische Risiko mindert (bspw. bzgl. effizientem Betrieb, Reputation, etc.)	>Sterne-Bewertung<	>>Freitext<<
Risikominderung – Arbeitsschutz Grad, zu dem die Dienstleistung das Risiko für die damit arbeitenden Nutzer mindert, bei angedachter Nutzung	>Sterne-Bewertung<	>>Freitext<<
Risikominderung – Umwelt Grad, zu dem die Dienstleistung das Risiko für Eigentum und Umwelt mindert, bei angedachter Nutzung	>Sterne-Bewertung<	>>Freitext<<

Qualitätskriterien	Bewertung	Ergänzende Kommentare
Inhaltlicher Abdeckungsgrad – Vollständigkeit Grad, zu dem die Dienstleistung effizient und effektiv, frei von Risiken und mit Vergnügen in allen beabsichtigten Nutzungsszenarien genutzt werden kann	>Sterne-Bewertung<	>>Freitext<<
Inhaltlicher Abdeckungsgrad – Flexibilität Grad, zu dem die Dienstleistung effizient und effektiv, frei von Risiken und mit Vergnügen in Nutzungsszenarien genutzt werden kann, die nicht zu Beginn spezifiziert wurden	>Sterne-Bewertung<	>>Freitext<<

10.5 Zusammenfassung der Ergebnisse und Ausblick

Gerade für mittelständische Unternehmen ist es eine große Herausforderung, die im Beschaffungsprozess relevanten Qualitätsanforderungen festzulegen und die zugehörigen Qualitätsinformationen bezüglich der am Markt verfügbaren und prinzipiell in Frage kommenden IT-Serviceangebote zu eruieren. Die im Projekt Value4Cloud erzielten Ergebnisse adressieren diese Herausforderung und versuchen sie zu mildern. Die entwickelte Servicebeschreibungssprache eUSDL und das dadurch präziser einsetzbare Vokabular zur Beschreibung von Cloud-Services unterstützen primär Service-Anbieter. Service-Anwender werden jedoch ebenso unterstützt, etwa wenn sie das Vokabular zur Spezifikation ihrer Anforderungen einsetzen. Darüber hinaus werden Anwender von Cloud-Services bei der Bedarfspezifikation durch die im Projekt Value4Cloud entwickelten Sets von Qualitätskriterien für exemplarisch gewählte Cloud-Services unterstützt.

In Summe adressieren die beschriebenen Value4Cloud-Projektergebnisse unterschiedlichste Herausforderungen, denen mittelständische Kunden von Cloud-Services gegenüberstehen. Wie die entwickelten Ergebnisse beispielhaft in der Unternehmenspraxis eingesetzt werden können, um ihre marktunterstützende Wirkung zu entfalten, wird in den Beiträgen in Kapitel 19-25 dieses Buches beschrieben.

10.6 Literaturverzeichnis

- Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; Zaharia, M. (2010):** A view of cloud computing. In: Communications of the ACM, Vol. 53 (2010) No. 4, S. 50-58.
- Barros, A.; Kylau, U.; Oberle, D. (2011):** Unified Service Description Language 3.0 (USDL) – Overview. SAP Research.
- Brickley, D. (2013):** Friend of a Friend (FOAF). <http://www.foaf-project.org/about>, zugegriffen am 28.07.2014.
- Durkee, D. (2010):** Why Cloud Computing Will Never Be Free. In: Communications of the ACM, Vol. 53 (2010) No. 5, S. 62-69.
- Hepp, M. (2013):** GoodRelations – The Web Vocabulary for E-Commerce. http://wiki.goodrelations-vocabulary.org/Main_Page, zugegriffen am 28.07.2014.
- Hoberg, P.; Wollersheim, J.; Krcmar, H. (2012):** Service Descriptions for Cloud Services – The Customer’s Perspective. Präsentiert auf der ConLife Academic Conference 2012, Köln, Deutschland..
- ISO/IEC 25010 (2011):** Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE), 2011.
- Kaisler, S.; Money, W.H. (2011):** Service Migration in a Cloud Architecture. Präsentiert auf der 44th Hawaii International Conference on System Sciences, Waikoloa, USA.
- NIST (2011):** The NIST Definition of Cloud Computing – Recommendations of the National Institute of Standards and Technology – Special Publication 800-145, U.S. Department of Commerce 2011.
- Oberle, D.; Barros, A.; Kylau, U.; Heinzl, S. (2013):** A unified description language for human to automated services. In: Information Systems, Vol. 38 (2013) No. 1, S. 155-181.
- Pedrinaci, C.; Leidig, T. (2013):** Linked USDL. <http://www.linked-usdl.org/node/68>, zugegriffen am 28.07.2014.
- Robertson, S. (2006):** Mastering the requirements process (Vol. 2), Addison Wesley Professional, Upper Saddle River, USA 2006.
- Sarkar, P.; Young, L. (2011):** Sailing the cloud: a case study of perceptions and changing roles in an australian university. Präsentiert auf der 19th European Conference on Information Systems, Helsinki, Finnland.
- Siegel, J.; Perdue, J. (2012):** Cloud Services Measures for Global Use: The Service Measurement Index (SMI). Präsentiert auf der Service Research and Innovation Institute (SRII) Global Conference, San Jose, USA, S. 411-415.
- SMI (2011):** Service Measurement Index 1.0. Moffet Field, USA: Carnegie Mellon University.
- Wollersheim, J.; Hoberg, P.; Krcmar, H. (2013):** How to specify cloud service demand – An approach recognizing planned application. Präsentiert auf der ConLife Academics 2013, Berlin, Deutschland.

- Wollersheim, J.; Krcmar, H. (2013):** Purchasing processes for cloud services – An exploratory study of process influencing factors. Präsentiert auf der 22nd Annual IPSERA Conference, Nantes, Frankreich.
- Wollersheim, J.; Krcmar, H. (2014):** Quality analysis approaches for cloud services – Towards a framework along the customer’s activity cycle. In: Trusted Cloud Computing. Reussner, R.; Rumpe, B.; Krcmar, H. (Hrsg.). Springer, Wiesbaden, Deutschland.
- Wynstra, F.; Axelsson, B.; Van der Valk, W. (2006):** An application-based classification to understand buyer-supplier interaction in business services. In: International Journal of Service Industry Management, Vol. 17 (2006) No. 5, S. 474-496.

11 Entwicklung und Implementierung eines Softwareprototyps zur Informationsunterstützung und Qualitätsbewertung

A. Reidt, H. Krcmar

11.1 Hintergrund des Prototyps

Im Rahmen des Value4Cloud-Projektes wurde ein Prototyp des „Informations- und Qualitätsbewertungsdienstes“ entwickelt. Als Technologiebasis wurde der Prototyp als Webportal entwickelt, um potenziellen Kleingruppen in Workshops (siehe dazu Kapitel 24) den Beschaffungsprozess bei Cloud-Services prototypisch vorzuführen. Weiterhin ermöglicht das Webportal eine detaillierte Auswertung der durch Teilnehmer ausgewählten wichtigsten Cloud-Service-Merkmale.

Der Prototyp ist als Marktplatz aufgebaut und bildet exemplarisch den gegenseitigen Informationsaustausch zwischen Cloud-Service-Providern und Cloud-Service-Nutzern ab. Deswegen wurde der Prototyp so aufgebaut, dass er den kompletten Workflow eines Marktplatzes abbilden kann. Cloud-Service-Providern wird die Möglichkeit geboten, strukturierte Servicebeschreibungen auf dem Portal einzustellen und damit potenziellen Nutzern ihr Serviceportfolio zu präsentieren. Das Portal bietet den Providern Funktionalitäten, um Services anhand eines standardisierten Merkmalskatalogs zu beschreiben und bestehende Beschreibungen zu überarbeiten.

Cloud-Service-Nutzer sollen sich anhand der Servicebeschreibungen einen Überblick über die am Markt verfügbaren Cloud-Services verschaffen und Services vergleichen können. Nutzern von auf dem Portal beschriebenen Services wird die Möglichkeit gegeben, Services anhand bestimmter Qualitätseigenschaften strukturiert zu bewerten. Dabei bieten Kommentarfunktionen und Bewertungsmöglichkeiten Providern und Nutzern die Möglichkeit zum gegenseitigen Informations- und Erfahrungsaustausch.

Darüber hinaus wird eine Userverwaltung angeboten, wobei unter User alle Nutzeraccounts, wie des Admins, Cloud-Service-Nutzer und Cloud-Service-Provider, zu verstehen sind. Diese Verwaltung erlaubt die Registrierung von Usern und deren Verwaltung durch den zuständigen Portalbetreiber. Hierbei ist es notwendig, User eindeutig identifizieren zu können.

11.2 Datenmodell Plattform

In den folgenden Abschnitten wird der Prototyp des Informations- und Qualitätsbewertungsdienstes anhand seines Datenmodells und mit Abbildungen der Oberfläche vorgestellt. Diese Abbildungen dienen dazu, die Funktionalitäten auf plastische Art und Weise darzustellen. In [Abbildung 1](#) wird das Datenmodell visualisiert.

CloudService: Die Tabelle CloudService enthält die Daten der vom Portal verwalteten Cloud-Services. Die Tabelle umfasst eine strukturierte Liste von Merkmalen. Ein Cloud-Service wird anhand verschiedener Merkmale wie der Servicekategorie, dem Namen des Service, dem Preismodell oder den Service Level Agreements (SLA) beschrieben. Der so entstehende Merkmalskatalog dient zur Strukturierung der Servicebeschreibung durch Service-Provider sowie als Richtlinie bei der Bewertung der wahrgenommenen Servicequalität durch Anwender. Die Merkmale sind als Eigenschaften des Cloud-Service zu verstehen. Alle wichtigen Informationen zur Auswahl innerhalb des Beschaffungsprozess sind hier hinterlegt.

Als Primärschlüssel wird der synthetische Schlüssel *serviceId* verwendet. Durch den Fremdschlüssel *providerId* wird auf den jeweiligen Anbieter des Service verwiesen. Dabei kann ein Cloud-Service immer nur einem Service-Provider zugeordnet sein.

Die Qualität eines Cloud-Service kann durch die User des Portals bewertet werden (ServiceRating). Ein Service kann beliebig viele Bewertungen erhalten. Jeder User kann einen Service jedoch lediglich einmal bewerten.

Im Falle einer unsachgemäßen Beschreibung des Service durch den Provider kann dies durch die User gemeldet werden (Reporting). Ein Cloud-Service kann beliebig oft gemeldet werden, jedoch nur jeweils einmal pro Nutzer und Service.

Abbildung 1: Datenmodell Plattform

ServiceRating: Die Tabelle ServiceRating enthält die Daten einer Bewertung eines Cloud-Services. Ein Service Rating wird von einem User anhand verschiedener Attribute wie der Benutzbarkeit, der Verfügbarkeit oder dem Preis vorgenommen. Eine Bewertung ist durch den Fremdschlüssel *userId* genau einem Benutzer zugeordnet. Es gilt die Bedingung, dass ein User zu jedem Cloud-Service nur eine Bewertung abgeben darf. Als Primärschlüssel wird der synthetische Schlüssel *serviceRatingId* verwendet. Durch den Fremdschlüssel *serviceId* ist jede Bewertung mit einem Cloud-Service verbunden.

Ein Service Rating kann durch User kommentiert werden (RatingComment). Auf diese Weise lassen sich besonders hilfreiche Bewertungen kennzeichnen.

Analog zum Cloud-Service können unsachgemäße Service Ratings durch User gemeldet werden (Reporting). Die Meldung eines Service Ratings kann jedoch durch jeden User lediglich einmal vorgenommen werden.

RatingComment: Die Tabelle RatingComment enthält Kommentare zu Bewertungen von Services. Ein Kommentar besteht neben einer Positiv-/Negativ-Bewertung („hilfreich“, „nicht hilfreich“) aus einem schriftlichen Kommentar. Der schriftliche Kommentar ist optional. Ein Kommentar wird eindeutig über den synthetischen Fremdschlüssel *ratingCommentId* identifiziert. Jeder Kommentar bezieht sich entweder auf eine Service-Bewertung oder auf eine Provider-Bewertung. Die Assoziation zwischen Kommentar und Bewertung erfolgt über den Fremdschlüssel *serviceRatingId*.

User: Die Tabelle User enthält Informationen über die genannten User des Portals. Ein User wird eindeutig über den synthetischen Fremdschlüssel *userId* identifiziert. Ein User kann mit einem Service Provider assoziiert sein.

Jedem User ist eine Rolle zugeordnet. Jede Rolle verfügt über unterschiedliche Berechtigungen (siehe *RoleDetails*).

ServiceProvider: Die Tabelle ServiceProvider enthält Informationen über die Service Provider, die sich auf dem Portal registriert haben.

RoleAssignment: In dieser Tabelle erfolgt die Zuordnung, welchem User welche Rolle (*roleId*) zugeordnet wurde. Die drei Basisrollen sind: „Service-

Nutzer“, „Service-Provider“ und „Administrator“. Jedem User wird genau eine Rolle zugeordnet.

RoleDetails: In dieser Tabelle werden die Informationen zu den unterschiedlichen Userrollen gespeichert. In der Rolle „Service-Nutzer“ kann ein User Cloud-Services bewerten, Bewertungen kommentieren sowie Service-Beschreibungen und Bewertungen melden. In der Rolle „Service-Provider“ kann ein User Servicebeschreibungen neu erstellen oder vorhandene Beschreibungen editieren. Zusätzlich können Bewertungen gemeldet und kommentiert werden. In der Rolle „Administrator“ können u. a. User verwaltet, Servicebeschreibungen freigeben und Bewertungen, Kommentare und Servicebeschreibungen gelöscht oder editiert werden.

Reporting: Eine Meldung mitsamt *reportingId* wird hier gespeichert. Eine Meldung ist dabei ein Hinweis an den Administrator, dass eine Service- oder Provider-Bewertung nicht den Richtlinien des Portals entspricht. Ein Reporting ist entweder einer Provider- oder Service-Bewertung, einem Service oder einer Bewertungskommentierung zugeordnet. Pro User und zu bewertender Entität kann maximal ein Reporting erstellt werden.

CloudServiceSearchProfile: Ein Suchprofil wird in dieser Tabelle abgelegt. Es beinhaltet den Namen des Profils und alle möglichen Ausprägungen, nach denen in der Cloud-Service-Suche nach Services gesucht werden kann. Der Primärschlüssel ist die *profileId*.

11.3 Funktionen und Darstellung

In dem folgenden Abschnitt werden die wichtigsten Funktionen der Plattform anhand von Abbildungen dargestellt. Diese Abbildungen untergliedern sich nach der spezifischen Sichtweise der jeweiligen Rollen. Identische Inhalte werden nur einmal pro Rolle ausführlich aufgezeigt.

11.3.1 Administrator

Bei dem Aufrufen der Plattform erscheint zuerst ein Login-Bildschirm zur Anmeldung. Erkennen kann man diesen in [Abbildung 2](#).

Abbildung 2: Login-Bildschirm

Nach dem Anmelden gelangt man mit Adminrechten auf die Startseite, wie in [Abbildung 3](#) dargestellt. Dort wird der Prototyp und dessen Zweck vorgestellt. Zu Demonstrationszwecken können dort alle Rollen imitiert werden.

Das Einloggen als Admin ermöglicht dem Benutzer entweder die Unterseiten „(Admin-)Home“, „Nutzerhome“, „Service Suche“ und die „Provider Suche“ per Tabs (siehe [Abbildung 3](#)) auszuwählen. Diese beinhalten alle Sichten der restlichen Nutzer, damit der Administrator das Aussehen jeder Sicht überprüfen kann. In [Abbildung 4](#) wird der „(Admin-)home“-Bildschirm angezeigt. Man erkennt dort alle eingestellten Services und Bewertungen. Bei der Auswahl eines Services, dessen Seite bei der Unterkategorie des Service-Nutzer genauer beschrieben wird, hat der Admin mehrere Auswahl-buttons, die sich von den anderen Rollen unterscheiden.

Abbildung 3: Startscreen

11.3.2 Service-Nutzer

Wählt man auf der Startseite (siehe [Abbildung 3](#)) den Link zum Service-Nutzer aus, so gelangt man auf dessen Startseite. Dort sind die verfügbaren Services, die sich der Nutzer anschauen kann, ähnlich wie beim „(Admin-) Home“ aufgelistet. Er kann dort die Services auswählen und näher betrachten. Des Weiteren kann er nach Services und Providern suchen. Dazu muss er die entsprechenden Tabs auswählen.

[Start](#)
[Home](#)
[Nutzerhome](#)
[Service Suche](#)
[Provider Suche](#)

Übersicht aller Services

Sie sind eingeloggt als: **Administrator**

« Zurück [+ Neues Rating anlegen](#) [+ Neuen Service anlegen](#)

Cloud Services, die zur Freigabe überprüft werden sollen (0)

ServiceName	Provider	Datum	Aktionen
Keine Einträge gefunden			

Freigegebene Services (7)

ServiceName	Provider	Datum	Aktionen
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon Web Services LLC	18:43 04.11.2013	
Adobe Photoshop Express	Adobe	19:47 04.11.2013	
KINAMU CRM	KINAMU	20:21 04.11.2013	
Scopevisio Buchhaltungssoftware	Scopevisio	20:33 04.11.2013	
ABAS ERP	ABAS Software AG	20:57 04.11.2013	
Scopevisio Finanzbuchhaltung	Scopevisio	10:09 05.11.2013	
Cloud Storage for Salesforce	Apprio	10:20 05.11.2013	

Geänderte Services (0)

ServiceName	Provider	Datum	Aktionen
Keine Einträge gefunden			

Zurückgewiesene Services (0)

ServiceName	Provider	Datum	Aktionen
Keine Einträge gefunden			

Abbildung 4: Admin-Home-Screen

Wählt der Nutzer einen bestimmten Service aus, gelangt er auf dessen genaue Beschreibung, die sich auf den Kriterienkatalog aus Kapitel 9 bezieht. Dargestellt wird ein Ausschnitt in [Abbildung 5](#). Durch die Auswahl der zwei Buttons, am unteren Ende des Bildschirms zu erkennen, hat der Nutzer die Möglichkeit, zu einem Service eine Bewertung abzugeben oder den Service aufgrund von unangemessenen Informationen zu melden.

Abbildung 5: Nutzersicht Cloud-Service

Unter dem Tab „Bewertungen“ kann der Nutzer alle Bewertungen zu einem Service erkennen. Die Bewertungen werden anhand von Kommentierungen („War diese Bewertung hilfreich?“) in mehrere Kategorien unterteilt und die jeweilig beste Bewertung dargestellt.

[Start](#)
[Home](#)
[Service Suche](#)
[Provider Suche](#)

Bewertung für Cloud Service erstellen

Sie sind eingeloggt als: **ServiceNutzer**

[« Zurück](#) [+ Neues Rating anlegen](#)

0 / 0 Nutzer fanden diese Bewertung hilfreich

Allgemein

Kategorie	Bewertung
Service:	Service wählen
Gesamtbewertung:	☆☆☆☆☆
Titel:	
Was ist besonders positiv aufgefallen?	
Was könnte man noch verbessern?	
Fazit:	

Zur Person

Kategorie	Bewertung
Name / Alias	CloudServiceUser
In welchem Bereich arbeiten Sie?	
Wie lange sind Sie dort schon tätig?	
Kurze Beschreibung zu Ihrer Person	

Abbildung 6: Bewertung anlegen

Klickt der Nutzer auf „Service bewerten“, gelangt er auf die in [Abbildung 6](#) dargestellte Seite. Dort kann er gemäß den vorhandenen Bewertungskriterien den jeweiligen Service bewerten.

Bestehende Bewertungen kann der Nutzer ebenso gemäß ihrer Qualität bewerten. Dazu kann er angeben, ob eine Bewertung hilfreich war oder nicht, und einen Kommentar zu dieser verfassen. Weiterhin hat er ebenso die Möglichkeit, eine Bewertung zu melden, falls diese unangemessen ist.

Abbildung 7: Service-Suche

Der Nutzer gelangt nach Auswahl des Tabs (Navigationsleiste am Anfang der Webseite) „Service-Suche“ zu der in [Abbildung 7](#) dargestellten Ansicht. Dort kann er sich für die Suche nach Profilen oder eine Expertensuche entscheiden.

Suchprofile ermöglichen einen leichteren Einstieg in die Suche, so dass Suchkriterien mit bestimmten Merkmalen vorselektiert werden. Die ausgewählten Merkmale des Profils werden in der Suchmaske dargestellt und können erweitert oder auch geändert werden.

Bei der Expertensuche kann der Nutzer alle Merkmale ohne Vorauswahl selbst bestimmen.

In [Abbildung 8](#) erkennt man eine Seite mit ausgewählten Kriterien. Dort sind die jeweiligen Kriterien der Kategorie „Operativ“ dargestellt. Die Kriterien sind mit einem Informationsbutton verknüpft, der bei Bedarf weitere Informationen zu dem Kriterium anzeigt.

Wird die Suche gestartet und werden mindestens zwei Services zu den ausgewählten Kriterien gefunden, können diese auf Unterschiede und Gemeinsamkeiten untersucht werden. Diese Services werden so gegenübergestellt, dass die Kriterien übersichtlich miteinander verglichen werden können ([Abbildung 9](#)).

Ausgewähltes Profil: IaaS/PaaS Beschaffungen

Das ausgewählte Suchprofil kann, sofern gewünscht, weiter spezifiziert werden. Die Auswahl von "Suchen" startet ihre Cloud Service Suche.

ÜbersichtBasisTechnischFunktionalOperativRechtlich

Service-Management

Konfigurationsmöglichkeiten

Möglichkeiten definiert

Notfallmanagement - Reaktionszeit auf Ausfall (in Stunden)

Notfallmanagement - Wiederanlaufzeit nach Serviceausfall (in Stunden)

Backup

Backup bezeichnet das Kopieren von Daten in der Absicht, diese im Falle eines Datenverlustes zurückkopieren zu können.

Inklusive

Nicht inklusive

Recovery

sive

Nicht inklusive

Egal

On-demand Self Service

Ja

SLA-Monitoring

Inklusive

Nicht inklusive

Egal

Suchen

Zurück zur Auswahl

Suche zurücksetzen

Suche speichern

Suche exportieren

Suche exportieren (inkl. Beschreibung)

Abbildung 8: Suchkriterien der Cloud-Service-Suche

Services vergleichen

Adobe Photoshop Express

KINAMU CRM

Vergleichen

	Adobe Photoshop Express	KINAMU CRM
SLA - Service		
SLA Zusicherung:	Ja	Ja
Zugesicherte Verfügbarkeit - Messzeitraum	-	-
Zugesicherte Verfügbarkeit - Service Level (im Mittel pro Jahr)	[Mehr als 99,5%]	[98 - 99,5%]
Zugesicherte Verfügbarkeit - Service Level Details	[Weniger als maximal 1 Stunde Ausfall/Tag]	[SLO individuell verhandelbar]
Zugesicherte Skalierbarkeit	[Keine Anpassungsmöglichkeit]	[Manuelle Anpassung durch Anwender]

Abbildung 9: Nutzer-Service-Suche und Vergleich

Name	Anzahl CloudServices
ABAS Software AG	1
Adobe	1
Amazon Web Services LLC	1
Appinio	1
KINAMU	1
Scopevisio	2

Abbildung 10: Nutzer-Provider-Suche

Die ausgewählten Suchkriterien können vom Nutzer gespeichert werden und bei späterer Verwendung wieder geladen werden. Ebenso ist es möglich, die Kriterien als .xls (Excel-Dateiformat) zu exportieren. Dies ermöglicht im Workshop die Auswertung von angelegten Suchprofilen der Nutzer. Hierdurch kann genauer analysiert werden, welche Kriterien beispielsweise besonders wichtig für Nutzer sind.

Neben der Service-Suche kann der Nutzer ebenso nach Providern suchen. Die dazugehörige Suchmaske ist in [Abbildung 10](#) zu erkennen. Dort wurde eine Suche nach allen Providern durchgeführt (leeres Feld).

Wählt der Nutzer einen Provider aus, werden auf der folgenden Seite Informationen zu diesem Provider und dessen Services angezeigt.

11.3.3 Service-Provider

Neben den beiden vorigen Rollen gibt es die Rolle des Service-Providers. Dieser sieht auf seinem „Home“-Bildschirm, dargestellt in [Abbildung 11](#), Neuigkeiten zu seinen eingestellten Services. Dies beinhaltet u. a., ob diese

Prototyp Informations- und Qualitätsbewertungsdienst

Start Home Service Suche Provider Suche

Cloud Services von Adobe Sie sind eingeloggt als: **Adobe**

« Zurück + Neuen Service anlegen

Cloud Services, die zur Freigabe überprüft werden sollen (1)

Servicename	Datum
Adobe Flash Collaboration Service	09:48 14.06.2013

Freigegebene Services (3)

Servicename	Datum
Adobe Creative Cloud	09:23 07.06.2013
Adobe Photoshop Express	13:15 07.06.2013
Photoshop Premium Cloud	12:23 24.06.2013

Geänderte Services (0)

Servicename	Datum
Keine Einträge gefunden	

Zurückgewiesene Services (1)

Servicename	Datum
Photoshop Test	14:13 18.06.2013

Bewertungen (2)

Titel	Service Name	Bewertung	Zuletzt geändert am
Sehr hilfreicher Service	Adobe Creative Cloud	★★★★☆	14:36 18.06.2013
Viel zu teuer für die Leistung	Adobe Creative Cloud	★★★☆☆	13:27 25.06.2013

Copyright fortiss GmbH

Abbildung 11: Service-Provider-Home

Services vom Administrator freigegeben oder zurückgewiesen wurden. Daneben werden alle Bewertungen zu den Services dargestellt.

Der Provider kann Services erstellen und hat ebenso wie der Nutzer die Möglichkeit, Bewertungen zu melden. Im Gegensatz zum Service-Nutzer jedoch nur bei seinen eigenen Services.

11.4 Zusammenfassung der Ergebnisse und Ausblick

Für die Unterstützung von Workshops im Rahmen des Value4Cloud-Projektes wurde der Prototyp des „Informations- und Qualitätsbewertungsdienstes“ entwickelt. Dieser bildet eine typische Tätigkeit im Beschaffungsprozess für Cloud-Services ab, daher ist der Prototyp als Marktplatz aufgebaut. Dieser Marktplatz bildet exemplarisch den gegenseitigen Informationsaustausch zwischen Cloud-Service-Providern und Cloud-Service-Nutzern ab. Durch den Einsatz des Prototyps wird es ermöglicht, das Nutzerverhalten bzw. Nutzerinteressen bei Merkmalen zu analysieren und den Beschaffungsprozess zu simulieren.

12 Empfehlungen zur Gestaltung von Cloud-Service-Zertifizierungen

S. Schneider, J. Lansing, A. Sunyaev

12.1 Einleitung¹

Zertifizierungen von Cloud-Services können Entscheidungsträger bei der Auswahlentscheidung unterstützen, Transparenz am Markt schaffen, Vertrauen und Akzeptanz auf der Anwenderseite erhöhen sowie es Cloud-Service-Anbietern ermöglichen, ihre Systeme und Prozesse zu überprüfen und zu verbessern (Sunyaev/Schneider 2013; Bundesamt für Sicherheit in der Informationstechnik 2011; Khan/Malluhi 2010). Derzeit existieren eine Reihe von Rahmenwerken, die Cloud-spezifische Herausforderungen adressieren und darauf abzielen, die Auswahl, Einführung sowie den operativen Betrieb von Cloud-Services zu unterstützen (z. B. Bundesamt für Sicherheit in der Informationstechnik 2011; Cloud Security Alliance 2011). Kunden können jedoch kaum verifizieren, ob sich die Cloud-Service-Anbieter an die in den Rahmenwerken definierten Vorgaben halten. Organisationen wie EuroCloud oder die Cloud Security Alliance haben dieses Problem erkannt und Programme zur Zertifizierung von Cloud-Services initiiert. Weitere Rahmenwerke zur Zertifizierung von Cloud-Services sind derzeit in der Entstehung (z. B. ISO 27017). [Tabelle 1](#) bietet einen Überblick über Cloud-spezifische Zertifizierungen. Diese Zertifizierungen befinden sich jedoch noch in der Reifephase.

Unsere Forschung zeigt, dass sowohl Anwender als auch Anbieter durchaus einen Nutzen in der Zertifizierung von Cloud-Services sehen. Dieser Nutzen ist jedoch an bestimmte Rahmenbedingungen geknüpft, die existierende Zertifizierungen nur teilweise erfüllen (vgl. Teil B).

1 Aufbauend auf der bereits im wissenschaftlichen Kontext von Schneider et al. (2013) erfolgten Veröffentlichung zum Thema dieses Kapitels werden nachfolgend die wesentlichen Aspekte kurz zusammengefasst.

Tabelle 1: Überblick über existierende Cloud-Service-Zertifizierungen

Zertifizierung	Organisation	Prozess	Inhalt
CSA STAR	H: Cloud Security Alliance A: -	P: Selbstevaluation G: 1 Jahr	D: Compliance, Daten-Governance, Elastizität, Operations Management, Risikomanagement, Release Management, Recht, Sicherheit (Rechenzentrum, Personal, Information), Sicherheitsarchitektur R: International B: CSA Cloud Controls Matrix (CCM), CSA Consensus Assessments Initiative (CAI)
EuroCloud Star Audit	H: EuroCloud A: EuroCloud	P: Dokumentenreview, Vor-Ort-Audit G: 2 Jahre	D: Anbieterprofil, Vertrag und Compliance, Sicherheit, Betrieb und Infrastruktur, Betriebsprozesse, Anwendung, Implementierung R: National B: BSI Sicherheitsempfehlungen für Cloud Computing Anbieter, ISO IT Prüfstandards (z. B. ISO 27001), CSA Guidance for Critical Areas of Focus in Cloud-Computing, ENISA Cloud-Computing: Benefits, Risks and Recommendations for Information Security
EuroPriSe	H: ULD Schleswig-Holstein A: Zwei akkreditierte Experten (Recht und IT)	P: Dokumentenreview, Vor-Ort Audit G: 2 Jahre	D: Datenschutz R: Europäische Union B: EU Direktive 95/45/EC
FedRAMP	H: General Services Administration A: Akkreditierte Zertifizierungsorganisation	P: Dokumentenreview, Vor-Ort Audit, kontinuierliches Monitoring G: Monatliche Berichtspflichten	D: Sicherheit R: USA B: NIST Special Publications (z. B. 800-37, 800-53, 800-137)

Zertifizierung	Organisation	Prozess	Inhalt
ISO 27017 (in Arbeit)	H: ISO A: Zertifizierte Auditoren	P: Dokumentenreview, Vor-Ort Audit G: Noch nicht entschieden	D: Noch nicht entschieden; angelehnt an ISO 27002 R: International B: ISO 27002
Trust in Cloud	H: Cloud-EcoSystem A: Cloud-EcoSystem	P: Selbstevaluation, Dokumentenreview G: Unbegrenzt	D: Referenzen, Datensicherheit, Qualität der Bereitstellung, Entscheidungssicherheit, Vertragsbedingungen, Service-Orientierung, Cloud-Architektur R: Deutschland B: -
Trusted Cloud	H: TÜV Austria A: TÜV Austria	P: Dokumentenreview, Vor-Ort-Audit G: 3 Jahre	D: Anforderungen an Personal, Monitoring & Security Incident Management, Notfallmanagement, Rechtemanagement, Sicherheit (Netz, Rechenzentrum, Server), Sicherheitsmanagement beim Anbieter, Transparenz R: Deutschland, Österreich B: „Internationale Standards“
TÜV Cloud Security	H: TÜV Rheinland A: TÜV Rheinland	P: Dokumentenreview, Vor-Ort-Audit G: Keine Angabe	D: Infrastruktur: Virtualisierung von Rechenzentren, Systeme, Zugriffskonzepte, Netzwerk, Systemschnittstellen, administrative Prozesse, Service-Prozesse, Compliance; Anwendung: Mandantenfähigkeit der Applikation, Datentrennung, Funktionalität, Applikationsschnittstellen, Entwicklungsprozesse R: Deutschland B: ISO 27001, ISO 27002, BSI IT-Grundschutz, BDSG
TRUSTed Cloud Data Privacy Certification	H: TRUSTe A: TRUSTe	P: System- und Dokumentenreview G: 1 Jahr	D: Datenschutz R: International B: -
A: Auditor, B: Basis (zugrunde liegende Rahmenwerke), D: Zertifizierungsdimensionen, G: Gültigkeitsdauer, H: Herausgeber, P: Prozessart, R: Reichweite			

Um dieser Problematik entgegenzuwirken, wurde die Forschung und Entwicklung von Cloud-Service-Zertifizierungen (CSZ) zu einem zentralen Element der EU-Cloud-Strategie erklärt (European Commission 2012).

Dieser Beitrag bietet einen Überblick zur Zertifizierungslandschaft im Bereich Cloud-Computing und zeigt Empfehlungen zur Gestaltung effektiver CSZ auf. Die Grundlage dieses Beitrags bilden 20 semi-strukturierte Experteninterviews im Zeitraum Juni bis Oktober 2012 mit Führungskräften und Managern von Anwendern, Anbietern und Beratern aus dem Cloud-Computing-Umfeld. In den Interviews wurden Interviewpartner nach ihrer Wahrnehmung von und den Anforderungen für CSZ befragt. Aus den Interviews wurden zehn Zertifizierungsdimensionen abgeleitet, deren relative Wichtigkeiten mittels eines Discrete-Choice-Experiments gemäß der Best-Worst-Scaling-Methodik (BWS) evaluiert wurden (Finn/Louviere 1992). Die Umfrage wurde im März und April 2013 unter 110 Führungskräften und Managern von Anwendern, Anbietern und Beratern aus dem Cloud-Umfeld durchgeführt. Für weitere Details zur Anwendung der BWS-Methode, Experimentdesign und -durchführung sowie detaillierter Auswertungen im Konsumentenkontext vergleiche Lansing et al. (2013).

12.2 Wahrnehmung von Cloud-Service-Zertifizierungen

Die Interviewpartner haben eine überwiegend positive Einstellung gegenüber der CSZ, wonach der Nutzen weit über die reine Entscheidungsunterstützung hinausgeht. Anbieter heben drei wesentliche Vorteile hervor. Erstens helfen Zertifizierungen bei der Strukturierung und Verbesserung der eigenen internen Prozesse. Zweitens bieten sie die Möglichkeit nachzuweisen, dass ein Anbieter fähig ist, hochqualitative Cloud-Services bereitzustellen und darüber das Vertrauen potenzieller Kunden zu erlangen. Drittens können Zertifikate als Marketinginstrumente eingesetzt werden und den Eintritt in ansonsten schwer zugängliche Märkte erleichtern (z.B. öffentlicher Sektor). Um diese Vorteile zu erzielen, sind Anbieter bereit, in eine entsprechende Zertifizierung zu investieren. Voraussetzung dafür ist allerdings, dass ein weit verbreitetes, anerkanntes und von Anwendern nachgefragtes Zertifikat existiert. Dieser Bedarf besteht aber auf Anwenderseite bisher nur nachgelagert. Explizit werden CSZ nur sehr selten angefordert.

Die positive Einstellung gegenüber einer CSZ bei Anwendern manifestiert sich insbesondere in wahrgenommenen Vorteilen wie Vertrauensgewinn in den Anbieter, Förderung von Mindestqualitätsstandards sowie Unterstützung bei der Auswahlentscheidung. Zertifizierungen werden jedoch nicht als Allheilmittel gesehen, die eine detaillierte Auseinandersetzung mit den auszuwählenden Cloud-Services erübrigen. Anwender haben konkrete Anforderungen an Cloud-Services und stellen eigene Anforderungskataloge zusammen, die mit dem Kriterienkatalog einer Zertifizierung – sofern er denn offengelegt ist – abgeglichen werden müssen. Anwender bemängeln, dass insbesondere branchenspezifische Anforderungen bisher nicht abgedeckt werden und häufig nicht auf Anhieb klar ist, was in welcher Detailtiefe überprüft wurde. Zudem garantieren Zertifikate nicht unbedingt die Einhaltung der Zertifizierungskriterien, sondern nur, dass sie zum Zeitpunkt der Ausstellung des Zertifikats einem gewissen Mindestqualitätsstandard entsprochen haben.

Die aktuell existierenden CSZ ([Tabelle 1](#)) waren den befragten Experten größtenteils unbekannt. Bei Auswahlentscheidungen wurde eher auf eine ISO 27001 Zertifizierung geachtet, die zwar nicht Cloud-spezifisch ist, jedoch im IT-Service-Sektor weite Verbreitung und Anerkennung findet. Sowohl Anbieter als auch Anwender schätzen die derzeitige Relevanz von CSZ für Entscheidungsprozesse als eher gering ein. Bemerkenswerterweise bewerten auch bereits zertifizierte Anbieter ihre Zertifizierung als nachgelageretes Auswahlkriterium. Die befragten Experten betonen jedoch, dass diese Einschätzungen nicht auf einen generellen Mangel an Relevanz von CSZ hindeuten, sondern vielmehr auf den Entwicklungsstand des Zertifizierungsmarktes für Cloud-Services zurückzuführen sind. Den Experten zufolge fehlt es an etablierten und bekannten CSZ, was bedeutet, dass die derzeit existierenden Zertifizierungen die Anforderungen des Marktes noch nicht umfassend abdecken.

12.3 Gestaltungsempfehlungen für Cloud-Service-Zertifizierungen

Im Rahmen der Studien wurden Anforderungen erhoben, die eine CSZ erfüllen muss, um Akzeptanz am Markt und damit eine Steigerung des Vertrauens von Kunden in die zertifizierten Cloud-Services zu erreichen. Aus diesen

Anforderungen lassen sich Gestaltungsempfehlungen ableiten, die in [Tabelle 2](#) zusammengefasst sind.

Tabelle 2: Gestaltungsempfehlungen für Cloud-Service Zertifizierungen

Charakteristik		Bevorzugte Ausprägung
Organisation	Herausgeber	Standardisierungsgremium oder Branchenverband Unabhängige Organisation mit langjähriger Erfahrung und hoher Reputation, der potenzielle Anwender hohes Vertrauen zuschreiben
	Auditor	Akkreditierte Organisation oder Branchenverband Auditor losgelöst vom Beratungsauftrag zur Vorbereitung auf die Zertifizierung
Prozess	Auditierungsprozess	Vor-Ort-Audit, Dokumentenreview und Interviews Aufwand für Audit und Umfang der Zertifizierung transparent und sofort ersichtlich dargelegt
	Gültigkeit und Re-Auditierung	Maximal zwei Jahre (Teil-)automatisiertes Monitoring zur kontinuierlichen Überwachung der zertifizierten Services
Inhalt	Dimensionen	Fokus auf nicht-funktionale Eigenschaften: siehe Tabelle 3
	Objekt	Cloud-Service
	Umfang	Optionale branchenspezifische Bausteine Kriterienkatalog abgestimmt auf unterschiedliche Informationsbedürfnisse verschiedener Stakeholder
	Reichweite	International abgestimmtes Rahmenwerk mit rechtlichen Bausteinen auf nationaler bzw. Rechtsraumbene
	Basis (zugrunde liegendes Rahmenwerk)	Standard: öffentlich zugänglicher und detaillierter Kriterienkatalog Einsetzbar als Katalog zur Zertifizierung von Cloud-Services, Selbstbewertung und Leitfaden zur Entscheidungsunterstützung Publiziert in einer maschinenlesbaren Servicebeschreibungssprache

Die Zertifizierung sollte von einer unabhängigen Organisation gestaltet und herausgegeben werden, nicht aber von privaten Organisationen oder öffentlichen Einrichtungen. Der eigentliche Audit-Prozess sollte von akkreditierten Organisationen durchgeführt werden, zum Beispiel Branchenverbänden oder privatwirtschaftlichen Unternehmen. Branchenverbände als Herausgeber von Zertifizierungen wurden mit gemischten Meinungen bewertet, da eigene (u. a. auch monetäre) Ziele die Unabhängigkeit einer Zertifizierung beeinflussen können. Andererseits entsteht aufgrund der hohen Dynamik im Cloud-Computing-Markt das Problem, dass angesichts der langen Zeitspanne, bis international anerkannte Normen veröffentlicht werden (z.B. ISO), ein Branchenverband als Herausgeber (z.B. EuroCloud) als einzige, kurzfristig gangbare Lösung wahrgenommen wird. Falls der Audit von privatwirtschaftlichen Organisationen durchgeführt wird, ist es von entscheidender Bedeutung, Mechanismen zur Verhinderung von Gefälligkeitsaudits zu etablieren. So wurde insbesondere die Konstellation als kritisch bewertet, in der die auditierende Organisation ebenfalls den Beratungsauftrag zur Vorbereitung auf die Zertifizierung übernimmt. Um diese Konstellation zu vermeiden, ist eine Trennung von ausstellenden, auditierenden und beratenden Organisationen zur Vorbereitung auf den Audit unabdingbar.

Der Zertifizierungsprozess muss eine Vor-Ort-Prüfung beinhalten und sollte neben Re-Audits (mindestens alle zwei Jahre) auch auf (teil-)automatisierte Mechanismen zur kontinuierlichen Überwachung und Erneuerung der Zertifizierung zurückgreifen. Mit automatisierten Überwachungsmechanismen kann ein konstantes Niveau an Servicequalität nachgewiesen werden, das mit regelmäßigen Vor-Ort-Audits nicht auf wirtschaftliche Art und Weise erreicht werden kann.

Als Schwachstelle aktueller Zertifizierungen wurde die häufig bestehende Unklarheit über Zertifizierungsinhalte und -umfang genannt. Um dies zu beheben, muss das zugrunde liegende Rahmenwerk mit Zertifizierungskriterien detailliert und öffentlich zugänglich sein und nicht nur auf abstrakter Ebene beschrieben sein. Hier besteht die Problematik, dass Zertifizierungsorganisationen ihre Rahmenwerke in der Regel als proprietäres Eigentum auslegen und diese daher aus wirtschaftlichen Gründen nicht offenlegen. Zudem muss der durch den Auditor in eine Vor-Ort-Zertifizierung investierte Aufwand

transparent kommuniziert und an prominenter Stelle im Zertifizierungsbericht ersichtlich sein, ebenso wie der Umfang der zertifizierten Komponenten des Services.

Eine CSZ sollte auf einen einzelnen Service bezogen sein und nicht auf den gesamten Anbieter. Die Zertifizierung sollte sich nur auf nicht-funktionale Eigenschaften eines Services konzentrieren. Die wichtigsten Zertifizierungsdimensionen sind in [Tabelle 3](#) zusammengefasst. Zusätzliche branchenspezifische Anforderungen sollten im zugrunde liegenden Rahmenwerk enthalten sein und vom Anbieter nach Bedarf zertifiziert werden können. Um die unterschiedlichen Informationsbedürfnisse der Kunden zu erfüllen, sollte eine Zertifizierung daher mehrere Dimensionen abdecken (siehe [Tabelle 3](#)).

Die Interviewergebnisse lassen den Schluss zu, dass die identifizierten Dimensionen unterschiedliche Prioritäten bei verschiedenen Interessengruppen aufweisen. Während zum Beispiel Sicherheit und Verfügbarkeit primäre Anliegen des Managements sind, betreffen Kundensupport und Prozesse beim Anbieter eher die Mitarbeiter des Anwenderunternehmens, die nach Einführung eines Cloud-Services mit dem Anbieter interagieren.

Die Ergebnisse der nachgelagerten Umfrage deuten darauf hin, dass sich die relativen Wichtigkeiten einzelner Zertifizierungsdimensionen je nach Zielgruppe unterscheiden. Daher sollte der Kriterienkatalog sowie der darauf basierende Bericht auf die Informationsbedürfnisse der unterschiedlichen Stakeholder abgestimmt sein, zum Beispiel je nach Rolle und Position der Entscheidungsträger im Unternehmen. Idealerweise liegt der Bericht digital, interaktiv und filterbar vor, optimal sogar maschinenlesbar. Eine international gültige Zertifizierung wird als Idealzustand angesehen. Jedoch erscheint die Umsetzung einer solchen Zertifizierung aufgrund der unterschiedlichen rechtlichen Gegebenheiten und Rechtsprechungen äußerst herausfordernd. Zertifizierungen sollten daher auf einem international vereinbarten Rahmenwerk aufbauen, rechtliche Compliance muss jedoch auf nationaler bzw. Rechtsraumbene beurteilt und zertifiziert werden. Anwender sehen in einer solchen Zertifizierung bereits einen Mehrwert, wenn sie für einzelne Länder klarstellt, inwieweit der zertifizierte Cloud-Service mit den jeweiligen gesetzlichen Vorschriften konform ist.

Tabelle 3: Rangfolge und Definitionen der Zertifizierungsdimensionen

Rang	Definition
1	Datenschutz: Zertifizierung, dass (i) der Anbieter sich an geltendes Datenschutzrecht hält, (ii) durch den Anbieter keine inhaltliche Auswertung der im Cloud-Service gespeicherten Nutzdaten des Kunden erfolgt, (iii) sämtliche Kundendaten nach Beendigung des Vertragsverhältnisses vollständig und nicht wiederherstellbar gelöscht werden, (iv) Kundendaten durch den Anbieter nicht an dritte Organisationen verkauft, verliehen oder weitergegeben werden.
2	IT-Sicherheit: Zertifizierung, dass der Anbieter Maßnahmen etabliert hat, die sicherstellen, dass Daten sicher gespeichert und übertragen werden sowie vor unberechtigtem Zugriff durch Dritte und andere Cloud-Service-Nutzer geschützt sind.
3	Verfügbarkeit: Zertifizierung, dass der Cloud-Service die versprochenen Performancezusagen einhält sowie die Verfügbarkeit der Daten sicherstellt und Maßnahmen zur Verhinderung eines Datenverlustes betreibt.
4	Rechtliche Compliance: Zertifizierung, dass der Anbieter rechtliche und regulatorische Vorgaben an Cloud-Services einhält.
5	Vertragsbedingungen: Zertifizierung, dass verständliche Vertragsvereinbarungen existieren, die der gängigen Geschäftspraxis entsprechen, sowie dass die Vertragsbedingungen die Eigentumsrechte des Kunden an den im Cloud-Service gespeicherten Kundendaten nicht einschränken.
6	Interoperabilität: Zertifizierung, dass die Kundendaten in standardisierten Formaten gespeichert und exportiert werden können, dass der Cloud-Service über eine offene Schnittstelle zur Integration mit anderen Cloud-Services oder sonstigen Anwendungen verfügt, sowie dass über diverse Endgeräte ortsunabhängig auf den Cloud-Service zugegriffen werden kann.
7	Kundensupport: Zertifizierung, dass der Anbieter Erreichbarkeiten und Reaktionszeiten des Kundensupports zusichert und einhalten kann sowie eine proaktive Informationspolitik gegenüber den Kunden betreibt.
8	Finanzielle Stabilität: Zertifizierung, dass die mittelfristige finanzielle Tragfähigkeit des Anbieters sichergestellt ist.
9	Flexibilität: Zertifizierung, dass die bezogene Leistung durch den Kunden selbstständig angepasst werden kann und die Anpassung automatisiert, in kürzester Zeit und bei transparenten Kosten durchgeführt wird.
10	Prozessreife: Zertifizierung, dass der Reifegrad der Geschäftsprozesse des Anbieters etablierten Best Practices im IT-Service-Bereich entspricht.

12.4 Fazit

Sowohl Anbieter als auch Anwender schätzen die Wirkung von CSZ für den Entscheidungsprozess derzeit als eher gering ein. Dies lässt sich auf einen Mangel an etablierten und bekannten CSZ sowie die eingeschränkte Abdeckung der Marktanforderungen durch existierende Zertifizierungen zurückführen. Der Vergleich existierender Zertifizierungen ([Tabelle 1](#)) mit den im Rahmen der Studien abgeleiteten Anforderungen an CSZ ([Tabelle 2](#) und [3](#)) zeigt, dass existierende Zertifizierungen die Anforderungen nur teilweise abdecken.

Insbesondere besteht Forschungsbedarf bei der Entwicklung von (teil-) automatisierten Mechanismen zur kontinuierlichen Überwachung und Erneuerung der Zertifizierung sowie der strukturierten und maschinenlesbaren Beschreibung von Zertifizierungskriterien und Auditreports. FedRAMP² bietet bereits erste Ansätze zur kontinuierlichen Überwachung, auf denen weitere Forschungs- und Entwicklungsarbeit aufbauen kann. Plattformneutrale Servicebeschreibungssprachen wie die Unified Service Description Language (USDL) bieten einen vielversprechenden Ansatz, modulare, maschinenlesbare Zertifizierungen zu implementieren. USDL zielt darauf ab, Maschinen dabei zu unterstützen, Services automatisiert über das Internet auszutauschen (Oberle et al. 2013), und bietet sich sowohl zur Beschreibung der Zertifizierungskriterien als auch des Auditreports an. Ein solches Vorgehen würde es Anwendern ermöglichen, ihre Mindestanforderungen an Cloud-Services in einem USDL-Anforderungsprofil zu beschreiben und anhand des Anforderungsprofils entsprechende Cloud-Services automatisiert zu finden.

2 Das Federal Risk and Authorization Management Program (FedRAMP) ist eine staatliche Zertifizierung in den USA, die von Cloud-Anbietern erreicht werden muss, um Behörden und öffentlichen Einrichtungen Cloud-Services anbieten zu können. Es beschreibt einen standardisierten Ansatz zur Sicherheitsbewertung, Autorisierung und zum kontinuierlichen Monitoring von Cloud-Services.

12.5 Literaturverzeichnis

- Bundesamt für Sicherheit in der Informationstechnik (2011):** Sicherheitsempfehlungen für Cloud Computing Anbieter (Mindestsicherheitsanforderungen in der Informationssicherheit). http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile, zugegriffen am 28.07.2014.
- Cloud Security Alliance (2011):** Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>, zugegriffen am 28.07.2014.
- European Commission (2012):** Unleashing the Potential of Cloud Computing in Europe. http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf, zugegriffen am 02.10.2012.
- Finn, A.; Louviere, J.J. (1992):** Determining the Appropriate Response to Evidence of Public Concern: The Case of Food Safety. In: Journal of Public Policy & Marketing, Vol. 11 (1992) No. 2, S. 12–25.
- Khan, K.M.; Malluhi, Q. (2010):** Establishing Trust in Cloud Computing. In: IT Professional, Vol. 12 (2010) No. 5, S. 20–27.
- Lansing, J.; Schneider, S.; Sunyaev, A. (2013):** Cloud Service Certifications: Measuring Consumers' Preferences for Assurances. Präsentiert auf der 21st European Conference on Information Systems, Utrecht, Niederlande.
- Oberle, D.; Barros, A.; Kylau, U.; Heinzl, S. (2013):** A unified description language for human to automated services. In: Information Systems, Vol. 38 (2013) No. 1, S. 155–181.
- Schneider, S.; Lansing, J.; Sunyaev, A. (2013):** Empfehlungen zur Gestaltung von Cloud-Service-Zertifizierungen. In: Industrie Management, Vol. 4 (2013), S. 13–17.
- Sunyaev, A.; Schneider, S. (2013):** Cloud Services Certification. In: Communications of the ACM, Vol. 56 (2013) No. 2, S. 33–36.

13 Vertrauensunterstützende Mehrwertdienste – Ein systematisches Vorgehen zur Förderung von Vertrauen im Cloud-Computing-Umfeld

L. Gebauer, M. Söllner, J.M. Leimeister

13.1 Prozess zur systematischen Vertrauensunterstützung

In diesem Kapitel wird ein Prozess zur Entwicklung vertrauensunterstützender Mehrwertdienste erarbeitet, um mit den daraus abgeleiteten Lösungen den Vertrauensproblematiken im Cloud-Computing-Umfeld (siehe Kapitel 6) zu begegnen. Dazu wurde die Methode zur Entwicklung vertrauensunterstützender Komponenten für sozio-technische ubiquitäre Systeme nach Söllner et al. (2012a) auf den Cloud-Computing-Kontext übertragen und weiterentwickelt.

Der Prozess zur systematischen Vertrauensunterstützung umfasst fünf aufeinander folgende Schritte ([Abbildung 1](#)) und soll Cloud-Computing-Anbieter befähigen ihre Cloud-Computing-Dienste vertrauenswürdiger zu gestalten. Jeder einzelne Schritt wird durch eine Leitfrage angeleitet, um so die Erarbeitung der einzelnen Entwicklungsaktivitäten zu unterstützen. Der Prozess zielt darauf ab, Lösungen in Form von vertrauensunterstützenden Mehrwertdiensten für den ausgewählten Cloud-Computing-Dienst abzuleiten. In den nachfolgenden Abschnitten wird der Prozess zur systematischen Vertrauensunterstützung erklärt und allgemein für Cloud-Computing durchlaufen, jedoch ohne Bezugnahme auf einen konkreten Dienst. Die exemplarischen Ergebnisse können von den Cloud-Computing-Anbietern als Grundlage verwendet werden, um eigene, individuelle Lösungen zu entwickeln. Dennoch empfiehlt es sich, eine kritische Überprüfung hinsichtlich der Übertragbarkeit auf den ausgewählten Cloud-Computing-Dienst durchzuführen. Es kann nicht ausgeschlossen werden, dass bestimmte Aspekte für den ausgewählten Cloud-Computing-Dienst keine Relevanz haben oder wiederum wichtige Aspekte noch nicht berücksichtigt wurden.

Abbildung 1: Prozess zur systematischen Vertrauensunterstützung für Cloud-basierte Dienstleistungen (In Anlehnung an Söllner et al. 2012a).

Im ersten Schritt des Prozesses zur systematischen Vertrauensunterstützung werden die Unsicherheiten bzw. die Nutzungshemmnisse der (potenziellen) Cloud-Computing-Nutzer identifiziert und analysiert. Im zweiten und dritten Schritt werden die relevanten Vertrauensdimensionen und -determinanten bestimmt, mit denen den identifizierten Unsicherheiten und Hemmnissen entgegengewirkt werden kann. Im vierten und fünften Schritt werden aufbauend auf den Ergebnissen vertrauensbezogene Anforderungen sowie vertrauensunterstützende Lösungen bzw. Mehrwertdienste erarbeitet.

13.2 Schritt 1: Identifikation relevanter Unsicherheiten

Im ersten Schritt erfolgt die Entwicklungsaktivität *„Identifikation relevanter Unsicherheiten“*. Im Zuge derer wird folgende Leitfrage beantwortet: *„Mit welchen Unsicherheiten wird der Nutzer konfrontiert und welche haben vor dem Hintergrund des Verwendungszwecks die höchste Priorität?“*. Zur exemplarischen Beantwortung dieser Frage werden die folgenden Kategorien von Nutzungshemmnissen genannt (siehe Kapitel 6), wobei deren Gültigkeit in Bezug auf den zu untersuchenden Cloud-Computing-Dienst überprüft und deren Relevanz im Hinblick auf den Verwendungszweck priorisiert werden sollte:

- Diskontinuität/ Ausfall des Dienstes
- Systemangriffe
- Netzwerkstörungen
- begrenzte Skalierbarkeit
- Zeit- und kostenintensive Datenübertragung
- mangelnde Datenintegrität
- Abhängigkeit vom Anbieter
- Abhängigkeit von anderen Nutzern
- mangelnde Kontrollmöglichkeiten
- mangelnde Reliabilität

- mangelnde rechtliche Standards
- Gefährdung interner IT

Workshops mit einem Anbieterunternehmen von Cloud-Computing-Diensten zeigen, dass es empfehlenswert ist, die (potenziellen) Kunden direkt nach deren Unsicherheiten und Bedenken gegenüber der Nutzung des Cloud-Computing-Dienstes zu befragen. In den Workshops ergaben sich beispielhaft die folgenden Unsicherheiten, Bedenken oder Fragen:

- Sicherstellung der Verfügbarkeit fraglich, z.B. aufgrund mangelnder Internetanbindung in verschiedenen Regionen
- Gewährleistung einer sicheren Verbindung zwischen internen und externen Mitarbeitern
- Bereitstellung einer maßgeschneiderten Kundenlösung fraglich
- Was ist günstiger: Service mieten oder eigenes Rechenzentrum betreiben?
- Schnittstellenprobleme durch unterschiedliche Software/ Betriebssysteme
- Sensible/ personenbezogene Daten: Was darf in die Cloud und was nicht?
- Unübersichtlichkeit am Markt: Wie finde ich bei den vielen Anbietern den richtigen Anbieter?
- Unübersichtlichkeit der Leistungsangebote: Wie finde ich den Cloud-Dienst, der zu mir passt?

Abschließend sollten die identifizierten Unsicherheiten in eine Rangfolge gebracht werden, um herauszustellen, welche Unsicherheiten vor dem Hintergrund des Verwendungszwecks des Cloud-Computing-Dienstes bei den (potenziellen) Kunden am stärksten ausgeprägt sind.

13.3 Schritt 2: Identifikation relevanter Vertrauensdimensionen

Im zweiten Schritt wird der Leitfrage nachgegangen: „Mit Hilfe welcher Vertrauensdimensionen kann den Unsicherheiten entgegengewirkt werden?“, um die Entwicklungsaktivität „Identifikation relevanter Vertrauensdimensionen“ zu adressieren. Bei der Beantwortung der Leitfrage wird zwischen dem *interpersonellen Vertrauen*, also dem Vertrauen in den Anbieter von Cloud-Computing-Diensten, und dem *Systemvertrauen*, also dem Vertrauen in die Cloud-Computing-Technik an sich, unterschieden. Forschungsarbeiten zeigen, dass sich diese beiden Komponenten von Vertrauen aus mehreren Dimensionen ergeben, die wiederum von unterschiedlichen Determinanten beeinflusst werden ([Abbildung 2](#)).

Vertrauen in den Anbieter setzt sich gemäß der Forschung (Söllner et al. 2013; Mayer et al. 1995) aus drei Dimensionen zusammen (vgl. [Abbildung 2](#)):

- Fähigkeit (im englischen Original: *Ability*),
- Wohlwollen (im englischen Original: *Benevolence*) und
- Integrität (im englischen Original: *Integrity*).

Die Dimension *Fähigkeit* beschreibt die Einschätzung des Vertrauensgebers, also des (potenziellen) Cloud-Computing-Nutzers, inwieweit dieser den Vertrauensnehmer, also den Cloud-Computing-Anbieter, für fähig erachtet, bei der Zielerreichung behilflich zu sein (Söllner et al. 2012a). Die Dimension *Wohlwollen* ist die Einschätzung des (potenziellen) Cloud-Computing-Nutzers, inwieweit der Cloud-Computing-Anbieter bereit ist, die Interessen des Nutzers zu berücksichtigen und zu wahren (Söllner et al. 2012a). *Integrität* ist die Einschätzung des (potenziellen) Cloud-Computing-Nutzers, inwieweit sich der Cloud-Computing-Anbieter an gewissen Prinzipien und Normen orientiert, die der Nutzer für gut erachtet (Söllner et al. 2012a).

Abbildung 2: Überblick Vertrauen im Cloud-Computing-Umfeld
(Quelle: Eigene Darstellung).

Das Systemvertrauen ergibt sich gemäß verschiedener Forschungsarbeiten (z. B. Söllner et al. 2012b; Lee/See 2004) aus der Einschätzung folgender Dimensionen (vgl. [Abbildung 2](#)):

- Performance (im englischen Original: *Performance*),
- Prozessnachvollziehbarkeit (im englischen Original: *Process*) und
- Zweckklarheit (im englischen Original: *Purpose*).

Die Dimension Performance umfasst „*die Einschätzungen des Nutzers dahingehend, wie gut ein System dazu in der Lage ist, ihn bei der Erreichung seiner Ziele zu unterstützen*“ (Söllner et al. 2012a, S. 117). *Prozessnachvollziehbarkeit* bedeutet die Nutzereinschätzung, „*wie das System funktioniert und welche grundlegenden Prinzipien beachtet werden*“ (Söllner et al. 2012a, S. 117). *Zweckklarheit* betrachtet weniger die Eigenschaften des Systems, sondern die Beurteilung aus der Sicht des Nutzers, zu welchem Zweck das System entwickelt wurde. Deckt sich dieser Zweck mit dem Ziel des Nutzers, „*so entsteht das Gefühl, dass das System die Anliegen des Nutzers in den Vordergrund stellt und beachtet*“ (Söllner et al. 2012a, S. 117).

Auch wenn Forschungsarbeiten zeigen, dass diese Dimensionen Vertrauen in Informationstechnologien und deren Anbieter ausmachen, sollten die Cloud-Computing-Anbieter kritisch überprüfen, ob diese Dimensionen auch für den betrachteten Cloud-Computing-Dienst relevant sind. Zudem sind diese Dimensionen noch sehr abstrakt und lassen sich nicht direkt zu vertrauensbezogene Anforderungen ableiten (Söllner et al. 2012a), weshalb im nächsten Schritt konkrete Vertrauensdeterminanten erarbeitet werden.

13.4 Schritt 3: Identifikation relevanter Vertrauensdeterminanten

Im dritten Schritt wird die Entwicklungsaktivität „*Identifikation relevanter Vertrauensdeterminanten*“ bearbeitet und die Leitfrage beantwortet: „*Mit Hilfe welcher Vertrauensdeterminanten kann den Unsicherheiten entgegengewirkt werden?*“.

Die Forschung liefert bisher wenige Erkenntnisse, welche konkreten Determinanten das interpersonelle Vertrauen in den IT-Anbieter beeinflussen.

Um dennoch exemplarisch Vertrauensdeterminanten vorzugeben, wurden Interviews mit Cloud-Computing-Experten (siehe Kapitel 22) durchgeführt. Gemäß der Auswertung der Experteninterviews (Buch/Gebauer 2013; Buch et al. 2014), beeinflussen die folgenden Determinanten das Vertrauen in den Cloud-Computing-Anbieter (vgl. [Abbildung 2](#)):

- *Qualität der Dienstleistung* (umfasst Aspekte, die herangezogen werden, um Rückschlüsse auf die Qualität der Dienstleistung und dessen Anbieter zu ziehen, bspw. Pünktlichkeit, die Verfügbarkeit, die Zuverlässigkeit),
- *frühere Erfahrungen mit Dienstleistern* (umfasst alle früheren Erfahrungen, die der potenzielle Kunde zuvor schon selbst mit dem Dienstleister gemacht hat),
- *Empfehlungen Dritter* (umfasst alle persönlichen Empfehlungen, die der potenzielle Kunde von Dritten erhalten hat, wie zum Beispiel von Kollegen, Freunden oder von eingestellten Beratern) und
- *Kundenorientierung des Dienstleisters* (umfasst, inwieweit der Dienstleister sich auf seine Kunden einstellt und auf dessen Wünsche eingeht) (Buch et al. 2014).

Die Zuordnung der identifizierten Determinanten anhand der Experteninterviews zu den Dimensionen erfolgte rein deskriptiv. Die statistischen Zusammenhänge sowie die Vollständigkeit sollten in weiteren Studien empirisch überprüft werden.

Für das Vertrauen in die Technik hingegen liefert die Forschung bereits Erkenntnisse, welche Determinanten die jeweiligen Dimensionen beeinflussen (Söllner et al. 2012b). Diese können als Grundlage ebenfalls für Cloud-Computing verwendet werden. Jedoch sollte im Falle des konkreten Cloud-Computing-Dienstes kritisch geprüft werden, ob diese für den Anwendungsfall relevant sind. Gemäß Söllner et al. (2012a) werden im Systemvertrauen die drei Vertrauensdimensionen von zwölf Determinanten beeinflusst. Für die Vertrauensdimension *Performance* wurden nach Söllner et al. (2012a) folgende Vertrauensdeterminanten identifiziert (vgl. [Abbildung 2](#)):

- *Eignung* (umfasst die Einschätzung des Nutzers, wie gut das System grundsätzlich dazu geeignet ist, ihn bei der Erreichung des Ziels zu unterstützen),
- *Informationsgenauigkeit* (umfasst die Einschätzung des Nutzers, wie präzise die bereitgestellten Informationen sind),
- *Verlässlichkeit* (entspricht der Einschätzung des Nutzers, wie verlässlich das System über die Zeit hinweg ist) und
- *Komplettheit* (beschreibt die Einschätzung des Nutzers, dass das System sämtliche Funktionen beinhaltet, um das gewünschte Ziel zu erreichen). (Söllner et al. 2012a).

Die Vertrauensdimension *Prozessnachvollziehbarkeit* wird nach Söllner et al (2012a) von folgenden Vertrauensdeterminanten bestimmt (vgl. [Abbildung 2](#)):

- *Konsistenz* (beschreibt die Einschätzung des Nutzers, inwieweit sich das System konsistent, also widerspruchsfrei, verhält),
- *Verständlichkeit* (beinhaltet die Einschätzung des Nutzers, inwieweit für diesen verständlich ist, wie das System funktioniert),
- *Kontrolle* (bedeutet die Einschätzung des Nutzers bzgl. seiner wahrgenommenen Kontrolle über das System),
- *Vorhersagbarkeit* (umfasst die Einschätzung des Nutzers, inwieweit das zukünftige Verhalten des Systems antizipiert werden kann) (Söllner et al. 2012a).

Die dritte Vertrauensdimension für das Systemvertrauen, die *Zweckklarheit*, umfasst nach Söllner et al. (2012a) folgende Vertrauensdeterminanten (vgl. [Abbildung 2](#)):

- *Kommunikation des Einsatzzweckes* (beschreibt die Einschätzung des Nutzers, ob der gedachte Einsatzzweck des Systems von den Entwicklern kommuniziert wurde),

- *Wohlwollen der Entwickler* (umfasst die Einschätzung des Nutzers, ob die Entwickler seine Interessen beachten) und
- *Glaube* (umschreibt die Einschätzung des Nutzers, dass dieser sich auch in Zukunft auf das System verlassen kann) (Söllner et al. 2012a).

Auf dieser theoretischen Grundlage werden nun im folgenden Schritt vertrauensbezogene Anforderungen abgeleitet, um im letzten Schritt exemplarisch Lösungen für die Vertrauensproblematiken im Cloud-Computing-Umfeld abzuleiten.

13.5 Schritt 4: Ableitung vertrauensbezogener Anforderungen

Im vierten Schritt folgt die Entwicklungsaktivität „*Ableitung vertrauensbezogener Anforderungen*“. Hierbei wird die Leitfrage beantwortet: „*Welche Anforderungen können auf Basis der Determinanten abgeleitet werden?*“.

Der Standard IEEE 610.12-1990 (IEEE 1990) definiert den Begriff *Anforderung* (im englischen Original: *requirement*) wie folgt: „*Eine Anforderung ist:*

- 1) *Eine Bedingung oder Eigenschaft, die ein System oder eine Person benötigt, um ein Problem zu lösen oder ein Ziel zu erreichen.*
- 2) *Eine Bedingung oder Eigenschaft, die ein System oder eine Systemkomponente aufweisen muss, um einen Vertrag zu erfüllen oder einem Standard, einer Spezifikation oder einem anderen formell aufgelegten Dokument zu genügen.*
- 3) *Eine dokumentierte Repräsentation einer Bedingung oder Eigenschaft wie in (1) oder (2) definiert.*“ (Pohl 2007, S. 13).

Forschungsarbeiten liefern bereits eine Auswahl an vertrauensbezogenen Anforderungen für verschiedenste IT-Systeme (Hoffmann et al. 2012; Hoffmann/Söllner 2014; Hoffmann et al. 2013). Cloud-Computing-Anbieter, welche den Prozess zur systematischen Vertrauensunterstützung durchlaufen, können die nachfolgenden vertrauensbezogenen Anforderungen als Grundlage verwenden, sollten aber kritisch prüfen, ob diese für den konkreten An-

wendungsfall relevant sind. Hoffmann (2014) identifizierte die folgenden vertrauensbezogenen Anforderungen, wobei diese dem Anbietervertrauen oder dem Systemvertrauen zugeordnet sind.

Anforderungen zur Schaffung von Vertrauen in den Anbieter des Systems:

Nach Hoffmann (2014) soll der Anbieter ...

- Referenzen durch Dritte zur Applikation bereitstellen,
- die Bewertung der Applikation durch unabhängige Institutionen bereitstellen (Zertifizierung),
- Benutzern die Abgabe von Feedback zur Applikation ermöglichen und das Feedback von Benutzern zur Applikation veröffentlichen,
- den Benutzern den Kontakt zu ihm ermöglichen,
- eine Erklärung zum Datenschutz bereitstellen,
- eine Erklärung zur Datensicherheit bereitstellen (Hoffmann 2014).

Anforderungen zur Schaffung von Vertrauen in das System:

Nach Hoffmann (2014) soll der Anbieter ...

- verdeutlichen, welche Aufgaben die Applikation für die Benutzer erfüllt,
- Informationen über die Leistungsfähigkeit der Applikation bereitstellen,
- verdeutlichen, wie die Applikation ihre Aufgaben löst,
- die Benutzer darüber informieren, wie die Applikation funktioniert,
- eine Vorschau der Interaktion mit der Applikation bereitstellen (Hoffmann 2014).

Nach Hoffmann (2014) soll die Applikation ...

- die Benutzer bei Bedarf vor der Ausführung einer Funktion über diese Funktion informieren,
- den Benutzern den Status von Funktionen anzeigen,

- die Benutzer bei Bedarf über durchgeführte Vorgänge in der Applikation informieren,
- die Benutzer bei Bedarf über Vorgänge informieren,
- den unberechtigten Zugriff auf gespeicherte Daten verhindern,
- Aktivierung und Deaktivierung von Funktionalitäten durch die Benutzer ermöglichen,
- den Benutzern die erfolgreiche Ausführung von Vorgängen bestätigen,
- Benutzern das Rückgängigmachen von Vorgängen ermöglichen,
- den Benutzern Eingaben bestätigen (Hoffmann 2014, S. 193-230).

Zudem kann die Vertrauenswürdigkeit des Anbieters und des Systems auch durch das Aufzeigen von Rechtskonformität bzw. Rechtsverträglichkeit gefördert werden (Jandt 2008; Hoffmann 2014). Dementsprechend kann Vertrauen auch durch eine rechtmäßige sowie rechtsverträgliche Gestaltung der Technik gefördert werden (Jandt 2008).

13.6 Schritt 5: Ableitung vertrauensunterstützender Mehrwertdienste

Im Rahmen der Entwicklungsaktivität *„Ableitung vertrauensunterstützender Mehrwertdienste“* wird die Leitfrage *„Welche vertrauensunterstützenden Mehrwertdienste können auf Basis der Anforderungen abgeleitet werden?“* beantwortet. Dazu werden anhand der vertrauensbezogenen Anforderungen konkrete Lösungen, Maßnahmen oder Gestaltungselemente abgeleitet, um so den Cloud-Computing-Dienst vertrauensförderlicher zu gestalten.

Unter Verwendung der individuellen Ergebnisse aus Schritt eins bis Schritt vier sollten Cloud-Computing-Anbieter befähigt sein, für den zu entwickelnden oder angebotenen Cloud-Dienst gezielt vertrauensunterstützende Mehrwertdienste abzuleiten und umzusetzen. Da die Anwendbarkeit und die Inhalte dieses Schrittes sehr stark von dem betrachteten Anwendungsfall abhängen, können keine allgemeingültigen vertrauensunterstützenden Mehr-

wertdienste genannt werden. Dennoch werden im Folgenden beispielhaft einige Anregungen gegeben.

Um die Vertrauensdeterminante „*Empfehlungen durch Dritte*“ zu adressieren, sind folgende vertrauensunterstützenden Maßnahmen denkbar:

- Der Anbieter stellt eine Übersicht über die bisherigen Kunden bereit.
- Der Anbieter liefert einen Nachweis, dass auch unabhängige Institutionen den Dienst geprüft haben, z. B. durch den Erwerb und die präsente Darstellung eines Zertifizierungssiegels.
- Der Anbieter schafft Raum für Kundenrezensionen, bei dem bestehende Kunden ihre Erfahrungen mit dem Dienst und dem Anbieter potenziellen Neukunden zur Verfügung stellen.

Um die „*Kundenorientierung*“ stärker herauszustellen, können beispielhaft folgende Maßnahmen ergriffen werden:

- Der Anbieter betreibt eine 24-h-Hotline, um den (potenziellen) Kunden das Gefühl zu geben, im Notfall rund um die Uhr einen Ansprechpartner zu haben (Hoffmann 2014).
- Der Anbieter stellt dem Nutzer eine kostenlose Testversion zur Verfügung (Hoffmann 2014).
- Der Anbieter zeigt dem Kunden mit Hilfe einer Demonstration, welche Möglichkeiten zur Anpassung an die Kundenbedürfnisse bestehen.

Auch für die Vertrauensdeterminante „*Kontrolle*“ können anhand der Anforderungen verschiedenste vertrauensunterstützende Maßnahmen abgeleitet werden:

- Bei der Installation des Systems wird die Zustimmung vom Nutzer für alle Funktionen eingeholt, die kritisch für diesen sein könnten. Zudem sollte dieser die Möglichkeit haben, diese Zustimmung jederzeit zu verändern.
- Das System gibt dem Nutzer proaktiv Rückmeldung zum aktuellen Stand der durchgeführten Vorgänge (z.B. Vorgang erfolgreich beendet).

- Der Anbieter stellt dem Kunden ohne dessen Aufforderung alle Informationen bereit, die dieser benötigt, um seinen rechtlichen Pflichten bei der Nutzung von Cloud-Computing-Diensten nachzukommen.

Zudem wurden weitere Maßnahmen zur vertrauensförderlichen Gestaltung von Cloud-Computing-Diensten mit Hilfe von Experteninterviews identifiziert (siehe Kapitel 21).

13.7 Zusammenfassung

In diesem Kapitel wurde die Methode zur Entwicklung vertrauensunterstützender Komponenten für sozio-technische ubiquitäre Systeme nach Söllner et al. (2012a) auf das Cloud-Computing-Umfeld übertragen und weiterentwickelt. Unter Anwendung des hier beschriebenen Prozesses zur systematischen Vertrauensunterstützung ist der Anbieter von Cloud-Computing-Diensten befähigt, diese zukünftig vertrauensförderlicher zu gestalten bzw. am Markt anzubieten. Die Abfolge der Schritte kann für jeden Cloud-Computing-Dienst durchlaufen werden. Dabei liefern die exemplarischen Antworten zu den Leitfragen bereits eine erste Hilfe zur Beantwortung. Dennoch sollten die Cloud-Computing-Anbieter die Übertragbarkeit dieser exemplarischen Anregungen auf den konkreten Anwendungsfall kritisch überprüfen.

13.8 Literaturverzeichnis

- Buch, M.; Gebauer, L. (2013):** Maßnahmenkatalog zur Vertrauenserrhöhung im Cloud Computing. In: Leimeister, J.M. (Hrsg.), (4. Aufl.). Kassel, Deutschland: Working Paper Series, Chair for Information Systems, Kassel University.
- Buch, M.; Gebauer, L.; Hoffmann, H. (2014):** Vertrauen in Cloud Computing schaffen – Aber wie? In: WIRTSCHAFTSINFORMATIK & MANAGEMENT, Vol. 03/2014 (2014), S. 67-77.
- Hoffmann, A. (2014):** Anforderungsmuster zur Spezifikation soziotechnischer Systeme – Standardisierte Anforderungen der Vertrauenswürdigkeit und Rechtsverträglichkeit (Dissertation) Kassel University Press, Kassel, Deutschland 2014.
- Hoffmann, A.; Hoffmann, H.; Söllner, M. (2013):** Fostering Initial Trust in Applications – Developing and Evaluating Requirement Patterns for Application Websites. Präsentiert auf der 21st European Conference on Information Systems, Utrecht, Niederlande.

- Hoffmann, A.; Söllner, M.; Hoffmann, H. (2012):** Twenty software requirement patterns to specify recommender systems that users will trust. Präsentiert auf der 20th European Conference on Information Systems, Barcelona, Spanien.
- Hoffmann, H.; Söllner, M. (2014):** Incorporating behavioral trust theory into system development for ubiquitous applications. In: Personal and Ubiquitous Computing, Vol. 18 (2014) No. 1, S. 117-128.
- IEEE (1990):** Standard Glossary of Software Engineering Terminology, IEEE Std 610.12-1990. IEEE Computer Society Press 1990.
- Jandt, S. (2008):** Vertrauen im Mobile Commerce – Vorschläge für die rechtsverträgliche Gestaltung von Location Based Services, Nomos, Baden-Baden, Deutschland 2008.
- Lee, J.D.; See, K.A. (2004):** Trust in Automation: Designing for Appropriate Reliance. In: Human Factors: The Journal of the Human Factors and Ergonomics Society, Vol. 46 (2004) No. 1, S. 50-80.
- Mayer, R.C.; Davis, J.H.; Schoorman, F.D. (1995):** An Integrative Model of Organizational Trust. In: The Academy of Management Review, Vol. 20 (1995) No. 3, S. 709-734.
- Pohl, K. (2007):** Requirements Engineering: Grundlagen, Prinzipien, Techniken, Dpunkt-Verlag 2007.
- Söllner, M.; Hoffmann, A.; Hoffmann, H.; Leimeister, J.M. (2012a):** Vertrauensunterstützung für sozio-technische ubiquitäre Systeme. In: Zeitschrift für Betriebswirtschaft, (2012) No. 4, S. 109-140.
- Söllner, M.; Hoffmann, A.; Hoffmann, H.; Wacker, A.; Leimeister, J.M. (2012b):** Understanding the Formation of Trust in IT Artifacts. Präsentiert auf der 33rd International Conference on Information Systems, Orlando, USA.
- Söllner, M.; Pavlou, P.; Leimeister, J.M. (2013):** Understanding Trust in IT Artifacts – A new Conceptual Approach. Präsentiert auf dem 73th Academy of Management Annual Meeting, Orlando, USA.

14 Open Service Innovation Online-Community für Cloud-Service-Ökosysteme

M. Kunz, P. Ebel, J.M. Leimeister

14.1 Einleitung

Innovationen spielen für einen nachhaltigen Unternehmenserfolg eine essenzielle Rolle. Besonders in Zeiten steigenden Wettbewerbsdrucks, immer kürzerer Produktlebenszyklen und limitierter F&E-Ressourcen sind Innovationen ein Kernerfolgsfaktor, um sich als Unternehmen in einem Markt etablieren und gegenüber Wettbewerbern positionieren zu können (Leimeister 2012). Rein unternehmensinterne Innovationen spielen zunehmend eine untergeordnete Rolle. Verstärkt rückt der Kunde in den Fokus von Innovations-tätigkeiten (Leimeister 2014). Dies gilt insbesondere im Hinblick auf die Ausgestaltung von Produkten und Services im Sinne von nutzerzentrierten Innovationen. Solche Innovationen ermöglichen es, kundenspezifische Anforderungen und Bedürfnisse zu ermitteln und gezielt in Angeboten zu adressieren.

Ein solches Vorgehen könnte die Adaption des Cloud-Computings fördern, indem es dazu beiträgt, die große Unsicherheit, die mit dieser Dienstleistung verbunden ist, zu reduzieren (Kunz et al. 2014). Durch eine direkte Kooperation im Innovationsprozess können Bedürfnisse – vor allem im Hinblick auf Vertrauens- und Sicherheitsthemen – identifiziert und nutzer-gerechte Lösungen entwickelt werden. Beteiligte Cloud-Nutzer fungieren dann nicht nur als Nutzer von Services, sondern als Mitgestalter, was letztlich auch zu gesteigerten Weiterempfehlungsraten von Services führen kann. Ein solcher Ansatz wird in der Literatur auch als Open Innovation bezeichnet (siehe hierzu auch Kapitel 7), wobei externe Stakeholder eines Unternehmens in den Innovationsprozess zur Steigerung des Innovationspotenzials direkt einbezogen werden (Reichwald/Piller 2006).

Die in diesem Kapitel vorgestellte *Open Service Innovation Online-Community für Cloud-Service-Ökosysteme* fußt auf dem Grundkonzept des „Open

Innovation“-Ansatzes und soll Unternehmen dabei unterstützen, einfach und intuitiv innovative Ideen im Bereich des Cloud-Computings zu generieren und diese in Zusammenarbeit mit unterschiedlichen Stakeholdern in marktfähige Geschäftsmodelle umzusetzen. Unterstützt wird der gesamte Geschäftsmodellentwicklungsprozess, wie in Kapitel 7 vorgestellt, zudem durch unterschiedliche Methoden und Werkzeuge. Ein Kernwerkzeug stellt dabei das Business Model Canvas (BMC) nach Osterwalder/Pigneur (2011) dar. Mit dem BMC wurde ein strategisches Management- und Unternehmer-Tool zur Visualisierung von Geschäftsmodellen entwickelt. Anhand von neun wichtigen Bestandteilen (Kundensegment, Wertangebot, Kanäle, Kundenbeziehungen, Einnahmequellen, Schlüsselressourcen, Schlüsselaktivitäten, Schlüsselpartner, Kostenstruktur) beschreibt das BMC ein Geschäftsmodell.

14.2 Zentrale Merkmale der Open Service Innovation Online-Community

14.2.1 Allgemeine Einführung

In diesem Kapitel sollen überblicksweise die Kernmerkmale der Open Service Innovation Online-Community für Cloud-Service-Ökosysteme dargestellt werden. Diese Online-Community soll cloud-interessierten Nutzern sowie Cloud-Service anbietenden IT-Unternehmen dabei helfen, Ideen zu veröffentlichen und gemeinschaftlich auszuarbeiten. Die Community ist nicht nur auf cloud-relevante Themen ausgerichtet, sondern kann zu unterschiedlichen Innovationsthemen in Anspruch genommen werden. Zentral für die Online-Community ist, dass der Entwicklungsprozess zweiteilig gegliedert ist. So sollen zum einen reine Innovationsideen entwickelt und veröffentlicht und zum anderen auch gesamte Geschäftsmodelle ausgearbeitet werden. Der Fokus auf letzteres hilft dabei, eine ganzheitliche Sicht auf eine gezielte Problemstellung zu richten und sowohl die Unternehmens- als auch die Kundensicht zu betrachten.

Abbildung 1 zeigt überblicksweise den Startbildschirm der Online-Community. Auf diesem werden allgemeine Informationen, wie neueste Ideen, aktivste Nutzer, aktuelle News oder neue Mitglieder, bereitgestellt. Darüber

Abbildung 1: Startseite Open Service Innovation Online-Community (Eigene Darstellung).

hinaus soll die Community an Social Media angebunden werden. Um jedoch einen vollständigen Zugriff auf unterschiedliche Funktionen zu haben, muss zunächst ein Mitgliedskonto erstellt werden. Nach erfolgter Registrierung wird es dem Nutzer nun möglich sein, eigene Ideen im Bereich „Ideen erstellen“ zu veröffentlichen und zu diskutieren. Unter der Maske „Ideen einsehen“ können Ideen der Community eingesehen und durchsucht werden. Dies ermöglicht je nach Interesse, die Identifikation relevanter Themenschwerpunkte. Unter dem Reiter „Business Plan Gruppen“ können Ideen zu gesamten Geschäftsmodellen ausgearbeitet und verfeinert werden. Dies erfolgt zumeist in Kooperation mit einem Unternehmen und weiteren betroffenen Interessengruppen. Über diese Funktion lassen sich marktreife Cloud-Service-Geschäftsmodelle entwickeln. Diese drei zuvor aufgeführten Funktio-

nen bilden den Kern der Lösung. Neben diesen zentralen Funktionen finden sich Zusatzfunktionen wie „Community“, „Profil“ und „News“. Sowohl die Kern- als auch Zusatzfunktionen werden in den folgenden Abschnitten näher beleuchtet.

14.2.2 Ideen erstellen

14.2.2.1 Erstellungsprozess von Einzel-, Gemeinschafts- und Businessplan-Ideen

Bei der Ausarbeitung der Idee unter der Funktion „Idee erstellen“ haben Anwender die Möglichkeit, entweder eine Gemeinschaftsidee oder eine Einzelidee zu erstellen ([Abbildung 2](#)). Gemeinschaftsideen können von der Community angesehen, bewertet, kommentiert oder weiterbearbeitet werden. Die Gemeinschaftsidee kann auf diese Weise mit neuen Aspekten angereichert werden. Eine Änderungshistorie wird hierbei gespeichert. Des Weiteren ist es möglich Änderungen jederzeit zurückzusetzen. Im Gegensatz zu den Gemeinschaftsideen können Einzelideen ausschließlich vom Anwender selbst überarbeitet werden. Andere Mitglieder der Community können die Einzelidee ansehen, kommentieren und bewerten. Eine Einzelidee ist u. a. dann sinnvoll, wenn sie einer breiten Masse an Kunden oder Mitgliedern vorgestellt und von diesen bewertet oder kommentiert werden soll. Dies kann u.a. dann der Fall sein, wenn Unternehmen neue Angebote planen, die jedoch keiner weiteren Bearbeitung durch Kunden oder andere Stakeholder bedürfen. Eine Gemeinschaftsidee hingegen hat konkret das Ziel, eine Idee gemeinsam mit anderen Mitgliedern auszuarbeiten und gemeinsam zu einem Konsens zu bringen. Dies könnte u. a. der Fall sein, wenn neue Services oder Produkte, etwa eine Branche, ermittelt werden sollen. Als Beispiel sei eine Software-as-a-Service (SaaS)-Lösung für Bauzeichner genannt. Bei einer Gemeinschaftsidee könnten direkt betroffene Anspruchsgruppen, hier Bauzeichner, zur Ausarbeitung der SaaS-Lösung zur Zusammenarbeit auf der Plattform eingeladen werden. Sowohl die Einzel- als auch die Gemeinschaftsideen sind für die Bearbeitung auf einen bestimmten Zeitraum begrenzt.

Abbildung 2: Funktion „Ideen erstellen“ (Eigene Darstellung).

In der Funktion der Ideenerstellung, unabhängig davon ob Gemeinschaftsidee, Einzelidee oder Businessplan-Idee, ist es notwendig, vorab relevante Informationen bereitzustellen, um Missverständnisse bei der Community zu vermeiden. Je detaillierter eine Idee beschrieben wird, desto verständlicher ist sie für die Community und lässt so eine fokussierte Bearbeitung der Idee zu. Die bereitzustellenden Informationen beziehen sich wie in [Abbildung 3](#) ersichtlich auf den Titel der Idee, eine Zusammenfassung und Beschreibung der Idee sowie Schlagworte und mögliche Dateianhänge. Die Informationen können wie folgt beschrieben werden.

- **Titel:** Der Anwender wird aufgefordert, seiner Idee einen Titel zu geben.

The screenshot shows a web browser window with the address bar displaying "Value4Cloud". The page header features a navigation menu with links: Home, Idee erstellen (highlighted), Idee ansehen, Community, Dein Profil, News, Businessplan Gruppen, and Abmelden. The main content area is titled "Businessplan erstellen" and contains several form fields: "Titel: *" (a single-line text input), "Zusammenfassung: *" (a multi-line text input), "Beschreibung der Idee: *" (a large multi-line text input), and "Schlagworte: *" (a single-line text input). Below these fields is a section for "Dateianhänge" (Attachments), which includes a "Neue Datei anfügen:" label, a "Datei auswählen" button, and an "Anfügen" button. At the bottom of the form are two buttons: "Speichern" (Save) and "Vorschau" (Preview).

Abbildung 3: Eingabe von Informationen zur Erstellung einer Idee (Eigene Darstellung).

- **Zusammenfassung:** In maximal drei Sätzen soll der Anwender seine Idee zusammenfassen. Orientieren soll er sich hierbei an den Fragen „Worum geht es bei meiner Idee?“, „Für welche Bereiche ist meine Idee relevant?“ und „Was ist das Besondere an meiner Idee?“.
- **Beschreibung der Idee:** In dem Feld „Beschreibung der Idee“ hat der Anwender die Möglichkeit, seine Idee ausführlich zu beschreiben. Empfohlen wird die Verwendung von mindestens 50 Wörtern, um eine aussagekräftige Beschreibung der Idee sicherzustellen.
- **Schlagworte:** Der Anwender wird in diesem Feld aufgefordert, eine Liste mit Schlagwörtern rund um die Idee zu erstellen.
- **Dateianhänge:** Darüber hinaus wird dem Anwender die Möglichkeit geboten, seiner beschriebenen Idee Dateianhänge anzufügen.

Die erstellte Idee kann nun von der Community abonniert und über diverse soziale Netzwerke geteilt werden ([Abb. 4](#)). Darüber hinaus wird die Möglichkeit geboten, diese Idee mit einem Klick auf den „Gefällt mir Button“ zu „ liken“. Mit Hilfe eines Kommentarfeldes sind die Mitglieder der Community in der Lage, die erstellte Idee zu kommentieren und ihre Anregungen kundzutun. Dies soll dem Ideenersteller dabei helfen, wichtige Informationen zu der eigenen Idee zu sammeln und auf Basis dieser gegebenenfalls Anpassungen vorzunehmen.

Der Hintergrund einer solchen ersten Ideenerstellung besteht darin, zunächst Ideen zu eruieren, bevor diese gegebenenfalls in weiteren Schritten, innerhalb der Businessplan-Gruppen, gemeinschaftlich zu Geschäftsmodellen ausgearbeitet werden.

Der gesamte Prozess dieser Ausarbeitung ist, wie bereits dargestellt, in zwei Phasen gegliedert. In der ersten Phase wird zunächst eine bestimmte Idee zu einem ausgewählten Themenfeld des Cloud-Computing innerhalb der Community bekannt gemacht, sodass eine konkrete Problemstellung herausgearbeitet werden kann. In einem weiteren Schritt können dann die entwickelten Ideen anhand der auf der Plattform abgebildeten Werkzeuge weiter ausgearbeitet werden.

The screenshot shows the Value4Cloud web application. At the top, there is a navigation bar with the site name 'Value4Cloud' and a search bar. Below this is a secondary navigation bar with links: Home, Idee erstellen (highlighted), Idee ansehen, Community, Dein Profil, News, Businessplan Gruppen, and Abmelden. The main content area is divided into several sections:

- Beispielidee:** A section showing an example idea by 'Max Mustermann' from '15.05.2014'. It includes a description: 'Diese Idee ist eine Einzelidee. Im Gegensatz zu Kollaborationsideen kann diese Idee nur von ihrem ursprünglichen Ideengeber überarbeitet werden. Du kannst Anregungen zu dieser Idee aber über die Kommentarfunktion hinzufügen.'
- Teilen und Bewerten:** A section with buttons for 'Gefällt mir', 'Inhalt teilen', and a dropdown menu for 'Abbonieren'. Below the dropdown is a checkbox for 'Diese Seite abonnieren' and a 'Speichern' button.
- Zusammenfassung:** A section with a label 'Beispielidee:' and a text input field for 'Beschreibung der Idee'.
- Kommentare:** A section with a label 'Kommentar hinzufügen' and a 'Betreff:' label followed by a text input field. Below this is a larger text area for the comment.

At the bottom of the form, there are two buttons: 'Speichern' and 'Vorschau'.

Abbildung 4: Idee erstellen und bewerten (Eigene Darstellung).

14.2.2.2 Die Besonderheiten der Businessplan-Gruppen

Businessplan-Gruppen beschäftigen sich mit der Ausarbeitung von Geschäftsmodellen von Produkten und Services. Der Unterschied zur reinen Ideenausarbeitung besteht darin, dass Geschäftsmodelle wesentlich detaillierter ausgearbeitet werden können. In einer solchen Bearbeitung wird der Fokus nicht nur auf die Kundenseite gelegt, sondern auch auf die des Unternehmens selbst und dabei insbesondere auf Ressourcen und Partner, die ein Unternehmen zur Umsetzung einer Idee benötigt, sowie auf die mit der Idee

verbundenen Kosten. Die Ausgestaltung eines Geschäftsmodells basiert auf dem bereits vorgestellten Werkzeug, dem Business Model Canvas (BMC). Die Nutzung des Werkzeuges wird zusätzlich durch Methoden des Collaboration Engineerings und den damit angebotenen weiteren Werkzeugen unterstützt. Diese sollen dabei helfen, den gemeinschaftlichen Kollaborationsprozess zu vereinfachen und zu unterstützen. Zu diesen Methoden gehören u. a. Anzeigen von Unterstützungsbedarfen, Versionshinweise, Chatfunktionen und Protokollnachrichten. Letztere dienen dazu, Neuerungen und Änderungen nachzuvollziehen und als Ersteller diese gegebenenfalls wieder zurückzusetzen.

Durch die Darstellung eines Geschäftsmodells über diese Plattform wird die Basis für jede weitere Analyse geschaffen. Ausgearbeitete Geschäftsmodelle helfen dabei, das bestehende Geschäft zu verstehen und Vergleiche anstellen zu können. Auf diese Weise können beispielsweise Optimierungspotenziale bei eigenen Geschäftsideen aufgedeckt werden. Die Geschäftsideen werden so systematisch entwickelt.

Entscheidet sich ein Mitglied der Community dazu, ein Geschäftsmodell kollaborativ auszuarbeiten, so müssen von diesem, ähnlich der Informationen der Ideenerstellung, Daten bereitgestellt werden, die es ermöglichen, das zu entwickelnde Geschäftsmodell zu verstehen. Neben den in 14.2.2.1 diskutierten relevanten Informationen erfordert die Geschäftsmodellbearbeitung weitere Informationen gemäß der Logik des BMC ([Abb. 5](#)). Diese Informationen gliedern sich in die Merkmale *Titel*, *Schlagworte*, *Key Activities*, *Value Propositions*, *Customer Relationships*, *Customer Segments*, *Key Resources*, *Channels*, *Cost Structure*, *Revenue Streams* und *Key Partners*. Diese Merkmale werden wie folgt beschrieben:

Im Feld **Titel** wird der Anwender aufgefordert, seinem Ideenkonzept einen Titel zu geben. Der Titel soll dabei helfen, den Kern der Idee sofort zu erkennen und als Mitglied entscheiden zu können, ob ein Beitrag auf Basis eigener Kompetenzen geleistet werden kann. Zusätzlich wird der Anwender aufgefordert, seine Idee über eine Liste mit **Schlagwörtern** zu konkretisieren. Dies hilft dabei, eine Idee gemäß eigener Präferenzen in der Funktion „Ideen ansehen“ zu suchen. Diesem Merkmal kommt besonders dann Bedeutung zu, wenn eine Vielzahl von Ideen in der Community veröffentlicht wird.

Je mehr Ideen eine Community erstellt, desto unübersichtlicher kann die Ideensuche werden.

Einer der neun Bausteine des BMC ist der Baustein **Key Activities**. Dieser Baustein beschreibt Handlungen, auf die ein Unternehmen angewiesen ist, um erfolgreich agieren zu können (Osterwalder/Pigneur 2011). Hier steht die Unterbreitung und Schaffung von Wertangeboten, das Erreichen von Märkten, die Aufrechterhaltung von Kundenbeziehungen und die Erzielung von Gewinnen im Mittelpunkt. Eine Kategorisierung kann in Bezug auf Produktion, Problemlösung und Plattform/Netzwerk vorgenommen werden. Dieser Baustein bietet dem Anwender die Möglichkeit, die wichtigsten Aktivitäten zu beschreiben, die erfolgen müssen, damit das Geschäftsmodell funktioniert. Folgende Fragen sollen hierbei beantwortet werden: Welche Schlüsselaktivitäten erfordern unsere Wertangebote? Unsere Distributionskanäle? Unsere Kundenbeziehungen? Unsere Einkommensquellen?

Der Baustein **Value Proposition** (Wertangebot) stellt ein entscheidendes Argument für Kunden in Bezug auf den Kauf eines Produktes oder einer Dienstleistung dar. Der Fokus liegt jedoch nicht nur auf einzelnen Produkten oder Services, sondern vielmehr im Angebot von Bündeln aus Produkten und/oder Services (Osterwalder/Pigneur 2011). Hierbei steht insbesondere der Nutzen des Kunden im Vordergrund. Dieser Nutzen kann beispielsweise durch die Neuheit, die Leistung, die Anpassung an Kundenwünsche, den Preis, das Design und die Verfügbarkeit von Produkten oder Dienstleistungen entstehen. Die Aufgabe des Anwenders ist es somit, in diesem Feld das Paket von Produkten und Dienstleistungen zu beschreiben, das für ein bestimmtes Kundensegment Wert schöpft. Folgende Fragen sollen hierbei handlungsleitend sein: Welchen Wert vermitteln wir dem Kunden? Welche der Probleme unseres Kunden helfen wir zu lösen? Welche Produkt- und Dienstleistungspakete bieten wir jedem Kundensegment an? Welche Kundenbedürfnisse erfüllen wir?

Der Baustein **Customer Relationship** befasst sich mit der Frage, ob das Unternehmen eher eine persönliche oder automatisierte Beziehung zum Kunden eingehen möchte (Osterwalder/Pigneur 2011). Dabei hat die Entscheidung für eine Art der Beziehung Auswirkungen auf die Kundenakquise, Kundenpflege, Verkaufssteigerung sowie die gesamte Kundenerfahrung. Der

Anwender beschreibt in diesem Baustein die Arten von Beziehungen, die er mit seiner Idee mit bestimmten Kundensegmenten eingeht. Folgende Fragen sollen dabei beantwortet werden: Welche Art von Beziehung erwartet jedes unserer Kundensegmente von uns? Welche haben wir eingerichtet? Wie sind sie in unser übriges Geschäftsmodell integriert? Wie kostenintensiv sind sie?

In dem Feld **Customer Segment** definiert der Anwender die verschiedenen Gruppen von Personen, die ein Unternehmen erreichen und bedienen will (Osterwalder/Pigneur 2011). Um Kunden auch individuell ansprechen zu können, werden Kundengruppen häufig anhand unterschiedlichster Merkmale differenziert. Der Zusammenhang mit Geschäftsmodellen besteht darin, dass ein Geschäftsmodell entweder ein oder mehrere Segmente von Kunden erfassen kann. Dabei können Kundensegmente unterschiedliche Ausprägungen haben. Folgende Fragen sollen dabei beantwortet werden: Für wen schöpfen wir Wert? Wer sind unsere wichtigsten Kunden?

Der Baustein **Key Resources** bietet dem Anwender die Möglichkeit, die wichtigsten Wirtschaftsgüter zu beschreiben, die für das Funktionieren eines Geschäftsmodells notwendig sind (Osterwalder/Pigneur 2011). Diese Schlüsselressourcen können finanzieller, intellektueller, physischer oder menschlicher Natur sein. Dabei ist sekundär, ob die Schlüsselressourcen im Besitz des Unternehmens sind, von Schlüsselpartnern gekauft oder vom Unternehmen selbst geleast werden. Folgende Fragen sollen dabei beantwortet werden: Welche Schlüsselressourcen erfordern unsere Wertangebote? Unsere Distributionskanäle? Unsere Kundenbeziehungen? Unsere Einnahmequellen?

Mit Hilfe des Bausteines **Cost Structure** beschreibt der Anwender alle Kosten, die bei der Ausführung seines Geschäftsmodells anfallen (Osterwalder/Pigneur 2011). Die Schaffung von Werten ist mit Kosten verbunden. Besonders der Unterschied in der Kostenstruktur zwischen unterschiedlichen Geschäftsmodellen ist hierbei zu beachten. Folgende Fragen sollten bei der Erstellung und späteren Ausarbeitung der Idee beantwortet werden: Welches sind die wichtigsten mit unserem Geschäftsmodell verbundenen Kosten? Welche Schlüsselaktivitäten sind am teuersten? Welche Schlüsselressourcen sind am teuersten?

The screenshot shows the 'Value4Cloud' web interface for creating a business plan. The header includes navigation links: Home, Idee erstellen, Idee ansehen, Community, Dein Profil, News, Businessplan, Gruppen, and Abmelden. The main form is titled 'Businessplan erstellen' and contains the following sections:

- Titel ***: A text input field.
- Schlagerwörter ***: A text input field with a circular icon on the right.
- Zielgruppe:** A dropdown menu labeled 'Gruppen' with a checkbox for 'Zielgruppe 1'.
- Textkörper:** A large text input area.
- Speichern** and **Vorschau**: Two buttons.
- Versionsinformation:** A section with a dropdown arrow and a text input field labeled 'Protokollnachricht'.
- Dateianhänge:** A section with a dropdown arrow, a 'Neue Datei anhängen:' label, a 'Datei auswählen' button, and an 'Anfügen' button.
- Key Activities:**, **Value Propositions:**, **Customer Relationships:**, **Customer Segments:**, **Key Resources:**, **Channels:**, **Cost Structure:**, **Revenue Streams:**, and **Key Partners:**: Each of these sections has a corresponding text input field.

Abbildung 5: Businessplan erstellen (Eigene Darstellung).

In dem Eingabefeld **Channels** beschreibt der Anwender, wie nach seinem Ideenkonzept seine beschriebenen Kundensegmente erreicht und angesprochen werden, um das Wertangebot zu vermitteln (Osterwalder/Pigneur 2011). Den Kommunikations-, Distributions- und Verkaufskanälen kommt eine Schnittstellenfunktion zu, denn diese verbinden das Unternehmen mit seinen Kunden. Dabei können fünf unterschiedliche Kanaltypen identifiziert werden, nämlich Verkaufsabteilungen, Internetverkauf, eigene Filialen, Partnerfilialen und Großhändler. Folgende Fragen sollen hierbei beantwortet werden: Über welche Kanäle wollen unsere Kundensegmente erreicht werden? Wie erreichen wir sie jetzt? Wie sind unsere Kanäle integriert? Welche funktionieren am besten? Welche sind am kosteneffizientesten? Wie integrieren wir sie in die Kundenabläufe?

Das Feld **Revenue Streams** soll vom Anwender mit Informationen über die Einkünfte ausgearbeitet werden, die sein Geschäftsmodell nach seinem Ideenkonzept aus jedem Kundensegment bezieht (Umsatz – Kosten = Gewinn) (Osterwalder/Pigneur 2011). Die Einnahmequellen zeigen, wodurch Umsätze erlangt werden. Dabei können Einnahmequellen von Geschäftsmodellen in zwei Arten unterschieden werden. Zum einen können durch Transaktionseinnahmen einmalige Kundenzahlungen generiert werden und zum anderen ist die Möglichkeit wiederkehrender Einnahmen gegeben. Diese Einnahmeart kann u. a. durch Güterverkauf, Nutzungsgebühren, Mitgliedschaftsgebühren, Leasing, Lizenzen, Maklergebühren und Werbung realisiert werden. Folgende Fragen sollen hierbei beantwortet werden: Für welchen Wert sind unsere Kunden wirklich zu zahlen bereit? Wofür bezahlen sie jetzt? Wie bezahlen sie jetzt? Wie würden sie gerne bezahlen? Wie viel trägt jede Einnahmequelle zum Gesamtumsatz bei?

In Bezug auf das Merkmal **Key Partners** beschreibt der Anwender das Netzwerk von Lieferanten und Partnern, die zum Gelingen seines Ideenkonzeptes beitragen (Osterwalder/Pigneur 2011). Partnerschaften werden von Unternehmen aus den unterschiedlichsten Gründen eingegangen. Auf der einen Seite kann eine Partnerschaft der Grundstein eines Geschäftsmodells sein und auf der anderen Seite das Geschäftsmodell selbst verbessern. Generell können vier Arten von Partnerschaften unterschieden werden. Erstens können Unternehmen, die nicht im direkten Wettbewerb stehen, strategische

Allianzen eingehen. Zweitens können Unternehmen, die im Wettbewerb stehen, strategische Partnerschaften eingehen. Drittens können zur Entwicklung neuer Geschäfte Joint Ventures gebildet. Viertens kann eine Käufer-Anbieter-Beziehung aufgebaut werden. Folgende Fragen sollen hierbei beantwortet werden: Wer sind unsere Schlüsselpartner? Wer sind unsere Schlüssellieferanten? Welche Schlüsselressourcen beziehen wir von Partnern?

Nach der finalen Bearbeitung des Ideengebers kann die Community das erstellte Geschäftsmodell gemäß der Standardvorlage des BMC einsehen ([Abbildung 6](#)) und über die Kommentarfunktion kommentieren. Zusätzlich zur reinen Kommentarfunktion ist jedoch auch die Möglichkeit gegeben, das erstellte Geschäftsmodell weiterzubearbeiten. Änderungen werden schließlich im Versionsprotokoll angezeigt.

Unter der Funktion der Businessplan-Gruppen können alle veröffentlichten Geschäftsmodelle eingesehen werden. Diese Übersicht beinhaltet die folgenden Komponenten ([Abbildung 7](#)):

- **Informationen zur Gruppe:** Diese Komponente enthält Informationen zum Namen der Gruppe, zur Anzahl der Mitglieder und zur Anzahl der hochgeladenen Geschäftsmodelle. Letzteres zeigt, dass mehrere Geschäftsmodelle eingereicht und diskutiert werden können. Ideenersteller können zudem weitere Benutzer zur Gruppe einladen. Über den „Mitgliedschaft verwalten“-Button können die Mitglieder die Gruppe auf Wunsch verlassen.
- **Gruppenmitglieder:** Dieses Feld zeigt, welche Mitglieder der Gruppe angehören. Dargestellt werden die Mitglieder mit Profildetails. Des Weiteren ist ersichtlich, welches Mitglied der Gruppenmanager ist.
- **Vorgeschlagene Mitglieder:** Themennahe Mitglieder aus der Community, die hilfreich in der weiteren Bearbeitung der Geschäftsmodelle sein können, werden in diesem Feld vorgeschlagen.
- **Experten für diese Gruppe suchen:** Dieses Feld ermöglicht eine Expertensuche gemäß der Schlagwörter der zu entwickelnden Idee.

Value4Cloud

Home Idee erstellen Idee ansehen Community Dein Profil News **Businessplan Gruppen** Abmelden

Beispielbusinessplan

- Max Mustermann
- Beispielbusinessplan
- 7 Mitglieder

Businessplan überarbeiten

Vorschau ansehen

Informationen zum Business Model Canvas

Businesspläne auf Value4Cloud basieren auf dem Business Model Canvas. Wie du den Canvas verwendest, erfährst du hier:

Key Partners

Key Activities

Value Propositions

Customer Relationships

Customer Segments

Key Resources

Channels

Revenue Streams

Cost Structure

Kommentare

Kommentar hinzufügen

Betreff:

Speichern

Vorschau

Abbildung 6: Businessplan überarbeiten & kommentieren (Eigene Darstellung).

Value4Cloud

[Home](#) | [Idee erstellen](#) | [Idee ansehen](#) | [Community](#) | [Dein Profil](#) | [News](#) | [Businessplan Gruppen](#) | [Abmelden](#)

Beispielgruppe

- Beispielgruppe
- 2 Businesspläne
- 7 Mitglieder

Mitglieder einladen

Mitgliedschaft verwalten

Businessplan erstellen

Gruppenmitglieder

Mitglied 1

Mitglied 2

Mitglied 3

Mitglied 4

Mitglied 5

Mitglied 6

Gruppenmitglieder

Max Mustermann
[Zur Gruppe einladen](#)

Infos zu Businessplangruppen

Die Businessplan Gruppen sollen es Euch ermöglichen die Ideenausarbeitung strukturierter und effektiver zu gestalten. Innerhalb dieser Gruppen, könnt ihr eure Ideen mit Hilfe des „Business Model Canvas“ von Alexander Osterwalder Stück für Stück weiterentwickeln. Das Canvas soll euch dabei unterstützen bestehende Geschäftsideen zu analysieren und weiter zu entwickeln, Ideenkonzepte zu dokumentieren und auszulesen oder neue Geschäftsideen zu entdecken und festzuhalten. Eure Geschäftsmodelle sind nur für Gruppenmitglieder sichtbar, d.h. jede Idee hat ihr eigenes Canvas. Ihr könnt jedoch jederzeit andere Mitglieder, mit bestimmten benötigten Fähigkeiten mittels Profilsuche identifizieren und zur Mitarbeit in einer Gruppe einladen.

Businesspläne in der Gruppe

Titel	Zuletzt aktualisiert wann	Kommentare
Beispiel 1	14.05.2014	6 Kommentare
Beispiel 2	13.04.2014	4 Kommentare

Shout box

Absenden

Experten für diese Gruppe

Abbildung 7: Businessplan-Gruppen (Eigene Darstellung).

- **Businesspläne in dieser Gruppe:** Diese Funktion gibt eine Übersicht über Titel, letzte Aktualisierung und Anzahl der Kommentare der in der Gruppe erstellten Geschäftsmodelle.
- **Shout box:** Eine Shout box innerhalb der Gruppe bietet der Community die Möglichkeit, sich gegenseitig auszutauschen und ohne große Schnittstellen zu kommunizieren.

Die Funktion der Geschäftsmodellentwicklung – Businessplan-Gruppen – ermöglicht somit eine strukturierte und effektive Vorgehensweise von der Ausarbeitung einer Idee bis hin zum Prototyp eines Geschäftsmodells. Die Grundstruktur des BMC hilft letztlich dabei, die Ideen zu analysieren, weiterzuentwickeln und zu vervollständigen. Darüber hinaus hilft das BMC, die Ideenkonzepte zu dokumentieren und auszutesten sowie die zur Umsetzung notwendigen strategischen Komponenten zu entdecken und festzuhalten.

14.2.3 Ideen ansehen

Eine weitere Kernfunktion der Community ist „Ideen ansehen“ ([Abbildung 8](#)). Über diese Funktion können eingereichte Ideen aller Community-Mitglieder eingesehen werden. Zudem kann über „Ideen suchen“ die gesamte Datenbank nach relevanten Ideen durchsucht werden. Die Auswahl einer Idee ermöglicht es, in einer weiteren Maske die Ideeninhalte sowie die Beschreibung der Idee und die Zusammenfassung zu der Idee einzusehen, zu kommentieren und in sozialen Netzwerken zu teilen. Darüber hinaus ist es ebenfalls möglich, aktiv an der Bearbeitung einer Idee mitzuarbeiten. Dies ist jedoch von der Art – Einzel- oder Gemeinschaftsidee – abhängig. Eine aktive Bearbeitung einer Idee ist lediglich bei Gemeinschaftsideen möglich. Einzelideen können jedoch über die Kommentarfunktion diskutiert werden.

Abbildung 8: Funktion „Ideen ansehen“ (Eigene Darstellung).

14.2.4 Weitere Funktionen

Weitere Funktionen der Plattform sind das Profilmanagement, der Newsfeed und die Community. Im Profilmanagement verwaltet der Nutzer unterschiedliche biografische Daten – Ausbildung, Kontaktdaten, Berufserfahrung, Weiterbildung. Neben der Angabe dieser Daten kann der Nutzer mit anderen Mitgliedern kommunizieren („Mailfunktion“) sowie Freundschaftsanfragen und Freundeslisten aus der Community einsehen und bearbeiten. Eine weitere Funktion im Bereich des Profilmanagements beinhaltet die Übersicht über eigene Community-Aktionen sowie neue Informationen zu abonnierten Themenschwerpunkten. Der Newsfeed erlaubt es Mitgliedern, aktuelle Begebenheiten auf der Plattform zu verfolgen, diese zu kommentieren und in

sozialen Netzwerken zu verteilen. Unter Community-Funktionen können Mitglieder gesucht und kontaktiert sowie Mitgliederprofile eingesehen werden.

14.3 Schlussbetrachtung

Die in diesem Kapitel vorgestellte Open Service Innovation-Online Community für Cloud-Service-Ökosysteme stellt eine onlinebasierte Innovation-Community zur Ausarbeitung von Cloud-Services, im Speziellen von Geschäftsideen und darauf bezogenen Geschäftsmodellen dar. Sie beruht dabei auf den Grundprinzipien einer Online-Community und wird hauptsächlich um das Werkzeug des Business Model Canvas erweitert. Diese Innovation-Community wird darüber hinaus durch weitere Werkzeuge und Methoden u.a. des Collaboration Engineering unterstützt. Die in diesem Kapitel vorgestellte Plattform hilft in zunehmendem Maße, Kunden und andere externe Stakeholder eines Unternehmens aktiv in den internen Innovationsprozess einzubinden. Sie hilft somit, das Erfahrungswissen, welches zur Umsetzung von Innovationsprojekten zwingend erforderlich ist, auszutauschen und gezielt zur Entwicklung innovativer Cloud-Services einzusetzen.

Ziel dieser Kooperationen ist darüber hinaus auch die Identifikation konkreter Problemstellungen von Stakeholdern und insbesondere der Kunden von Cloud-Service-Anbietern. Ein solches Vorgehen soll dabei helfen, an neue Lösungsinformationen im Cloud-Computing-Bereich zu gelangen, um diese letztlich in neuen Lösungen umsetzen zu können. Dadurch können innovative Cloud-Services realisiert werden, die durch die reine Betrachtung zukünftiger Kundenbedürfnisse nicht möglich gewesen wären.

Insgesamt stellt diese Plattform auf der einen Seite den zentralen virtuellen Interaktions- und Kommunikationsraum für unterschiedliche Stakeholder des Cloud-Ökosystems dar und ermöglicht auf der anderen Seite die orts- und zeitunabhängige Erreichbarkeit der dezentral verteilten Teilnehmer sowie die Ausarbeitung innovativer Geschäftsideen. Die kontinuierliche Kommunikation mit dem Kunden sowie die Einbindung des Kunden in die Ideenbearbeitungsphase können zu einer engen Verbundenheit mit dem Unternehmen führen. Diese Verbundenheit kann letztlich in der Nutzung und

der Weiterempfehlung des durch den Kunden mitgestalteten Produktes resultieren.

14.4 Literaturverzeichnis

- Kunz, M.; Söllner, M.; Leimeister, J.M. (2014):** Successfully funded! – Welche Geschäftsmodelle machen crowdfinanzierte Cloud-Startups erfolgreich? Präsentiert auf der Multikonferenz Wirtschaftsinformatik, Paderborn, Deutschland 2014.
- Leimeister, J.M. (2012):** Dienstleistungsengineering und -management, Springer, Heidelberg, Deutschland 2012.
- Leimeister, J.M. (2014):** Collaboration Engineering – IT-gestützte Zusammenarbeitsprozesse systematisch entwickeln und durchführen, Springer Gabler, Wiesbaden, Deutschland 2014.
- Osterwalder, A.; Pigneur, Y. (2011):** Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer, Campus Verlag 2011.
- Reichwald, R.; Piller, F.T. (2006):** Interaktive Wertschöpfung, Gabler, Wiesbaden, Deutschland 2006.

15 Datenschutzkonformes Cloud-Computing

S. Jandt, S. Kroschwald, A. Roßnagel, M. Wicker

15.1 Cloud-Computing und Datenschutzrecht

Die Nutzung einer Cloud verursacht beachtliche Datenströme und Datenverarbeitungsprozesse. Daten werden vom Cloud-Nutzer in eine Cloud im Internet übertragen, dort gegebenenfalls gespeichert, vervielfältigt, verändert, zurückübertragen oder möglicherweise sogar an weitere Stellen weitergegeben. Beim Cloud-Computing werden größere Informationsvolumina an einer Stelle gebündelt, mit Daten anderer vermischt und nur virtuell getrennt verarbeitet.¹ Informationen werden an weitere Stellen verteilt und Datenströme über öffentliche Netze geleitet.²

Dabei können unterschiedliche Risiken für die Beteiligten und Betroffenen entstehen. Insbesondere der Verlust der Beherrschbarkeit von Daten durch datenschutzrechtlich Verantwortliche stellt für Cloud-Nutzer, Cloud-Anbieter und weitere Beteiligte der „cloud-basierten“ Datenverarbeitung ein Risiko dar.³ Übertragungswege und Speicherorte sind in der Cloud häufig intransparent.⁴ Ein für die Daten Verantwortlicher kann meist nicht nachvollziehen, wo und durch wen seine Daten verarbeitet werden. Unerlaubte Zugriffe und der Missbrauch personenbezogener Daten durch einen Cloud-Anbieter oder einen externen Dritten lassen sich häufig nicht erkennen.⁵ Die Vorgänge in der Cloud betreffen oft mehrere Rechtsordnungen, sind aber in keiner spezifisch geregelt. Es gibt kein spezifisches „Cloud-Computing-Gesetz“, aus dem sich etwa datenschutzrechtliche Anforderungen an das Cloud-Computing ergeben würden. Daher müssen auf Cloud-Computing allgemei-

1 Bedner 2013, 7.

2 Deussen/Strick/Peters (ISPRAT) 2010, 15 f.

3 Zu einem zumindest „gefühlten“ Kontrollverlust Weiss, in: Hilber 2014, 1A Rn. 21; s. auch Bedner 2013, 7.

4 Weiss, in: Hilber 2014, 1A Rn. 21.

5 Bedner 2013, 104.

ne, unspezifische Regelungen Anwendung finden, die keine adäquaten und zeitgemäßen Antworten auf die Lebensrealität des Cloud-Computing enthalten. Insbesondere bei internationalen Datenbewegungen kommt hinzu, dass sich das nationale Recht häufig nicht durchsetzen lässt oder mit abweichenden Regelungsvorstellungen zum Datenschutz in anderen Ländern kollidiert.⁶

Ziel des folgenden Kapitels ist es, datenschutzrechtliche Anforderungen an das Cloud-Computing darzustellen. Hierauf aufbauend sollen Handlungs- und Gestaltungsempfehlungen entwickelt werden, die den Nutzer bei einer rechtsverträglichen Cloud-Nutzung unterstützen sollen.

15.1.1 Gegenstand des Datenschutzrechts

Der Umgang mit Informationen berührt unterschiedliche Grundrechtspositionen und wird durch Gesetze in verschiedenen Rechtsbereichen reguliert – abhängig von der Art der Daten und dem Zweck der Informationsverarbeitung. Das Datenschutzrecht hat dabei den Schutz des Persönlichkeitsrechts des Einzelnen in der Ausprägung der informationellen Selbstbestimmung beim Umgang mit personenbezogenen Daten zum Ziel.⁷ Die datenschutzrechtlichen Regelungen setzen entsprechend dort an, wo ein Umgang mit Informationen erfolgt, die sich einer Person zuordnen lassen – also dort, wo ein Personenbezug der Informationen besteht oder hergestellt werden kann. Zweck des Bundesdatenschutzgesetzes ist es folglich, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG). Nur wenn Daten einen Personenbezug aufweisen, ist überhaupt die Anwendung des Datenschutzrechts eröffnet.⁸

Nach dem Urteil des Bundesverfassungsgerichts gewährt das Recht auf informationelle Selbstbestimmung dem Einzelnen das Recht, selbst über das Schicksal seiner Daten zu entscheiden.⁹ § 4 Abs. 1 BDSG¹⁰ und § 12 Abs. 1

6 Masing, NJW 2012, 2309 f.; zu unterschiedlichen Datenschutzkulturen etwa Hoeren, ZRP 2010, 252.

7 BVerfGE 65, 1, 42 ff.

8 Karg, ZD 2012, 255; Roßnagel, ZD 2013, 562 ff.; Buchner, in: Taeger/Gabel 2013, § 3 BDSG, Rn. 3.

9 BVerfGE 65, 1, 43.

TMG¹¹ bilden dieses Selbstbestimmungsrecht ab. Danach ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur zulässig, wenn eine Einwilligung der betroffenen Person vorliegt oder ein Gesetz den Datenumfang erlaubt. Ein Umgang mit personenbezogenen Daten ist somit nur zulässig, soweit derjenige, auf den sich Daten beziehen, selbstbestimmt in den Umgang anderer eben mit diesen personenbezogenen Daten eingewilligt oder der Gesetzgeber den Datenumgang zugelassen hat.¹²

15.1.2 Datenschutzrechtlich Beteiligte beim Cloud-Computing

Für das Datenschutzrecht sind zunächst der Cloud-Nutzer und der Cloud-Anbieter relevant. Zwischen diesen beiden Stellen kommt es meist zu einer Datenübertragung in die Cloud, die je nach Einzelfall vom Cloud-Nutzer oder vom Cloud-Anbieter initiiert wird. In zahlreichen Cloud-Konstellationen initiiert der Cloud-Nutzer die Übertragung personenbezogener Daten an einen Cloud-Anbieter. Vorstellbar ist beispielsweise die Nutzung eines cloud-basierten Speicherdienstes, in den der Cloud-Nutzer private Daten wie Fotos überträgt, um sie dort zu speichern. Die Datenübertragung kann aber auch vom Cloud-Anbieter initiiert werden. Möglich ist beispielsweise, dass eine cloud-basierte Software auf das Endgerät des Nutzers zugreift und dort Daten wie etwa Positionsdaten oder Vitaldaten des Nutzers erfasst. Die Erhebung von Daten des Cloud-Nutzers durch den Cloud-Anbieter ist datenschutzrechtlich reglementiert. Der Cloud-Anbieter wird sich in der Regel für diese Datenerhebung nach dem Datenschutzrecht verantworten müssen. Die Übertragung von Daten auf Initiative des Cloud-Nutzers ist demgegenüber für ihn zunächst solange datenschutzrechtlich irrelevant, wie ausschließlich Daten mit Bezug zum Cloud-Nutzer selbst übertragen werden.¹³ In diesem

10 Spindler/Nink, in: Spindler/Schuster 2011, § 4 BDSG, Rn. 4.

11 Hornung/Bizer, in: Roßnagel 2013, § 12 TMG, Rn. 35 ff.

12 Sokol, in: Simitis 2014, § 4 Rn. 3; Weichert, in: Däubler/Klebe/Wedde/Weichert 2014, § 4 BDSG, Rn. 1; Bergmann/Möhrle/Herb 2013, § 4 BDSG, Rn. 7; Gola/Schomerus 2012, § 4 Rn. 3; Hornung/Bizer, in: Roßnagel 2013, § 12 TMG, Rn. 35 ff.

13 Der Betroffene kann nach dem Zweck des Datenschutzrechts nicht die verantwortliche Stelle sein. Zumindest sind die Vorschriften des Bundesdatenschutz-

Fall übt der Cloud-Nutzer mit der Weitergabe „seiner“ Daten an den Cloud-Anbieter sein Recht auf informationelle Selbstbestimmung aus. Das Datenschutzrecht schränkt ihn hierbei nicht ein.

Das Datenschutzrecht wird jedoch dann relevant, wenn sich die vom Cloud-Nutzer übertragenen Daten nicht nur auf den Cloud-Nutzer, sondern auch oder ausschließlich auf weitere Betroffene beziehen. In Abgrenzung zum Cloud-Nutzer als Betroffener sollen diese „anderen Betroffenen“ im Folgenden als „betroffene Dritte“ bezeichnet werden. Betroffene Dritte haben häufig keine Kenntnis davon, dass ihre Daten über öffentliche Netze an einen Cloud-Anbieter weitergegeben werden.¹⁴ Vorstellbar ist beispielsweise, dass der Cloud-Nutzer als Unternehmer eine Kundendatenbank in der Cloud führt und hierzu Daten, die er bei seinen Kunden (beispielsweise aufgrund eines Vertragsverhältnisses oder einer „Kundenkarte“) erhoben hat, in der Cloud speichert.¹⁵ Überträgt der Cloud-Nutzer die Daten der betroffenen Dritten in die Cloud, liegt ein datenschutzrechtliches Dreiecksverhältnis vor.¹⁶ Es besteht aus einem vom Datenschutzrecht geschützten „betroffenen Dritten“, einem Cloud-Nutzer, der regelmäßig als eine für den Datenschutz verantwortliche Stelle einzuordnen ist, sowie einem Cloud-Anbieter als Datenempfänger.

15.1.3 *Datenschutzrecht im Projekt Value4Cloud*

Probleme rund um den Datenschutz sind, sowohl auf Seiten der Cloud-Anbieter, der Cloud-Nutzer als auch der betroffenen Dritten, als wesentlicher Hemmschuh der Verbreitung der Cloud-Nutzung in Deutschland identifiziert worden.¹⁷ Betroffene Dritte sorgen sich dabei um den Schutz ihrer personen-

gesetzes auf eine eigenverantwortliche Verarbeitung „eigener“ Daten nicht anzuwenden, Dammann, in: Simitis 2014, § 3 Rn. 226.

14 S. zur Transparenz als Voraussetzung zur Geltendmachung von Betroffenenrechten Roßnagel/Pfitzmann/Garstka 2001, 169.

15 Insbesondere für kleine und mittlere Unternehmen könnten beispielsweise „CRM“-Programme aus der Cloud attraktiv sein.

16 Zwischen einem Zwei-Personen-Verhältnis und einem Dreiecksverhältnis unterscheiden auch Hornung/Sädler, CR 2012, 642 ff.

17 S. statt vieler Art. 29-Datenschutzgruppe 2012, WP 196; International Working Group on Data Protection in Telecommunications 2012.

bezogenen Daten. Insbesondere stellt sich für sie die Frage, ob und wie sie davon erfahren, dass ihre Daten in Cloud-Diensten verarbeitet werden, um überhaupt Rechte aus dem Datenschutzrecht geltend machen zu können. Fraglich in diesem Zusammenhang ist außerdem, wie sich Betroffenenrechte auch in einem internationalen Cloud-Umfeld durchsetzen lassen. Cloud-Nutzer und Cloud-Anbieter stehen als potenziell verantwortliche Stelle vor der Herausforderung, Vorgaben des Datenschutzrechts einzuhalten und den Datenumgang verantworten zu können. Aufgrund der Besonderheiten des Cloud-Computing ergeben sich hier rechtliche wie praktische Schwierigkeiten, die einer Cloud-Nutzung entgegenstehen könnten oder die Beteiligten zumindest in Abwägungs- und Rechtsunsicherheiten bringen könnten. So ist beispielsweise die Erfüllung von datenschutzrechtlich geforderten einzelfallbasierten Interessenabwägungen in einem elektronischen Massengeschäft wie dem Cloud-Computing häufig schwer umsetzbar. Vergleichbares gilt für die Einhaltung von Kontroll- und Weisungspflichten. Ein im Projekt Value4 Cloud entwickelter Dienst soll die Beteiligten bei der Wahl und Nutzung von Cloud-Diensten unterstützen und dabei helfen, Daten in der Cloud möglichst rechtsverträglich,¹⁸ also unter größtmöglicher Berücksichtigung datenschutzrechtlicher Schutzziele, zu verarbeiten.

Ziel der folgenden Untersuchung muss in einem ersten Schritt die Darstellung und Systematisierung der gesetzlichen Anforderungen als Informationsgrundlage sein. Hieraus kann dann eine einzelfallbasierte, gegebenenfalls auch pauschalierte Bewertung der Risiken für die Beteiligten und daraufhin eine Entscheidungshilfe entstehen. Selbst wenn ein Beteiligter, etwa der Cloud-Anbieter, im Einzelfall gar nicht Adressat der gesetzlichen Anforderungen ist, kann er dennoch mit Hilfe von Gestaltungsvorschlägen darin unterstützt werden, eine datenschutzrechtsverträgliche Cloud anzubieten. Hierdurch kann der gegebenenfalls gesetzlich verpflichtete Cloud-Nutzer in der Erfüllung seiner Pflichten unterstützt und von (rechtlichen) Risiken entlastet werden. Dies kann dem Cloud-Anbieter wiederum eine entsprechende Positionierung im Cloud-Markt ermöglichen.

18 S. zum Begriff „Rechtsverträglichkeit“ Kapitel 2.

15.2 Datenschutzrechtliche Anforderungen für Cloud-Nutzer

Im Folgenden sollen datenschutzrechtliche Anforderungen dargestellt werden, bei deren Erfüllung der Cloud-Nutzer durch Value4Cloud-Dienste unterstützt werden kann. Dabei ist für den Cloud-Nutzer zunächst zu ermitteln, welches Datenschutzrecht für ihn anwendbar ist¹⁹ und für welche Fälle er überhaupt Adressat und Verpflichteter der jeweiligen Regelung ist.²⁰ Hierauf aufbauend sind die Zulässigkeitsvoraussetzungen für eine Cloud-Nutzung in Abhängigkeit der Merkmale des jeweiligen Cloud-Dienstes aus Sicht des Cloud-Nutzers zu prüfen.²¹ Anschließend sollen weitere Pflichten, die sich aus dem Umgang mit personenbezogenen Daten durch den Cloud-Nutzer ergeben, dargestellt werden.²²

15.2.1 *Welchen Datenschutznormen unterliegt der Cloud-Nutzer?*

15.2.1.1 Datenschutzrelevante Handlungen des Cloud-Nutzers

Dem eigentlichen Cloud-Computing geht häufig eine Generierung und lokale Verwendung von Daten durch den Cloud-Nutzer voraus. Möglich ist, dass der Cloud-Nutzer Daten auf seinem Rechner erfasst oder aber auch Daten bei betroffenen Dritten erhebt. Ist der Cloud-Nutzer beispielsweise Unternehmer, so ist vorstellbar, dass der Cloud-Nutzer personenbezogene Daten von Kunden (Kundendaten) wie etwa Verkaufs- oder Rechnungsdaten oder von Mitarbeitern (Mitarbeiterdaten) wie etwa Zeiterfassungs- oder Personalstammdaten erhebt. Diese erste Phase begründet zwar noch nicht zwingend eine Cloud-Nutzung, kann jedoch bereits datenschutzrechtlich relevant sein, da ein Umgang mit personenbezogenen Daten stattfindet. Da diese Phase keine Besonderheit des Cloud-Computing darstellt, soll sie hier nicht näher beleuchtet werden.

Erst in einer zweiten Phase findet eine Datenübertragung in eine Cloud statt. Hierzu überträgt der Cloud-Nutzer seine oder die Daten der betroffenen

19 S. Abschnitt 15.2.1.

20 S. Abschnitt 15.2.1.3.

21 S. Abschnitt 15.2.2.

22 S. Abschnitt 15.2.3.

Dritten in der Regel über das Internet an den Cloud-Anbieter. In der dritten Phase handelt sodann der Cloud-Nutzer, wenn überhaupt, nur indirekt. Hier werden die Daten des Cloud-Nutzers oder der betroffenen Dritten durch den Cloud-Anbieter in der Cloud gespeichert und, je nach Bereitstellungsmodell,²³ geändert, an weitere Stellen oder an den Cloud-Nutzer zurückübertragen und gegebenenfalls sogar wieder gelöscht. In allen drei Phasen findet ein Datenumgang, also eine Datenerhebung, -verarbeitung oder -nutzung im Sinne des § 1 Abs. 1 BDSG mit personenbezogenen Daten, statt.²⁴

15.2.1.2 Sachlicher Anwendungsbereich – personenbezogene Daten

Für den Cloud-Nutzer ist zunächst zu prüfen, ob er im Rahmen der genannten Phasen mit personenbezogenen Daten im Sinne des Datenschutzrechts umgeht und so das Datenschutzrecht überhaupt zur Anwendung kommt. Grundsätzlich gilt das Bundesdatenschutzgesetz gemäß § 1 Abs. 2 BDSG für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die dort genannten Stellen. Das Datenschutzrecht findet also nur für den Umgang mit personenbezogenen Daten Anwendung.²⁵

Personenbezogene Daten

Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“. Die Daten müssen sich auf eine bestimmte oder bestimmbare Person beziehen. Nur wenn eine Zuordnung der Daten zu einer Person möglich ist,²⁶ sind die weiteren Vorschriften im Datenschutzrecht anwendbar. Der Personenbezug eröffnet nicht nur die Anwendbarkeit des Datenschutzrechts und die daraus resultierenden Pflichten der verantwortlichen Stellen. Die Vermeidung eines Personenbezugs beim Umgang mit Daten ist

23 „Deployment Model“, Hennrich, CR 2011, 546.

24 Zu den unterschiedlichen Phasen beim Cloud-Computing und deren datenschutzrechtlicher Berücksichtigung s. auch Kroschwald, ZD 2013, 388.

25 Roßnagel, digma 2011, 160; Karg, ZD 2012, 255; Buchner, in: Taeger/Gabel 2013, § 3 BDSG, Rn. 3.

26 Roßnagel, digma 2011, 160 ff.

gleichzeitig ein allgemeines Ziel des Datenschutzes.²⁷ Nach § 3a BDSG sollen der Umgang mit personenbezogenen Daten sowie die Prozesse der Datenverarbeitung an dem Ziel ausgerichtet werden, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Hierzu sollen insbesondere Daten anonymisiert oder pseudonymisiert werden.²⁸

Daten sind nicht nur dann personenbezogen, wenn durch sie eine Person ‚bestimmt‘ ist, sondern bereits dann, wenn die Personen ‚bestimmbar‘ sind. Bestimmbare Personen sind zwar nicht wie bestimmte Personen anhand der vorliegenden Merkmale identifiziert. Eine Zuordnung der Daten ist aber mittels so genannten „Zusatzwissens“ möglich.²⁹ Neben den Daten müssen demnach weitere Kenntnisse vorliegen, unter deren Einsatz eine Zuordnung möglich ist.³⁰ Da das Zusatzwissen bei verantwortlichen Stellen unterschiedlich ist, kann es sein, dass die gleichen Daten für eine verantwortliche Stelle aufgrund ihres hohen Zusatzwissens einer Person zuzuordnen sind, für eine andere verantwortliche Stelle, die über kein derart hohes Zusatzwissen verfügen kann, aber nicht. Die Bestimmbarkeit ist somit relativ.³¹

Liegen von Anfang an keine Daten vor, die Personen zugeordnet werden können, werden die Ziele des Datenschutzrechts am besten gefördert und somit das Persönlichkeitsrecht der Einzelnen am weitesten geschützt.³² Ist sichergestellt, dass Informationen keinen Personenbezug ermöglichen, hält sich das Datenschutzrecht dann auch mit seiner Regulierung zurück – ein Umgang mit solchen Daten wird vom Datenschutzrecht nicht beschränkt. Soll der Datenschutz maximiert werden und der Datenumgang für den Cloud-Nutzer nicht vom Datenschutzrecht begrenzt werden, muss der Cloud-

27 S. hierzu näher Roßnagel 2011, 41 ff; Roßnagel/Pfitzmann/Garstka 2001, 37.

28 S. hierzu auch Scholz, in: Simitis 2014, § 3a Rn. 30 ff.; Roßnagel/Pfitzmann/Garstka 2001, 37.

29 Roßnagel, digma 2011, 161 ff.; Damann, in: Simitis 2014, § 3 Rn. 26; Roßnagel/Scholz, MMR 2000, 723.

30 S. Gola/Schomerus 2012, § 3 Rn. 10; Roßnagel/Scholz, MMR 2000, 723.

31 S. Roßnagel, digma 2011, 161 ff.; Plath/Schneider, in: Plath 2013, § 3 BDSG Rn. 15; Gola/Schomerus 2012, § 3 BDSG Rn. 10; Tinnefeld, in: Roßnagel 2003, 4.1 Rn. 22; Damann, in: Simitis 2014, § 3 Rn. 32; Kroschwald, ZD 2014, 76.

32 Roßnagel/Scholz, MMR 2000, 721.

Nutzer also sicherstellen, dass er möglichst keine personenbezogenen Daten in die Cloud überträgt.³³ Von Bedeutung ist folglich die Frage, wie der Cloud-Nutzer sicherstellen kann, beim Cloud-Computing mit möglichst wenig personenbezogenen Daten umzugehen.

Möglich ist, dass der Cloud-Nutzer den Daten, beispielsweise vor ihrer Weitergabe, den Personenbezug aktiv entzieht, indem er die Daten anonymisiert. Gemäß § 3 Abs. 6 BDSG ist Anonymisieren „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“ Durch den Prozess des Anonymisierens wird also sichergestellt, dass durch die Daten Personen nicht oder nur noch mit einem unverhältnismäßigen Aufwand bestimmbar sind. Ist das gewährleistet, gelten die Daten als nicht mehr personenbezogen.³⁴

Folgen von Verschlüsselungen

Nur weil eine bestimmte Stelle Daten zu einer Person zuordnen kann, bedeutet dies aufgrund des „relativen Personenbezugs“ nicht automatisch, dass das Datum für alle Stellen personenbezogen ist. Daher kann es sein, dass etwa ein Pseudonym für eine Stelle ein personenbezogenes Datum darstellt, weil sie über Zuordnungsinformationen verfügt, für alle anderen Stellen aber ein anonymes Datum ist, weil sie über diese Zusatzinformationen nicht verfügen.³⁵ Um die Daten zu anonymisieren, muss der Cloud-Nutzer den Personenbezug unumkehrbar entfernen.³⁶ Wenn andere Stellen, also der Cloud-Anbieter und weitere Empfänger, nicht oder nur unter unverhältnismäßigem Aufwand in der Lage sind, die Daten einer natürlichen Person zuzuordnen,

33 Kroschwald, ZD 2014, 75 f.

34 Weichert, in: Däubler/Klebe/Wedde/Weichert 2014, § 3 BDSG, Rn. 49; Roßnagel/Scholz, MMR 2000, 723; Kroschwald, ZD 2014, 75 f.

35 Roßnagel/Scholz, MMR 2000, 725; Scholz, in: Simitis 2014, § 3 BDSG Rn. 217a; Kroschwald, ZD 2014, 76.

36 Damann, in: Simitis 2014, § 3 Rn. 200.

dürfen Daten an diese Stelle weitergegeben werden, ohne dass dabei das Datenschutzrecht berücksichtigt werden muss. Eine Zuordnung der anonymen Daten durch andere Stellen darf folglich nach der allgemeinen Lebenserfahrung oder, in Ermangelung entsprechender Erfahrungswerte, auf Grundlage einer Risikoprognose auf dem Stand der Wissenschaft nicht zu erwarten sein.³⁷ Dabei sind auch zukünftige technische Entwicklungen, die gegebenenfalls eine Re-Identifikation ermöglichen, zu berücksichtigen.³⁸

Zur Entfernung des Personenbezugs könnte der Cloud-Nutzer die Daten gegebenenfalls kryptographisch verschlüsseln. Unter kryptographischer Verschlüsselung sind „mathematische Methoden und Techniken, die zum Schutz von Informationen gegen unbefugte Kenntnisnahme und/oder absichtliche Manipulation dienen können“, zu verstehen.³⁹ Bei einer Verschlüsselung wird eine unverschlüsselte Nachricht (Klartext) mit Hilfe eines Chiffreverfahrens (Verschlüsselungsverfahren), einem mathematischen Algorithmus, in eine verschlüsselte Nachricht (Chiffretext) umgewandelt. Zum Verschlüsseln und zum Entschlüsseln wird ein Chiffrierschlüssel benötigt.⁴⁰ Durch die Verschlüsselung wird der Klartext, also der Inhalt der Daten, so verändert, dass der Chiffretext nur noch eine scheinbar nicht zusammenhängende, sinnlose Zeichenfolge ergibt. Nur mithilfe eines Zusatzwissens, dem Schlüssel, kann der Chiffretext wieder lesbar gemacht werden. Während die Daten verschlüsselt sind, kann somit niemand den tatsächlichen Inhalt der Daten wahrnehmen, der nicht über den Schlüssel verfügt. Nur dem Inhaber der Zusatzinformation (also dem Schlüsselinhaber) gelingt es, durch Entschlüsselung den Inhalt der Daten zur Kenntnis zu nehmen.⁴¹

Für ein sicheres Cloud-Computing könnte der Cloud-Nutzer seine Daten bereits vor der Cloud-Nutzung verschlüsseln, dann verschlüsselt in die Cloud übertragen, dort verschlüsselt ablegen, bei Bedarf wieder verschlüsselt an sich zurück übertragen und dann bei sich wieder entschlüsseln.⁴² Während

37 Roßnagel/Scholz, MMR 2000, 724.

38 Weichert, in: Däubler/Klebe/Wedde/Weichert 2014, § 3 BDSG, Rn. 47.

39 BSI 2011, IT Grundschutz, M 3.23, 2330.

40 Kappes 2007, 18; BSI 2011, IT Grundschutz, M 3.23, 2331.

41 Hierzu Kroschwald, ZD 2014, 75 ff.

42 Kroschwald, ZD 2014, 75, 76 f.

des gesamten Cloud-Nutzungsvorgangs ist somit ausschließlich der Cloud-Nutzer im Besitz des erforderlichen Schlüssels. Der Vorgang während des Cloud-Computing ist dann vergleichbar mit einer Ende-zu-Ende-Verschlüsselung, bei der aber beide Enden der Kommunikation beim Cloud-Nutzer liegen, er also sowohl Absender als auch Empfänger ist.⁴³ In diesem Fall fehlen allen Stellen außer dem Schlüsselinhaber die Informationen, die zur Bestimmung einer natürlichen Person erforderlich sind. Für sie sind die Daten anonym.⁴⁴ Verschlüsselung kann im Ergebnis dazu führen, dass der Personenbezug für eine Stelle vorhanden ist, für andere jedoch nicht.⁴⁵

Ist nur der Cloud-Nutzer im Besitz des Schlüssels und kann somit nur er die Daten entschlüsseln, bliebe allen anderen Stellen allenfalls die Möglichkeit, den Schlüssel, etwa mittels einer „Brute-Force-Attacke“, zu hacken. Die Möglichkeit einer Bestimmung durch andere Stellen als dem Schlüsselinhaber hängt folglich von den einsetzbaren technischen Mitteln sowie der Sicherheit der Verschlüsselung ab. Solange die Wahrscheinlichkeit ausreichend gering ist, dass ein solcher Angriff in einer vertretbaren Zeit und mit

43 Schaar 2002, 286.

44 Kroschwald, ZD 2014, 75, 77 f.; in einigen Landesdatenschutzgesetzen ist das Verschlüsseln etwa als das „Verändern personenbezogener Daten derart, dass ohne Entschlüsselung die Kenntnisnahme des Inhaltes der Daten nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist“, ausdrücklich definiert. Der Wortlaut der Definition der Verschlüsselung ähnelt dabei der des Begriffs der Anonymisierung. Die Begriffe der Verschlüsselung und des Anonymisierens verlangen jeweils, dass die Informationen nicht oder nur mit unverhältnismäßig hohem Aufwand einer weiteren Verwendung zugeführt werden können. Die wirksame Verschlüsselung geht insofern sogar weiter als die Anonymisierung, indem sie die Kenntnisnahme für den gesamten Inhalt ausschließt und damit Informationen dem Betrachter vollständig verschleiert. Beim Anonymisieren genügt bereits das Erschweren der Bestimmung einer Person.

45 Art. 29-Datenschutzgruppe 2007, WP 136, 21; Stiemerling/Hartung, CR 2012, 62; Bizer, DuD 1997, 204; Damann, in: Simitis 2014, § 3 Rn. 36; Schröder/Haag, ZD 2011, 152; Heidrich/Wegener, MMR 2010, 806; Spies, MMR-Aktuell 2011, 313727; Kühling/Klar, NJW 2013, 3615; knapp: Tinnefeld, in: Roßnagel 2003, 4.1 Rn. 22.

vertretbarem Aufwand gelingt, gelten die verschlüsselten Daten weder als personenbezogen noch als personenbeziehbar.⁴⁶

Die Verschlüsselung beim Cloud-Computing ist jedoch nur eine eingeschränkte Lösungsmöglichkeit, um Daten sicher und rechtskonform in die Cloud zu geben. Der Cloud-Nutzer muss bei der Verschlüsselung berücksichtigen, dass die Verschlüsselung ausreichend sicher ist, sodass weder jetzt noch in absehbarer Zeit der Schlüssel durch Hacking gebrochen werden kann – der Personenbezug würde sonst aufleben.⁴⁷ Darüber hinaus muss der verschlüsselnde Cloud-Nutzer eine Prognose zukünftiger Möglichkeiten der Entschlüsselung anstellen und die Risiken eines Auflebens des Personenbezugs abschätzen. Problematisch ist dabei, dass der Cloud-Nutzer auf plötzliche Entwicklungen, beispielsweise einen „Sprung“ in der Technikentwicklung bei der Rechenleistung für das Hacking von Verschlüsselungen, nicht mehr reagieren kann. Sind die Daten einmal in einer Cloud, werden sie schon für das Backup kopiert und verschoben und sind an sich nicht mehr sicher zurückholbar. Eine Neuverschlüsselung für den Fall, dass sich eine Sicherheitslücke aufzeigt, ist später kaum mehr möglich. Lebt der Personenbezug aber unverhofft auf, ist auch der Umgang mit den Daten wieder umgehend datenschutzrechtlich reglementiert. Der Cloud-Nutzer könnte so unvorhersehbar gegen Datenschutzpflichten verstoßen.⁴⁸ Überdies können Daten bislang nur verschlüsselt gespeichert werden. Für eine Verarbeitung der Daten in der Cloud, etwa für Anwendungsprozesse im Rahmen des ‚Software as a Service‘, müsste dem Cloud-Anbieter der Schlüssel mitgeteilt oder die Verschlüsselung anbieterseitig vorgenommen werden. Da der Anbieter dann aber über die Zuordnungsfunktion verfügt, kann eine solche anbieterseitige Verschlüsselung die Daten nicht anonymisieren.⁴⁹ Mögliche Zugriffe durch den Anbieter oder mit seiner Unterstützung durch andere können so nicht ausgeschlossen werden. Die Verarbeitung von Daten in der Cloud ist insofern nur empfehlenswert, wenn der Cloud-Anbieter durch nachprüfbare,

46 Kroschwald, ZD 2014, 77; hierzu auch Art. 29-Datenschutzgruppe 2007, WP 136, 21; Stiemerling/Hartung, CR 2012, 62.

47 Dammann, in: Simitis 2014, § 3 Rn. 48; Kroschwald, ZD 2014, 75, 77 f.

48 Zum Backup-Problem Kroschwald, ZD 2014, 75, 79 f.

49 Kroschwald, in: Taeger 2013, 300 f.

technische und organisatorische Selbstbeschränkung einer nutzerseitigen Verschlüsselung vergleichbar sicherstellen kann, dass auch er und Dritte keinen Zugriff auf die Daten während der Verarbeitung haben.⁵⁰

15.2.1.3 Persönlicher Anwendungsbereich – der Cloud-Nutzer als verantwortliche Stelle

Die Vorschriften des Datenschutzrechts richten sich für die Frage der Zulässigkeit des Datenumgangs sowie der Verantwortlichkeit gegenüber Betroffenen in erster Linie an die verantwortliche Stelle. Sie ist in der Regel Normadressat der datenschutzrechtlichen Regelungen. Durch die Ermittlung einer verantwortlichen Stelle wird also bestimmt, wem primär die Pflicht zur Einhaltung der Datenschutzbestimmungen zugewiesen wird.⁵¹

Kollektive Verantwortung

Gemäß § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Nach der Definition in der Datenschutzrichtlinie ist eine Stelle nur verantwortliche Stelle, wenn sie über Zwecke und Mittel der Verarbeitung eine eigenständige Entscheidung treffen kann.

Im Rahmen des Cloud-Computing muss es nicht zwingend eine einzige verantwortliche Stelle geben. Möglich ist auch, dass mehrere Stellen, etwa der Cloud-Nutzer und der Cloud-Anbieter, während des Cloud-Computing eine kollektive Verantwortung tragen.⁵² So ist vorstellbar, dass für verschiedene Phasen und Handlungen im Rahmen des Cloud-Computing jeweils der einen oder der anderen Stelle die Möglichkeit zur Entscheidung über Mittel und Zwecke zusteht. Bei der Nutzung eines Cloud-basierten Speicherdienstes

50 S. hierzu Kroschwald, in: Taeger 2013, 301.

51 Gola/Schomerus 2012, § 13 BDSG, Rn. 48; Dammann, in: Simitis 2014, § 3 BDSG, Rn. 225; Roßnagel/Pfitzmann/Garstka 2001, 63.

52 Diese ist abzugrenzen vom „Joint Controllership“-Ansatz im Sinne einer gemeinsamen, kumulativen Verantwortung, die zu einer gesamtschuldnerischen Haftung führen würde, s. hierzu Art. 29-Datenschutzgruppe 2010, WP 169, 22 und 27.

ist der Cloud-Nutzer beispielsweise für die Übermittlung der Daten sowie die anschließende Speicherung verantwortlich. Greift der Cloud-Anbieter auf die gespeicherten Daten jedoch, beispielsweise zur Wartungszwecken, zu, ist dieser für diesen Teil des Datenumgangs verantwortlich. Die Verantwortung für die Cloud-Nutzung besteht dann kollektiv nebeneinander.⁵³

Verantwortungsverteilung bei der Auftragsdatenverarbeitung

Für den Fall einer so genannten „Auftragsdatenverarbeitung“ sieht das Datenschutzrecht demgegenüber eine einheitliche Festlegung der Verantwortung für den gesamten Prozess vor. Bei einer Auftragsdatenverarbeitung unterwirft sich ein Auftragnehmer zum Zweck der Erfüllung einer Datenverarbeitungs-Dienstleistung vollständig den Weisungen und der Kontrolle des Auftraggebers.⁵⁴ Für diese arbeitsteilige Datenverarbeitung ergibt sich eine neue Verantwortungszuweisung. Aus § 3 Abs. 8 Satz 3 BDSG i. V. m. § 4 Abs. 4 Nr. 3 BDSG folgt, dass der Auftraggeber einer Auftragsdatenverarbeitung für den gesamten Verarbeitungsprozess alleinige verantwortliche Stelle ist.⁵⁵

Gibt ein Cloud-Nutzer im Rahmen des Cloud-Computing Daten an einen Cloud-Anbieter weiter, erfolgt dies in der Regel ausschließlich mit dem Ziel, Ressourcen des Cloud-Anbieters zu nutzen. Der Cloud-Anbieter soll sich beim Datenumgang auf die Erbringung des Dienstes gegenüber dem Cloud-Nutzer beschränken und kein eigenständiges Interesse am Inhalt der Daten begründen. Zumindest hinsichtlich des Zwecks der Datenverarbeitung verfügt der Cloud-Anbieter über keine Entscheidungsbefugnisse oder -spielräume.⁵⁶ Der Cloud-Nutzer, als Auftraggeber und damit als allein verantwortliche Stelle, muss sicherstellen, dass der Cloud-Anbieter die von ihm in Auftrag gegebenen Datenverarbeitungsprozesse so durchführt, wie der

53 Zur kollektiven Verantwortung Jandt/Roßnagel, ZD 2011, 160; Kroschwald, ZD 2013, 388 ff.

54 Räther, DuD 2005, 465; zur „Vertragstheorie“ Gabel, in: Taeger/Gabel 2013, § 11 Rn. 15.

55 Gola/Schomerus 2012, § 3 BDSG Rn. 34, 50, 55; Petri, in: Simitis 2014, § 11 BDSG Rn. 43; Kroschwald, ZD 2013, 392.

56 Art. 29-Datenschutzgruppe 2010, WP 169, 16; Jandt/Roßnagel, ZD 2011, 160.

Cloud-Nutzer das verlangt. Nur so genügt der Cloud-Nutzer seiner Weisungs- und Kontrollpflicht.

15.2.1.4 Räumlicher Anwendungsbereich des Datenschutzrechts auf den Cloud-Nutzer

Ob das deutsche Datenschutzrecht auf die Cloud-Nutzung anwendbar ist, hängt nach § 1 Abs. 5 BDSG zunächst von der Verantwortlichkeit des Cloud-Nutzers und sodann von seinem Sitz oder seiner Niederlassung sowie gegebenenfalls dem Ort des Datenumgangs ab. Der Cloud-Nutzer als Auftraggeber ist für die gesamte Auftragsdatenverarbeitung sowie, im Falle einer Datenübermittlung, zumindest für die Datenübermittlung in die Cloud verantwortlich.⁵⁷ Für die hier untersuchten Fälle kann die Annahme zugrunde gelegt werden, dass der Cloud-Nutzer als verantwortliche Stelle seinen Sitz in Deutschland hat und die Cloud auch von dort aus nutzt. Der Cloud-Nutzer ist folglich in der hier näher untersuchten Ausprägung als kleines oder mittleres Unternehmen nicht im Sinne des § 1 Abs. 5 Satz 2 BDSG außerhalb der EU oder des EWR belegen. Darüber hinaus ist der Cloud-Nutzer in den hier untersuchten Konstellationen auch nicht im Sinne des § 1 Abs. 5 Satz 1 außerhalb Deutschlands in einem anderen EU- oder EWR-Mitgliedsstaat belegen oder erhebt, verarbeitet oder nutzt Daten in einer europäischen Niederlassung außerhalb Deutschlands. Für die Auftragsdatenverarbeitung oder die Datenübermittlung in eine Cloud durch einen inländischen Cloud-Nutzer ist folglich, unabhängig vom Ort des Cloud-Anbieters, das deutsche Datenschutzrecht anwendbar.⁵⁸

15.2.1.5 Abgrenzung der anwendbaren Datenschutzgesetze

Für die konkreten Anforderungen des Datenschutzrechts ist zu ermitteln, welche konkreten inländischen Datenschutznormen auf den Fall anzuwenden sind. Infrage kommen Regelungen des Telekommunikationsgesetzes, des Telemediengesetzes und des Bundesdatenschutzgesetzes.

⁵⁷ S. Abschnitt 15.2.1.3.

⁵⁸ Hierzu beispielsweise Jotzo 2014, 128 ff.

Unter das Telekommunikationsgesetz fallen Sachverhalte, die sich auf den Informationsaustausch zwischen zwei Kommunikationspartnern unter Verwendung von Telekommunikationsdiensten beziehen. Die Transportleistung in Form der Übertragung von Signalen steht bei den Leistungen eines Telekommunikationsdienstes im Vordergrund.⁵⁹ Sprachtelefon- und Internetzugangsdienste sind typische Beispiele für den Transport von Signalen über eine gewisse Entfernung.⁶⁰ Zwar ist die Übertragung der Daten in und aus der Cloud zweifelsohne ein Datentransportvorgang. Dieser ist jedoch, wie jede andere Nutzung im Rahmen des Internet, ein durch den Telekommunikationsanbieter erbrachter Dienst und vom Verhältnis zwischen Cloud-Nutzer und Cloud-Anbieter unabhängig. Die Transportleistungen über das öffentliche Netz an sich erfolgen weder durch den Cloud-Nutzer noch durch den Cloud-Anbieter, sondern durch die entsprechenden Zugangsanbieter und Netzbetreiber. Das Telekommunikationsgesetz findet auf das Cloud-Computing daher keine Anwendung.⁶¹

Das Telemediengesetz regelt Informations- und Kommunikationsdienste, die nicht reine Signalübertragung, also Telekommunikation, oder Rundfunk sind. Darunter fallen die meisten Online-Dienste wie Informationsseiten, Blogs und Portale.⁶² Auch Cloud-Anbieter werden regelmäßig als Telemedienanbieter eingeordnet.⁶³ Von den Regelungen des Telemediengesetzes ist jedoch nur die Datenerhebung, -verarbeitung oder Nutzung durch den Cloud-Nutzer geregelt. §§ 11 ff. TMG beschränken sich dabei auf den Umgang mit Bestands- und Nutzungsdaten des Cloud-Nutzers. Diese fallen beispielsweise an, wenn der Cloud-Nutzer einen Cloud-Dienst bucht oder sich zum Zwecke der Nutzung des Dienstes einloggt. Daten, die der Cloud-Nutzer in der Cloud speichert oder verarbeitet, sind demgegenüber als Inhaltsdaten gesetzlich

59 Schütz, in: Geppert/Schütz 2013, § 3 TKG, Rn. 79.

60 Piepenbrock, in: Geppert/Piepenbrock/Schütz/Schuster 2006, § 3 Rn. 45, 47 ff.

61 Boos/Kroschwald/Wicker, ZD 2013, 205 f.

62 Roßnagel, in: Roßnagel 2013, Einl. TMG, Rn. 25 ff.; Gitter, in: Roßnagel 2013, § 1 TMG, Rn. 29 ff.; Müller-Broich 2012, § 1 Rn. 6.

63 Boos/Kroschwald/Wicker, ZD 2013, 205 f.; a.A., jedoch ohne Trennung zwischen einzelnen delivery models, Heidrich/Wegener, MMR 2010, 805; Schuster/Reichl, CR 2010, 42; Opfermann, ZEuS 2012, 131.

nicht geregelt.⁶⁴ Die Erhebung, Verarbeitung und Nutzung von Daten durch den Cloud-Nutzer oder Cloud-Anbieter bestimmt sich ausschließlich nach dem gemäß § 1 Abs. 3 BDSG subsidiär anzuwendenden Bundesdatenschutzgesetz.⁶⁵

15.2.2 Unter welchen Voraussetzungen darf ein Cloud-Nutzer eine Cloud nutzen?

Der Cloud-Nutzer ist im Rahmen des Cloud-Computing zumindest für die Weitergabe von Daten im Rahmen einer Übermittlung oder aber als Auftraggeber einer Auftragsdatenverarbeitung für den gesamten Datenverarbeitungsprozess verantwortlich.

Der Umgang mit Daten betroffener Dritter beim Cloud-Computing, in erster Linie die Übermittlung dieser Daten an einen Cloud-Anbieter sowie das weitere Schicksal nach der Datenweitergabe, bedarf grundsätzlich einer gesetzlichen Erlaubnis oder der Einwilligung des Betroffenen.⁶⁶ Der Cloud-Nutzer als verantwortliche Stelle muss somit prüfen, ob er über eine Erlaubnis zur Übermittlung oder anderweitigen Weitergabe von Daten betroffener Dritter verfügt. Dort wo keine Einwilligungen vorliegen, diese nicht wirksam eingeholt werden können oder widerrufen wurden, kann eine Datenübermittlung in die Cloud für den Cloud-Nutzer nur zulässig sein, wenn eine Rechtsvorschrift dies ermöglicht. Eine Weitergabe von Daten könnte jedoch – ohne sie als Datenübermittlung nach § 3 Abs. 4 Nr. 3 BDSG zu qualifizieren – zulässig sein, wenn sie ausschließlich im Rahmen einer Auftragsdatenverarbeitung erfolgt und die Voraussetzungen des § 11 BDSG eingehalten werden.

64 Dix/Schaar, in: Roßnagel 2013, § 15 TMG, Rn. 21 ff.; Roßnagel, in: Roßnagel 2003, Kap. 7.9 Rn. 37; Enzmann/Roßnagel, CR 2002, 142; Spindler/Nink, in: Spindler/Schuster 2011, § 15 TMG, Rn. 3;

65 Boos/Kroschwald/Wicker, ZD 2013, 205 f.

66 Dies ist bei jedem Eingriff in Grundrechte erforderlich. Dieser Zusammenhang wird zu Unrecht auch „Verbot mit Erlaubnisvorbehalt“ genannt – so z.B. Sokol, in: Simitis 2014, § 4 Rn. 3; Weichert, in: Däubler/Klebe/Wedde/Weichert 2014, § 4 Rn. 1; Bergmann/Möhrle/Herb 2013, § 4 BDSG, Rn. 7; Gola/Schomerus 2012, § 4 Rn. 3. Der Datenumgang wird jedoch nicht – wie bei einem Verbot mit Erlaubnisvorbehalt – von einer behördlichen Erlaubnis abhängig gemacht.

15.2.2.1 Chancen und Risiken der Auftragsdatenverarbeitung

Bei der Auftragsdatenverarbeitung gibt der Cloud-Nutzer als Auftraggeber dem Cloud-Anbieter als Auftragnehmer den Auftrag, Daten in der Cloud zu speichern oder zu verarbeiten. Nach § 3 Abs. 8 Satz 3 BDSG sind Auftragnehmer bei einer Verarbeitung von Daten innerhalb der EU und des EWR keine Dritten. Nur die Bekanntgabe personenbezogener Daten an einen Dritten begründet jedoch gemäß § 3 Abs. 4 Nr. 3 lit. a BDSG eine Datenübermittlung. Nach herrschender Meinung ist die Weitergabe von Daten an einen Auftraggeber folglich keine Bekanntgabe an einen Dritten und damit keine erlaubnispflichtige Datenübermittlung. Zwischen dem Auftraggeber und dem Auftragnehmer einer Auftragsdatenverarbeitung können Daten vielmehr ohne weitere Zulässigkeitsbeschränkungen zirkulieren.⁶⁷

Neben der bereits festgestellten Verantwortung des Cloud-Nutzers ist dieser für eine Datenweitergabe im Rahmen der Auftragsdatenverarbeitung zur Einhaltung der Vorgaben nach § 11 BDSG verpflichtet. Die in § 11 Abs. 2 BDSG genannten Pflichten des Auftraggebers dienen dazu, dass dieser seinen Einfluss auf die Mittel und Zwecke der Datenverarbeitung und die Einhaltung seiner Weisungen auch faktisch sicherstellt und so seiner Rolle als verantwortliche Stelle gerecht wird. Der Auftraggeber hat sich dabei zu vergewissern, dass der Auftragnehmer ebenso sorgfältig mit den Daten umgeht, als würde er die Daten selbst verarbeiten. Der Cloud-Nutzer muss dabei, um den eben genannten Pflichten zu genügen, nicht nur den Cloud-Anbieter sorgfältig auswählen, vertraglich verpflichten und anweisen, sondern die Einhaltung der Maßnahmen nach § 11 Abs. 2 Satz 4 BDSG auch regelmäßig überprüfen.

Auswahl und Kontrolle

Grundsätzlich ist der Cloud-Nutzer bei der Wahl seines Cloud-Anbieters frei. Jedoch ist er gemäß § 11 Abs. 2 Satz 1 BDSG verpflichtet, den Cloud-Anbieter „unter besonderer Berücksichtigung der Eignung der von ihm getrof-

67 Gola/Schomerus 2012, § 3 Rn. 34, 50, 55; Petri, in: Simitis 2014, § 11 Rn. 43.

fenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen“.

Der eigentlichen Auswahl gehen eine Risikoprüfung sowie die Erstellung eines Anforderungskonzepts voraus. Hierbei sind die gesamten Umstände der Auftragsdatenverarbeitung, von den Betroffenen, den Datenarten und -mengen bis hin zu potenziellen Empfängern und dem Potenzial zum Datenmissbrauch, einzubeziehen.⁶⁸ Aus der hieraus gewonnenen Risikoeinschätzung sind die Anforderungen an einen potenziellen Cloud-Anbieter als Grundlage für die eigentliche Auswahl zu erarbeiten.⁶⁹

Im Mittelpunkt der Auswahl steht sodann die Eignungsprüfung des potenziellen Auftragnehmers.⁷⁰ Zu prüfen ist, ob der Datenverarbeiter in der Lage, aber auch willens ist, die beispielsweise im Rahmen eines Sicherheitskonzepts entwickelten Anforderungen an die technische und organisatorische Datensicherheit und Datensicherung zu erfüllen.⁷¹ Zu einer sorgfältigen Auswahl des Auftragnehmers gehört, dass der Auftraggeber sich nicht nur von den technischen und organisatorischen Maßnahmen,⁷² sondern auch von dem Auftragnehmer insgesamt ein umfassendes Bild verschafft.⁷³ Hierzu muss er beispielsweise die finanzielle und personelle Ausstattung,⁷⁴ die Erfahrung und gegebenenfalls Referenzen,⁷⁵ die Bestellung eines betrieblichen Datenschutzbeauftragten⁷⁶ sowie die Verpflichtung der Mitarbeiter auf das Datengeheimnis prüfen.

§ 11 Abs. 2 Satz 4 BDSG verpflichtet den Auftraggeber, „sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim

68 Gabel, in: Taeger/Gabel 2013, § 11 BDSG, Rn. 32.

69 Bergmann/Möhrle/Herb 2013, § 11 BDSG, Rn. 31; Gabel, in: Taeger/Gabel 2013, § 11 BDSG, Rn. 32; Petri, in: Simitis 2014, § 11, Rn. 58; Bergmann/Möhrle/Herb 2013, § 11 BDSG, Rn. 33.

70 Gabel, in: Taeger/Gabel 2013, § 11 BDSG, Rn. 32.

71 BT-Drs. 16/13657, 18; Gola/Schomerus 2012, § 11 Rn. 20; Hoeren, in: Roßnagel 2003, Kap. 4.6 Rn. 102.

72 BT-Drs. 16/13657, 18.

73 Gabel, in: Taeger/Gabel 2013, § 11 BDSG, Rn. 33.

74 Gabel, in: Taeger/Gabel 2013, § 11 BDSG, Rn. 33.

75 Wedde, in: Däubler/Klebe/Wedde/Weichert 2014, § 11 BDSG, Rn. 29.

76 Petri, in: Simitis 2014, § 11, Rn. 57.

Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen“. Der Auftraggeber muss demgemäß bereits vor Aufnahme der Auftragsdatenverarbeitung und auch während der Auftragsdatenverarbeitung regelmäßig den ausgewählten Auftragnehmer dahingehend überprüfen, ob dieser die Anforderungen und Weisungen des Auftragnehmers hinsichtlich der technischen und organisatorischen Maßnahmen einhält.⁷⁷ Die Entscheidung über den erforderlichen Prüfturnus muss dem Gefährdungspotenzial im konkreten Fall entsprechen.⁷⁸ Kontrollen müssen bei einem konkreten Anlass auch unmittelbar möglich sein.⁷⁹ Stellt der Auftraggeber während einer Kontrolle Verstöße gegen vereinbarte Maßnahmen oder Weisungen fest, so muss er beim Auftragnehmer auf deren Einhaltung hinwirken. Gegebenenfalls, beispielsweise bei Unwilligkeit des Auftragnehmers oder wiederholten Verstößen, muss er das Auftragsverhältnis auflösen.⁸⁰

Weder § 11 Abs. 2 Satz 2 BDSG noch § 11 Abs. 2 Satz 4 BDSG enthalten Anweisungen, wie die Auswahl beziehungsweise Kontrolle im konkreten Fall praktisch zu erfolgen hat. Dies führt zur Unsicherheit, ob zur Auswahl und Kontrolle eine höchstpersönliche Überprüfung der Verhältnisse beim Auftragnehmer erforderlich ist. Ebenso unklar ist, inwiefern der Auftraggeber hierbei eine Vor-Ort-Kontrolle durchführen muss.⁸¹ Eine aktive, höchstpersönliche Prüf- und Kontrollpflicht „vor Ort“ ergibt sich aus dem Gesetzestext nicht.⁸² Anders als beim klassischen Outsourcing stehen beim Cloud-Computing einem großen Auftragnehmer häufig zahlreiche, oftmals „kleine“ Auftraggeber in einem Massengeschäft gegenüber. Diese wollen standardisierte Dienste schnell, einfach und flexibel buchen.⁸³ Die Auswahl, Weisung und Kontrolle muss somit für den Auftraggeber ebenso schnell und

77 Eckhardt, DuD 2009, 589.

78 Gabel, in: Taeger/Gabel 2013, § 11 BDSG, Rn. 37; Petri, in: Simitis 2014, § 11 Rn. 58; Eckhardt, DuD 2009, 589.

79 Wedde, in: Däubler/Klebe/Wedde/Weichert 2014, § 11 Rn. 30; Petri, in: Simitis 2014, § 11 Rn. 61.

80 Wedde, in: Däubler/Klebe/Wedde/Weichert 2014, § 11 Rn. 26; Petri, in: Simitis 2014, § 11 Rn. 61.

81 S. auch Petri, in: Simitis 2014, § 11 Rn. 78.

82 Eckhardt, DuD 2013, 588, Eckhardt, DuD 2009, 589.

83 S. Schaffland/Wiltfang 2013, § 11 Rn. 9a.

einfach und für den Auftragnehmer standardisiert ablaufen. Bereits die sorgfältige Auswahl eines geeigneten Cloud-Anbieters als Auftragnehmer könnte den Cloud-Nutzer als Auftraggeber aufgrund fehlenden Fachwissens überfordern.⁸⁴ Auch die höchstpersönliche Kontrolle vor Ort ist für das Cloud-Computing praktisch nur schwer vorstellbar. Müsste jeder Cloud-Nutzer seinen Cloud-Anbieter regelmäßig vor Ort kontrollieren und hierzu die Geschäfts- und vor allem die Serverräume betreten und besichtigen, würde dies in einen regelrechten „Prüftourismus“⁸⁵ münden. Dieser kann weder von den Beteiligten gewollt sein, noch wäre er im Hinblick auf die Mobilität der Daten technisch umsetzbar.⁸⁶ Eine höchstpersönliche Vor-Ort-Kontrolle ist deshalb beim Cloud-Computing regelmäßig nicht möglich.

Denkbar ist allerdings die Überprüfung durch einen unabhängigen, externen Dritten. Das Prüfergebnis könnte in Form eines Zertifikats die Einhaltung bestimmter Anforderungen an die technisch-organisatorische Datensicherheit bestätigen und so die höchstpersönliche Vor-Ort-Kontrolle durch den Auftraggeber ersetzen.⁸⁷ Für den Cloud-Nutzer wird sich jedoch regelmäßig die Frage ergeben, welche Anforderungen an den Kontrolleur, an die Kontrolle sowie an den Inhalt und die Qualität des Zertifikats zu stellen sind und wie diese für ihn prüfbar sind. Vor allem interessiert ihn, inwiefern ihn das Zertifikat von der eigenen Kontrollpflicht gegenüber dem Auftragnehmer entlasten kann.⁸⁸ Eine Pflicht, den Kontrolleur und die Kontrolle ihrerseits intensiv zu prüfen, würde den eigentlichen Zweck der externalisierten Kontrolle durch Zertifizierungen ad absurdum führen. Der Cloud-Nutzer soll gerade auf das Verfahren und Ergebnis der Kontrolle vertrauen dürfen. In der Praxis sind jedoch insbesondere in der jüngeren Vergangenheit unzählige Zertifizierungsangebote entstanden, die nicht übergreifend standardisiert

84 Niemann/Hennrich CR 2010, 690.

85 Trusted Cloud, AG Rechtsrahmen 2012, 8.

86 Niemann/Hennrich CR 2010, 691; Trusted Cloud, AG Rechtsrahmen 2012, 8; Engels, K&R 2011, 550; Gaul/Köhler, BB 2011, 2232; Heidrich/Wegener, MMR 2011, 806.

87 Trusted Cloud, AG Rechtsrahmen 2012, 8 f.

88 Gola/Schomerus 2012, § 11 Rn. 21; Petri, in: Simitis 2014, §11 Rn. 59; Vander, K&R 2010, 295.

sind, sondern jeweils nach eigenen Kriterien und mit unterschiedlichen Qualitätsgraden zu einer Zertifizierung gelangen.⁸⁹ Auch sind die Vertrauenswürdigkeit und Transparenz über das Verfahren und die gestellten Anforderungen, die zu einer Zertifizierung führen, bei diesen Angeboten nicht immer gegeben.⁹⁰

Weitere Voraussetzungen aus § 11 BDSG

Über die Auswahl und Kontrolle hinaus muss der Cloud-Nutzer als Auftraggeber gemäß § 11 Abs. 2 und 3 BDSG die Auftragsdatenverarbeitung dokumentieren, unter Einhaltung eines vertraglichen Pflichtenkatalogs einen schriftlichen Auftragsdatenverarbeitungsvertrag abschließen und bei Bedarf dem Auftragnehmer Weisungen erteilen.

Nach § 11 Abs. 2 Satz 5 BDSG ist das Ergebnis der Kontrolle nach § 11 Abs. 2 Satz 4 BDSG zu dokumentieren. Viele Prozesse in der Cloud finden ausschließlich digital auf den Servern statt und sind mit menschlichen Sinnen nicht zu erfassen. Eine Dokumentation, auch während des Betriebs zu Dauerkontrollzwecken, ist deshalb häufig selbst nur automatisiert möglich. Eine technische Möglichkeit der automatisierten Dokumentation von Prozessen und Kontrollen besteht mit elektronisch signierten LOG-Dateien.⁹¹

§ 11 Abs. 2 Satz 2 BDSG verpflichtet den Auftraggeber ausdrücklich dazu, einen schriftlichen Auftrag zu erteilen. Ein Anforderungskatalog aus § 11 Abs. 2 Satz 2 Halbsatz 2 BDSG nennt Regelbeispiele, die als Mindestinhalt eines Vertrags zur Auftragsdatenverarbeitung eingefordert werden.⁹² Der Auftragsdatenverarbeitungsvertrag soll sicherstellen, dass dem Auftraggeber, hier dem Cloud-Nutzer, auch im Innenverhältnis die Rechte und Pflichten zur Weisung und Kontrolle zustehen. Als verantwortliche Stelle obliegt es eigentlich dem Cloud-Nutzer, den Auftrag zu erteilen und dem

89 Scholz, in: Simitis 2014, § 9a Rn. 10 f.

90 S. hierzu Scholz, in: Simitis 2014, § 9a Rn. 10 f.; zu Lösungsansätzen bei Trusted Cloud s. Trusted Cloud, AG Rechtsrahmen 2012.

91 S. hierzu ausführlich Kunz/Niehues/Waldmann, DuD 2013 523 f.; s. auch Selzer, DuD 2013, 218; Eckhardt, DuD 2013, 587; Petri, in: Simitis 2014, § 11 Rn. 64.

92 Petri, in: Simitis 2014, § 11 Rn. 65; Gabel, in: Taeger/Gabel 2013, § 11 BDSG, Rn. 41.

Cloud-Anbieter als Auftragnehmer die Klauseln vorzugeben. Häufig werden aber Vertragsklauseln zur Auftragsdatenverarbeitung durch den oft verhandlungsstärkeren Cloud-Anbieter regelrecht diktiert werden. Dem Cloud-Nutzer bleibt deshalb zumindest eine Prüfpflicht hinsichtlich der Einhaltung des gesetzlichen Klauselkatalogs sowie der eigenen Weisungen.

15.2.2.2 Keine geeigneten Erlaubnisvorschriften

Besteht zwischen dem Cloud-Nutzer als Auftraggeber und dem Cloud-Anbieter als Auftragnehmer kein wirksames Auftragsverhältnis oder werden die Vorgaben des § 11 BDSG nicht erfüllt, ist die Weitergabe von Daten durch den Cloud-Nutzer an den Cloud-Anbieter eine erlaubnisbedürftige Datenübermittlung. Fraglich ist, ob es für diese Datenübermittlung eine gesetzliche Erlaubnis gibt. Für den Datenumgang im Rahmen des Cloud-Computing gibt es bislang keine „cloudspezifischen“ Erlaubnistatbestände. Für die Frage nach der Zulässigkeit sind daher die allgemeinen datenschutzrechtlichen Erlaubnistatbestände des Bundesdatenschutzgesetzes⁹³ auf das Cloud-Computing anzuwenden.⁹⁴

§ 28 BDSG regelt den Datenumgang im nicht-öffentlichen Bereich, sofern dieser als Mittel zur Erfüllung eigener Geschäftszwecke erfolgt.⁹⁵ Übermittelt der Cloud-Nutzer Daten an einen Cloud-Anbieter, so geschieht dies regelmäßig als „Mittel zum Zweck“.⁹⁶ Der vom Cloud-Nutzer intendierte Zweck des Datenumgangs durch den Cloud-Anbieter liegt häufig darin, eine Cloud als internetbasierte Ressource zu nutzen. Der Datenumgang erfolgt somit zur Erfüllung eines Geschäftszwecks im Sinne des § 28 BDSG und nicht als eigenständiger Geschäftszweck, wie etwa bei den von § 29 BDSG erfassten Geschäftsbereichen. Für die Frage der Zulässigkeit einer Daten-

93 Für den öffentlichen Bereich aus §§ 14 bis 16 sowie § 20 Abs. 2 und 3 BDSG und für den nichtöffentlichen Bereich aus §§ 28 bis 32 BDSG.

94 Im Einzelfall könnte sich ein Erlaubnistatbestand für den Umgang mit Inhaltsdaten aus Spezialgesetzen ergeben, etwa bei der Nutzung einer Cloud durch bestimmte Behörden oder beim Umgang mit besonders sensiblen Daten, wie zum Beispiel die Datenhaltung in Krankenhäusern.

95 Wedde, in: Däubler/Klebe/Wedde/Weichert 2014, § 28 Rn. 1.

96 S. hierzu Simitis, in: Simitis 2014, § 28 Rn. 22; Bergmann/Möhrle/Herb 2013, § 28 BDSG, Rn. 14.

übermittlung durch den Cloud-Nutzer an den Cloud-Anbieter könnten insbesondere die Erlaubnistatbestände des § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG von Bedeutung sein.⁹⁷

Zulässigkeit aufgrund eines Schuldverhältnisses

Ein Datenumgang zur Erfüllung eigener Geschäftszwecke ist nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig, „wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist“. Für eine zulässige Datenerhebung, -verarbeitung und -nutzung muss nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG folglich ein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis bestehen. Daten, die auf Grundlage des § 28 Abs. 1 Satz 1 Nr. 1 BDSG verwendet werden, müssen sich auf die Begründung, Durchführung oder Erfüllung des diesem Zweck dienenden Vertrags oder anderweitigen Schuldverhältnisses beziehen. Hierzu zählen regelmäßig beispielsweise Basisdaten, wie Name und Anschrift des Vertragspartners, Zahlungsinformationen sowie Daten zu Inhalt und Gegenstand des Vertrages.⁹⁸

Damit § 28 Abs. 1 Satz 1 Nr. 1 BDSG als Erlaubnisvorschrift im Cloud-Kontext anwendbar ist, müsste der Cloud-Nutzer mit dem (datenschutzrechtlich) betroffenen Dritten in einem Schuldverhältnis stehen, das eine Datenübermittlung in die Cloud für die Vertragsabwicklung als erforderlich bedingt.⁹⁹ So müsste die Datenübermittlung zum Beispiel zwingend erforderlich sein, um einen Kaufvertrag zwischen dem Cloud-Nutzer und dem betroffenen Dritten zu erfüllen. Nur wenn die Begründung, Durchführung oder Beendigung dieses Schuldverhältnisses zwischen dem Cloud-Nutzer und dem betroffenen Dritten ohne diese Übermittlung objektiv nicht möglich wäre, würde die Vorschrift des § 28 Abs. 1 Satz 1 Nr. 1 BDSG eine Cloud-Nutzung rechtfertigen. Da allerdings Verträge zwischen dem Cloud-Nutzer

⁹⁷ Weichert, DuD 2010, 683.

⁹⁸ Simitis, in: Simitis 2014, § 28 Rn. 60; Wedde, in: Däubler/Klebe/Wedde/Weichert 2014, § 28 Rn. 18.

⁹⁹ S. hierzu Taeger, in: Taeger/Gabel 2013, § 28 BDSG, Rn. 47; Simitis, in: Simitis 2014, § 28 Rn. 69.

und einem betroffenen Dritten in der Regel auch ohne Datenübermittlung in die Cloud erfüllbar sind, erlaubt § 28 Abs. 1 Satz 1 Nr. 1 BDSG regelmäßig keine Übermittlung von Daten in die Cloud durch den Cloud-Nutzer.¹⁰⁰

Zulässigkeit nach Interessenabwägung

Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG könnte die Cloud-Nutzung zulässig sein, „soweit [diese] zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt“.

Die Cloud-Nutzung kann einem berechtigten Interesse des Cloud-Nutzers dienen – etwa der Möglichkeit, eigene Ressourcen und damit Kosten zu sparen.¹⁰¹ Allerdings müssen diese berechtigten Interessen des Cloud-Nutzers an einer Cloud-Nutzung mit den schutzwürdigen Interessen des Betroffenen im Einzelfall abgewogen werden. Entgegenstehende, schutzwürdige Interessen können sich in erster Linie aufgrund des Dateninhalts, des Datenumgangs und des Verarbeitungszwecks ergeben.¹⁰² Auch zusätzliche Risiken der Datensicherheit sowie ein möglicher Kontrollverlust, etwa im Hinblick auf zulässige oder unzulässige Zweckänderungen, oder eine erschwerte Durchsetzung von Betroffenenrechten können als schutzwürdige Interessen einer Datenübermittlung entgegenstehen.¹⁰³ In der Einzelfallabwägung sind so beispielsweise die Sensitivität der Daten, die in die Cloud übermittelt werden sollen, die Menge der Daten und die Anzahl der Betroffenen sowie ein möglicherweise geäußerter Wille und eine besondere Zweckbindung durch die Betroffenen zu berücksichtigen.¹⁰⁴ Von besonderer Schwere bei der Abwägung sind aber Risiken, die sich aus der Eigenart des Cloud-Computing

100 Weichert, DuD 2010, 683.

101 Hierzu statt vieler Bedner 2013, 85 f., Niemann/Paul, K&R 2009, 449.

102 Bergmann/Möhrle/Herb 2013, § 28 BDSG, Rn. 139

103 So etwa, wenn die Datenübermittlung zur Eingrenzung der „Entscheidungsfreiheit“ des Betroffenen führt, Simitis, in: Simitis 2014, § 28 Rn. 151.

104 Zur Wirkung eines entgegenstehenden Willens Ganßauge 1995, 170; Simitis, in: Simitis 2014, § 28 Rn. 143; Taeger, in: Taeger/Gabel 2013, § 28 BDSG, Rn. 63; s. auch Bergmann/Möhrle/Herb 2013, § 28 BDSG Rn. 258.

ergeben. Die schwer herstellbare Transparenz und Kontrollierbarkeit von Datenwegen und erstellten Kopien, potenzielle Empfänger und Speicherorte sowie die Möglichkeit unerlaubter Zugriffe sprechen zugunsten der Betroffeneninteressen. Auch die weltweite und damit grenzüberschreitende Datenverarbeitung, die fehlende Durchsetzbarkeit des deutschen Datenschutzrechts in anderen Rechtsregimen, die Gefahr staatlichen oder privaten Datenmissbrauchs sowie unerlaubte Zweckänderungen und die Verknüpfungsmöglichkeiten vor dem Hintergrund der Datenvielfalt und Datenmengen in Clouds sind im Einzelfall zur Abwägung zu bringen. Eine Abwägung kann an dieser Stelle nicht pauschal erfolgen, sondern hängt stets vom Einzelfall ab, insbesondere auch von dem gewählten Cloud-Anbieter und seiner technisch-organisatorischen Gestaltung des Cloud-Angebots. Vor dem Hintergrund der abstrakten Gefahren des Cloud-Computing dürften im Regelfall die schutzwürdigen Interessen des Betroffenen überwiegen. Dies führt in diesen Fällen zur Unzulässigkeit der Übermittlung personenbezogener Daten vom Cloud-Nutzer an den Cloud-Anbieter.¹⁰⁵

15.2.2.3 Anforderungen an Einwilligungslösungen

Eine weitere Möglichkeit für die datenschutzrechtliche Zulässigkeit der Cloud-Nutzung ist neben der Zulässigkeit aufgrund einer Rechtsvorschrift die Einwilligung des betroffenen Dritten.¹⁰⁶ Diese muss den Anforderungen des § 4 a BDSG genügen.

Eine wirksame Einwilligung hat bestimmte Voraussetzungen – insbesondere zu Form, Bestimmtheit, Informiertheit und Freiwilligkeit. Hintergrund hierfür ist der Bedarf an einer Art „Grundschutz“ der Betroffenen. Mit Vorgaben zur Einwilligung sollen Betroffene geschützt und somit eine echte Grundrechtsausübung im Sinne einer Selbstbestimmung erst ermöglicht wer-

105 Heidrich/Wegener, MMR 2010, 806; Niemann/Paul, K&R 2009, 449; wohl auch Weichert, DuD 2010, 683; Thalhofer, CCZ 2011, 223; Opfermann, ZEuS 2012, 138; s. auch Nägele/Jacobs, ZUM 2010, 290; Schulz, MMR 2010, 78; Niemann/Hennrich, CR 2010, 688; Reindl, in: Taeger/Wiebe 2009, 445 (jeweils zum Teil bezogen auf die Zulässigkeit im Rahmen einer Übermittlung in Drittländer); a.A. wohl Splittgerber/Rockstroh, BB 2011, 2182.

106 S. Kroschwald/Wicker, DSB-Newsletter zum 15. Datenschutzkongress 2014, 12.

den. Dies trifft insbesondere für Betroffene zu, die sich in einer im Vergleich zur verantwortlichen Stelle (sozial) schwächeren Position befinden.¹⁰⁷

Freiwilligkeit nach dem deutschen und europäischen Datenschutzverständnis bedeutet, dass der Betroffene ohne Zwang aufgrund einer freien Entscheidung in das Cloud-Computing einwilligt.¹⁰⁸ Ein faktischer Zwang kann beispielsweise vorliegen, wenn sich der Einwilligende in einem sozialen oder wirtschaftlichen Abhängigkeitsverhältnis befindet oder ein massives Ungleichgewicht zwischen den beiden Parteien herrscht.¹⁰⁹

Insbesondere bei der Begründung, Durchführung und Beendigung von Arbeitsverhältnissen kann ein faktischer Zwang bestehen.¹¹⁰ Will etwa ein Arbeitgeber Bewerberdaten in der Cloud speichern und verlangt hierfür eine Einwilligung durch den betroffenen Bewerber, wird man kaum davon ausgehen können, dass eine in diesem Kontext erteilte Einwilligung des Bewerbers freiwillig erfolgt ist.¹¹¹ Der Bewerber, der seine Chancen auf eine Einstellung nicht schmälern will, wird sich gezwungen sehen, mit der Cloud-Nutzung des potenziellen Arbeitgebers einverstanden zu sein. Auch im bestehenden Arbeitsverhältnis ist aus Sicht des Mitarbeiters bei vielen Cloud-Diensten nicht gesichert, ob er „eine echte Wahl hat und seine Einwilligung zu einem späteren Zeitpunkt widerrufen werden kann, ohne dass ihm daraus Nachteile erwachsen“.¹¹² Die Beteiligung des Betriebsrats ist hier zwar ein Indiz zugunsten der Freiwilligkeit, macht jedoch die Einwilligung nicht pauschal gültig. Liegt demgegenüber eine Betriebsvereinbarung vor, kann diese eine Einwilligung des Arbeitnehmers ersetzen.¹¹³ Auch bei Verbraucherverträgen

107 S. näher z.B. Kroschwald/Wicker, DSB-Newsletter zum 15. Datenschutzkongress 2014, 12.

108 Das Tatbestandselement der Freiwilligkeit findet sich auch in Art. 2 lit. H) DSRL, wonach eine Einwilligung eine Willensbekundung voraussetzt, die unter anderem „ohne Zwang“ erfolgt.

109 BGH, NJW 2008, 3056.

110 Kroschwald/Wicker, DSB-Newsletter zum 15. Datenschutzkongress 2014, 12.

111 S. Taeger, in: Taeger/Gabel 2013, § 4a BDSG, Rn. 69; Art. 29-Datenschutzgruppe 2001, WP 48, 27.

112 Art. 29 Datenschutzgruppe 2001, WP 48, 28.

113 Zur Wirkung und Reichweite von Betriebsvereinbarungen Sokol, in: Simitis 2014, § 4, Rn. 17 mit weiteren Nachweisen.

kann ein Ungleichgewicht zwischen den Vertragspartnern bestehen, das die Freiwilligkeit einer Einwilligung infrage stellen könnte.¹¹⁴

Freiwilligkeit beinhaltet überdies das Merkmal der Informiertheit.¹¹⁵ § 4a Abs. 1 Satz 2 BDSG verpflichtet die verantwortliche Stelle zu Information und Hinweisen gegenüber dem betroffenen Dritten, dessen Einwilligung zum Cloud-Computing begehrt wird. Der potenzielle Cloud-Nutzer ist „auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen“. Die dem Cloud-Computing immanente Intransparenz der Daten- und Verarbeitungswege kann eine solche Information an den Betroffenen allerdings erschweren. Kann der Cloud-Nutzer aus diesem Grund die geforderten Informationen nicht geben, sind Einwilligungen im Rahmen des Cloud-Computing nicht wirksam und können eine Datenübermittlung in die Cloud nicht legitimieren.¹¹⁶

Zudem muss die einwilligende Person für die Rechtswirksamkeit einer Einwilligung einsichtsfähig sein.¹¹⁷ Insbesondere bei Minderjährigen ist die Beurteilung der Einsichtsfähigkeit problematisch und für die verantwortliche Stelle, die sich als Cloud-Nutzer auf die Einwilligung berufen will, kaum durchführbar.¹¹⁸

Häufig werden Einwilligungserklärungen zusammen mit Allgemeinen Geschäftsbedingungen abgedruckt. Hierbei sind die Vorgaben der §§ 305 ff. BGB zu berücksichtigen. Maßgeblich ist dabei, dass die datenschutzrechtliche Einwilligung sich optisch als solche von den weiteren Bestimmungen erkennbar abhebt und als Opt-In-Klausel vorgesehen ist.¹¹⁹ Da jedoch gemäß

114 Zur Wirkung von „Verhandlungsungleichgewichten“ Taeger, in: Taeger/Gabel 2013, § 4a BDSG, Rn. 55.

115 Roßnagel/Pfitzmann/Garstka 2001, 91; Däubler, in: Däubler/Klebe/Wedde/Weichert 2014, § 4a Rn. 8.

116 Kroschwald/Wicker, DSB-Newsletter zum 15. Datenschutzkongress 2014, 13.

117 Taeger, in: Taeger/Gabel 2010, § 4a BDSG, Rn. 29; Simitis, in: Simitis 2014, § 4a Rn. 20 ff.

118 In diese Richtung auch Bergmann/Möhrle/Herb 2013, § 4a BDSG, Rn. 10.

119 Bergmann/Möhrle/Herb 2013, § 4a BDSG, Rn. 26c; LG München I, DuD 2006, 310.

§ 4a Abs. 1 Satz 2 BDSG die Einwilligung grundsätzlich schriftlich zu erfolgen hat, ist der Einsatz im digitalen Raum bis jetzt schwierig.¹²⁰

Cloud-Computing wird häufig vor dem Hintergrund des Flexibilitätsgewinns und der Ressourceneinsparung in Unternehmen etabliert. Eine Nutzung von Cloud-Diensten ist in der Regel nur sinnvoll, wenn gleichzeitig lokal vorgehaltene Ressourcen eingespart werden können. Ein Cloud-Nutzer, der eine ehemals lokal betriebene Ressource künftig aus der Cloud beziehen und Daten betroffener Dritter deshalb in der Cloud speichern oder verarbeiten möchte, wäre insofern auf die wirksame Einwilligung aller betroffenen Dritten angewiesen. Wird die Einwilligung auch nur von wenigen Betroffenen verweigert, nachträglich widerrufen oder wäre aufgrund der genannten Einschränkungen unwirksam, müsste der Cloud-Nutzer parallel eine lokale Datenhaltung und -verarbeitung betreiben, in der die Daten mit „fehlenden Einwilligungen“ gespeichert und verarbeitet werden. Die von der Cloud-Nutzung erhofften Kostenersparnisse und Flexibilitätsgewinne gingen dadurch jedoch wieder verloren.¹²¹

Im Ergebnis können Einwilligungen im Cloud-Computing zwar theoretisch eine Lösung darstellen, bieten praktisch jedoch zahlreiche Schwächen. Daher stellen sie regelmäßig keine Alternative für den potenziellen Cloud-Nutzer dar.¹²²

15.2.2.4 Zulässigkeit des internationalen Cloud-Computing

Beim internetbasierten Cloud-Computing überschreiten Daten häufig staatliche Grenzen. Daten werden nicht nur über internationale Telekommunikationswege geleitet, sondern möglicherweise auch an Stellen in anderen Ländern – etwa auf dortige Server – übertragen. Solange sich der Datenfluss auf die EU oder den EWR beschränkt, ist der grenzüberschreitende Datenumgang einer rein inländischen Übermittlung nach § 4b Abs. 1 BDSG gleichge-

120 Kritisch zum Schriftformerfordernis Taeger, in: Taeger/Gabel 2013, § 4a BDSG, Rn. 37.

121 Kroschwald/Wicker, DSB-Newsletter zum 15. Datenschutzkongress 2014, 13.

122 So insgesamt für Einwilligungen im Rahmen vertraglicher Datenverarbeitung Kamp/Rost, DuD 2013, 84; zum Cloud-Computing Kroschwald/Wicker, DSB-Newsletter zum 15. Datenschutzkongress 2014, 12 f.

stellt.¹²³ Auch eine Auftragsdatenverarbeitung ist innerhalb der EU und des EWR nach denselben Voraussetzungen möglich wie eine rein inländische Auftragsdatenverarbeitung.¹²⁴

Problematisch wird allerdings eine Cloud-Nutzung in einem Staat außerhalb der EU und des EWR. Für den Cloud-Nutzer stellt sich die Frage, ob er im Rahmen der Cloud-Nutzung personenbezogene Daten außerhalb der EU und des EWR übermitteln, für die Auftragsdatenverarbeitung weitergeben oder selbst mit diesen Daten umgehen darf. Vorstellbar ist beispielsweise, dass ein Cloud-Nutzer mit Sitz in Deutschland Daten an einen außereuropäischen Cloud-Anbieter übermittelt oder im Rahmen der Auftragsdatenverarbeitung Daten an einen Cloud-Anbieter mit Sitz im außereuropäischen Ausland (Datenexport in ein Drittland) weitergibt. Möglich ist auch, dass der betreffende Cloud-Anbieter seinen Sitz in Deutschland hat, jedoch die Daten selbst an eigene oder fremde ausländische Server außerhalb der EU und des EWR weitergibt.¹²⁵ § 4b und § 4c BDSG enthalten Regelungen zur Datenübermittlung an ausländische Stellen außerhalb der EU und des EWR.

Zwei-Stufen-Prüfung

§ 4b BDSG ist keine eigenständige Rechtsgrundlage für die Datenübermittlung in ein Drittland.¹²⁶ Die Anforderungen des § 4b Abs. 2 Satz 2 BDSG gelten im Falle eines Drittlandexports vielmehr zusätzlich zu den bereits für die Inlandsübermittlungen geltenden Zulässigkeitsvoraussetzungen. Der Cloud-Nutzer muss deshalb beim Datenexport in ein Drittland eine zweistu-

123 Gabel, in: Taeger/Gabel 2013, § 4b BDSG, Rn. 3; Däubler, in: Däubler/Klebe/Wedde/Weichert 2014, § 4b Rn. 2; Bergmann/Möhrle/Herb 2013, § 4b BDSG, Rn. 18; v. d. Busche, in: Plath 2013, § 4b Rn. 13.

124 So für das Cloud-Computing und im Ergebnis unbestritten, z.B. AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2011, 10.

125 Zu verschiedenen Konstellationen Düsseldorfischer Kreis, Beschluss vom 19./20.4.2007, Fallgruppen zur internationalen Auftragsdatenverarbeitung, Handreichung des Düsseldorfischen Kreises zur rechtlichen Bewertung.

126 V. d. Busche, in: Plath 2013, § 4b Rn. 4; Gabel, in: Taeger/Gabel 2013, § 4b BDSG, Rn. 9.

fige Prüfung vornehmen. Zuerst müssen die Voraussetzungen für eine Datenübermittlung – entsprechend einer Übermittlung im Inland – vorliegen. Der Datenexport in ein Drittland bedarf also im Sinne des § 4 Abs. 1 BDSG zwingend einer Einwilligung des Betroffenen oder einer gesetzlichen Erlaubnis, etwa nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Zusätzlich ist in einem zweiten Schritt zu prüfen, ob die Voraussetzungen eines Datenexports in ein Drittland nach §§ 4b und 4c BDSG gegeben sind.

Bereits auf der ersten Prüfstufe ist ein innereuropäisches Cloud-Computing regelmäßig nur auf Basis einer Auftragsdatenverarbeitung möglich.¹²⁷ Sollen die Daten jedoch in ein Drittland übermittelt werden, steht das Mittel der Auftragsdatenverarbeitung nur begrenzt zur Verfügung. Die „Privilegierung“ aus § 3 Abs. 8 Satz 3 BDSG, wonach eine Auftragsdatenverarbeitung keine Datenweitergabe an Dritte darstellt und somit keine erlaubnispflichtige Datenübermittlung ist, greift bei Datenübertragungen in Drittländer nicht. Werden Daten im Rahmen einer Auftragsdatenverarbeitung in ein Drittland weitergegeben, so führt dies zu einer erlaubnispflichtigen Datenübermittlung. Eine Interessensabwägung, wie sie nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu erfolgen hat, muss bei Auslandsberührung zusätzlich die damit zusammenhängenden besonderen Risiken für den Betroffenen berücksichtigen. Die Zulässigkeit des Cloud-Computing in Drittländern ist daher bereits auf dieser ersten Stufe regelmäßig fraglich.¹²⁸

Angemessenes Datenschutzniveau

Auf der zweiten Prüfstufe muss der Cloud-Nutzer für einen Datenexport die Vorgaben aus den §§ 4b und 4c BDSG berücksichtigen. Ein Datenexport in ein Drittland ist nach § 4b Abs. 2 Satz 2 BDSG nicht zulässig, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Für den Fall des § 4b BDSG ist das schutzwürdige Interesse zwar nicht näher definiert.¹²⁹ Ein Datenexport ist jedoch zumindest dann unzuläs-

127 S. Abschnitt 15.2.2.2.

128 So im Ergebnis auch Weichert, DuD 2010, 686.

129 Simitis, in: Simitis 2014, § 4b Rn. 45.

sig, wenn bei den Empfängerstellen ein angemessenes Datenschutzniveau nicht gewährleistet ist.¹³⁰

Gemäß Art. 25 Abs.1 DS-RL kommt es dabei aber nicht nur auf die einzelne Stelle, sondern vor allem auf den Empfängerstaat und dessen Datenschutzregime an. Grundsätzlich kann ein Datenschutzniveau eines Staates nur angemessen sein, wenn es auf Regeln beruht, die hinsichtlich Ziel, Intensität und Verbindlichkeit zumindest im Wesentlichen den Anforderungen der Datenschutzrichtlinie entsprechen. Weist ein potenzielles Empfängerland folglich kein dem europäischen Datenschutzregime vergleichbares Datenschutzniveau auf, ist ein Datenexport im Grundsatz nicht zulässig.¹³¹

Die Beurteilung, ob ein Drittland über ein angemessenes Datenschutzniveau verfügt, obliegt eigentlich dem Cloud-Nutzer als verantwortlicher Stelle. Meist kann jedoch der Cloud-Nutzer nicht selbst zuverlässig entscheiden, wie die Beurteilung ausfallen muss. Nach Art. 30 Abs. 1b DSRL kann deshalb die Europäische Kommission so genannte Angemessenheitsbeschlüsse fassen. Auf Grundlage des Art. 25 Abs. 6 in Verbindung mit Art. 31 Abs. 2 DSRL kann die Kommission verbindlich feststellen, dass in einem bestimmten Land ein angemessenes Datenschutzniveau gewährleistet ist. Da diese Beschlüsse für die Mitgliedsstaaten bindend sind, ist ein Datenexport, sofern er nach der ersten Prüfstufe zulässig ist, wohl auch nach § 4b BDSG möglich.¹³² Solche Angemessenheitsbeschlüsse sind bislang jedoch nur zu wenigen Staaten ergangen.¹³³ Die meisten für das Cloud-Com-

130 S. hierzu auch von d. Bussche, in: Plath 2013, § 4b BDSG, Rn. 21; Rätter/Seitz, MMR 2002, 426.

131 S. Simitis, in: Simitis 2014, § 4b Rn. 52; Gabel, in: Taeger/Gabel 2013, § 4b BDSG, Rn. 21; v. d. Busche, in: Plath 2013, § 4b Rn. 28.

132 S. von d. Bussche, in: Plath 2013, § 4b Rn. 29; Gabel, in: Taeger/Gabel 2013, § 4b BDSG, Rn. 22; Gola/Schomerus 2012, § 4b Rn. 14; „faktisch als verbindlich angesehen“, Däubler, in: Däubler/Klebe/Wedde/Weichert 2014, § 4b BDSG, Rn. 13; a. A. Simitis, in: Simitis 2014, § 4b Rn. 66, nach dem die ‚Angemessenheitsliste‘ der EU-Kommission zwar zur Kenntnis genommen, „aber nur als Anregung angesehen werden“ muss.

133 Angemessenheitsbeschlüsse der Kommission erfolgten bislang für die Datenschutzniveaus der Staaten Schweiz, Kanada, Argentinien, Guernsey, Isle of Man, Jersey, Färöer, Andorra, Israel, sowie neuerdings auch Uruguay und Neuseeland.

puting wesentlichen Drittländer, wie etwa die USA, verfügen über kein von der Kommission festgestelltes Datenschutzniveau. Zwar besteht mit den USA ein so genanntes Safe-Harbor-Abkommen, das auch über einen Angemessenheitsbeschluss verfügt. Allerdings werden hierdurch nur einzelne Datenexporte an so genannte Safe-Harbor-zertifizierte Unternehmen ermöglicht. Überdies ist Safe Harbor aufgrund von Durchsetzungsdefiziten, praktischer Schwächen und aktueller Geheimdienstkandale mittlerweile derart umstritten, dass auch von Datenschutzbehörden dessen Anwendung in Frage gestellt wird.¹³⁴

Ausnahmen

Bei einer Pauschalprüfung muss der Cloud-Nutzer also davon ausgehen, dass der Datenexport in ein Drittland im Rahmen des Cloud-Computing regelmäßig in einen Staat ohne angemessenes Schutzniveau erfolgt und daher nach § 4b BDSG nicht zulässig ist. Allerdings sind in § 4c BDSG Ausnahmen normiert, unter denen ein Datenexport in ein Drittland trotz eines nicht angemessenen Datenschutzniveaus dennoch möglich ist. Ausnahmetatbestände nach § 4c BDSG wurden vom Gesetzgeber geschaffen, um einen Datenexport in solchen Einzelfällen zu ermöglichen, in denen der Betroffene mit dem Datenexport einverstanden ist. Dies wird deutlich, wenn er ausdrücklich in diesen eingewilligt hat oder selbst ein Vertragsverhältnis im Drittland abgeschlossen hat oder durch ein solches dort begünstigt wird. Auch explizit genannte öffentliche Interessen, wie etwa die öffentliche Sicherheit, können einen Datenexport ermöglichen. Aus § 4c Abs. 1 BDSG ergibt sich aber keine Ausnahme für einen pauschalen Datenexport in die Cloud. Die dort genannten Ausnahmen werden nur selten gegeben sein.

Relevanter könnte der Ausnahmetatbestand des § 4c Abs. 2 BDSG sein. Dieser sieht die Möglichkeit vor, Daten in ein Drittland, das über kein aus-

¹³⁴ Art. 29 Datenschutzgruppe 2012, WP 196, S. 17; so im Ergebnis auch Düsseldorfischer Kreis 2010, S. 1; Rath/Rothe, K&R 2013, 629, sowie aktuell Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juli 2013, http://www.bfdi.bund.de/DE/Home/homepage_Kurzmeldungen2013/PMDerDSK_SafeHarbor.html; s. hierzu auch Götz, DuD 2013, 636; Roßnagel/Jandt/Richter, DuD 2014, 545 ff.

reichendes Datenschutzniveau verfügt, zu exportieren, soweit im Einzelfall¹³⁵ „ausreichende Garantien“ der verantwortlichen Stelle vorliegen, die das Persönlichkeitsrecht und die Ausübung der damit verbundenen Rechte gewährleisten.¹³⁶ In § 4c Abs. 2 Satz 1 Halbsatz 2 BDSG werden als Beispiele für mögliche Garantien ausdrücklich Vertragsklauseln und verbindliche Unternehmensregelungen genannt. Vertragsklauseln sind individuell vereinbarte Regelungen zwischen Datenexporteur und Datenimporteur (hier also Cloud-Nutzer und Cloud-Anbieter) zur Sicherstellung eines zwischenparteilichen Datenschutzniveaus. Verbindliche Unternehmensregelungen zum Datenschutz sollen demgegenüber den Datenexport innerhalb eines Konzerns zwischen einzelnen Konzernunternehmen ermöglichen.¹³⁷ Sowohl die Aushandlung individueller Verträge als auch verbindliche Unternehmensregelungen stoßen als Lösung im Rahmen des Cloud-Computings allerdings an praktische Grenzen. Die individuelle Vereinbarung ist, ähnlich wie die Weisung und Kontrolle bei der Auftragsdatenverarbeitung,¹³⁸ bei einem Massengeschäft wie dem Cloud-Computing nur schwer umsetzbar. Dabei stehen insbesondere häufige, kurzfristige und unerwartete Vertragsänderungen sowie Wechsel von Vertragspartnern und Unterauftragsverhältnissen individuell vereinbarten Cloud-Verträgen entgegen. Da Cloud-Computing vor allem bei kleinen und mittleren Unternehmen nicht in Konzernstrukturen erfolgt, Cloud-Nutzer und Cloud-Anbieter also nicht gemeinsame Konzernunternehmen sind, kommt auch die Nutzung von verbindlichen Unternehmensregelungen nicht in Betracht. Überdies erfordern sowohl Vertragsklauseln als auch Unternehmensregeln nach § 4c Abs. 2 BDSG eine Genehmigung der

135 „Einzelfallentscheidung“ Simitis, in: Simitis 2014, § 4c Rn. 29.

136 Simitis, in: Simitis 2014, § 4c Rn. 32; Däubler, in: Däubler/Klebe/Wedde/Weichert 2014, § 4c BDSG, Rn. 12, Bergmann/Möhrle/Herb 2013, § 4c BDSG, Rn. 21; v. d. Busche, in: Plath 2013, § 4c BDSG, Rn. 20.

137 Roßnagel/Jandt/Richter, DuD 2014, 550 f.; Gabel, in: Taeger/Gabel 2013, § 4c BDSG, Rn. 28; BT-Drs. 14/4329, 35 (für alle Teilnehmer unabhängig von ihrem Standort); Art. 29-Datenschutzgruppe 2009, WP 155, 2.

138 S. Abschnitt 15.2.2.1.

Aufsichtsbehörden im Einzelfall.¹³⁹ Der Cloud-Nutzer müsste folglich als verantwortliche Stelle mit jedem Cloud-Anbieter in einem unsicheren Drittland einen solchen Vertrag schließen und im Einzelnen von der Aufsichtsbehörde genehmigen lassen. Der durch Cloud-Computing mögliche Effizienzgewinn wird bei einem solchen schwierigen datenschutzrechtlichen Verfahren häufig wieder aufgezehrt.

Standardvertragsklauseln und Processor Binding Corporate Rules

Weiterhelfen könnten jedoch „Standardvertragsklauseln“ für die Auftragsdatenverarbeitung. Solche ermöglicht Art. 26 Abs. 4 DSRL. Dieser sieht vor, dass die EU-Kommission in einem Verfahren nach Art. 31 Abs. 2 DSRL solche Klauseln entwickeln darf. Diese sollen für einen Datenexport ausreichende „Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bieten“. Verwendet der Cloud-Nutzer für den Datenexport genau diese Klauseln, gilt die aufsichtsrechtliche Genehmigung als vorweggenommen. Bei der wortgenauen Übernahme der Klauseln ist somit keine Genehmigung der Aufsichtsbehörden mehr erforderlich.¹⁴⁰ Standardvertragsklauseln bieten für das Cloud-Computing folglich den Vorteil, dass sie nicht mehr individuell ausgehandelt und genehmigt werden müssen und somit für das Massengeschäft, mit kurzfristigen Zu- und Abbuchungen von Clouds und Wechseln der Anbieter, tauglich sind.

Die EU-Kommission hat inzwischen mehrere Standardvertragsklauselmuster verabschiedet. Für ein Outsourcing im Rahmen einer Auftragsdatenverarbeitung wurden die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländer am 5.2.2010 in

139 Gabel, in: Taeger/Gabel 2013, § 4c BDSG, Rn. 31; Däubler, in: Däubler/Klebe/Wedde/Weichert 2014, § 4c BDSG, Rn. 22 von d. Bussche, in: Plath 2013, § 4c BDSG, Rn. 42.

140 Däubler, in: Däubler/Klebe/Wedde/Weichert 2014, § 4c BDSG, Rn. 18c; Gola/Schomerus 2012, § 4c Rn. 12 und 14; Düsseldorfer Kreis 2007, Beschluss vom 19./20.4.2007, Fallgruppen zur internationalen Auftragsdatenverarbeitung – Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung, S. 5.

einer revidierten Fassung erlassen.¹⁴¹ Zum Schutz des Betroffenen enthalten sie beispielsweise Drittbegünstigtenklauseln, die einem betroffenen Dritten als Nicht-Vertragspartner dennoch Ansprüche zugestehen. Darüber hinaus enthalten die Klauseln weitere Regelungen zum Betroffenenenschutz sowie Vorgaben zur Aufsicht und dem Gerichtsstand, die die Durchsetzung des europäischen Datenschutzrechts unterstützen sollen.¹⁴²

Ausreichende Garantien wie die Standardvertragsklauseln können zwar den Datenexport in ein „unsicheres“ Drittland nach § 4c BDSG auf der zweiten Prüfstufe ermöglichen. Hiervon unberührt bleibt aber das Ergebnis der ersten Prüfstufe. Trotz der Standardvertragsklauseln zur Auftragsdatenverarbeitung lässt § 3 Abs. 8 Satz 3 BDSG einer Datenweitergabe nur als erlaubnispflichtige Datenübermittlung zu.¹⁴³ Auch, wenn der Cloud-Nutzer also einen Auftragsdatenverarbeitungsvertrag abschließt, die Vorgaben zu § 11 BDSG einhält und zusätzlich die Standardvertragsklauseln verwendet, muss ein Erlaubnistatbestand für die Datenübermittlung an den Cloud-Anbieter, etwa aus § 28 BDSG, einschlägig sein oder eine Einwilligung des Betroffenen vorliegen. Immerhin allerdings kann im Rahmen der Interessenabwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG der hohe Sicherheitsstandard einfließen, der sowohl durch den Auftragsdatenverarbeitungsvertrag, die Einhaltung der Vorgaben des § 11 BDSG als auch durch die Standardvertragsklauseln geschaffen wird.¹⁴⁴ Vor diesem Hintergrund sind Datenübermittlungen an Cloud-Anbieter in einem Drittland zum Teil zulässig. Dies gilt aber nicht pauschal. Vor allem, soweit besondere Arten personenbezogener Daten übermittelt werden, kann eine Rechtfertigung auf dieser Basis nicht erfolgen.¹⁴⁵

Die revidierten „Standardvertragsklauseln für Auftragsverarbeiter“ enthalten auch Regelungen zu Unterauftragsverhältnissen. Die Standardvertragsklauseln stehen demnach einer Unterbeauftragung durch den Auftrag-

141 K(2010) 593, ABl. EG Nr. L 39/5 v. 12.2.2010.

142 S. zu diesen z.B. Roßnagel/Jandt/Richter, DuD 2014, 549 f.

143 So z.B. auch Brennscheidt 2013, 80; Weber/Voigt, ZD 2011, 76.

144 So wohl auch Eckhardt, DuD 2013, 590.

145 Weber/Voigt, ZD 2011, 76; Scholz/Lutz, CR 2011, 426; a.A. dagegen Rittweger/Schmidl, DuD 2004, 620.

nehmer im Drittland nicht grundsätzlich entgegen. Wesentliche Bedingungen für eine Unterbeauftragung sind aber zum einen eine einzelfallbezogene Zustimmung des Auftraggebers. Zum anderen müssen Pflichten aus dem Ursprungsauftrag weitergegeben werden.¹⁴⁶ Problematisch ist jedoch der Fall eines EU/EWR-Auftragnehmers, der einen Unterauftragnehmer im Drittland beauftragen will. Hier wird der Auftragnehmer zum Datenexporteur, ist jedoch selbst keine verantwortliche Stelle. In diesem Fall sind die Standardvertragsklauseln – auch nicht analog – anwendbar. Der Cloud-Nutzer müsste in dieser Konstellation folglich einen Unterauftrag mit jedem Unterauftragnehmer, also beispielsweise jedem beteiligten Serveranbieter, schließen. Dies ist praktisch kaum realisierbar.¹⁴⁷

Dieses Problem der Unterbeauftragung könnte aber durch so genannte Processor Binding Corporate Rules (PBCR) eingedämmt werden. PBCR beruhen auf dem Gedanken, dass große Auftragnehmer, wie etwa häufig Cloud-Anbieter, Unterbeauftragungen innerhalb ihres eigenen Verbundes, ihrer Organisation oder ihres Konzerns vornehmen. Sind solche Cloud-Anbieter international aufgestellt, kommt es grenzüberschreitend zu „größeren Datenübermittlungen“ zwischen den Verbund-, Organisations- oder Konzernunternehmen.¹⁴⁸ Nach einer aktuellen Kommissionsentscheidung können PBCR als ausreichende Garantien genehmigt werden. PBCR können nach einmaliger Genehmigung damit wohl zumindest den Datentransfer zwischen Servern in der Cloud grenzüberschreitend ermöglichen. Voraussetzung ist allerdings, dass der Datenexporteur innerhalb des EWR oder Drittlands sitzt und alle Empfänger mit dem exportierenden Cloud-Anbieter in einem Konzernverbund sind.

15.2.3 Welche Betroffenenrechte muss der Cloud-Nutzer berücksichtigen?

Mit der Regulierung des Umgangs mit den personenbezogenen Daten ist dem Betroffenen noch nicht viel geholfen. Ob sich der Cloud-Nutzer als verantwortliche Stelle an seine Pflichten hält und der Betroffene tatsächlich geschützt ist, lässt sich für Betroffene und häufig auch für Aufsichtsbehörden

146 Moos, CR 2010, 283; Gabel, in: Taeger/Gabel 2013, § 4c BDSG, Rn. 26.

147 Düsseldorf Kreis, Beschluss vom 19./20. April 2007, 4 f. (Fall B).

148 Art. 29-Datenschutzgruppe 2013, WP 204, Kap. 1.3, 6.

als Außenstehende nicht beurteilen. Betroffenenrechte sollen daher für den Betroffenen Transparenz und Einflussmöglichkeiten gewährleisten.¹⁴⁹ Im Einzelnen lassen sich die Betroffenenrechte in Transparenzrechte (Benachrichtigung und Auskunft) sowie Gestaltungsrechte (Beschwerde, Widerspruch, Berichtigung, Löschung, Sperrung und Schadensersatzansprüche) unterteilen. Diese Rechte können nach § 6 Abs. 1 BDSG nicht durch Rechtsgeschäfte ausgeschlossen werden.

15.2.3.1 Transparenzpflichten gegenüber Betroffenen

Daten sind nach § 4 Abs. 2 Satz 1 BDSG grundsätzlich beim Betroffenen zu erheben. Zusätzlich hat ihn die erhebende Stelle nach § 4 Abs. 3 BDSG über die Speicherung, die Art der Daten, die Zweckbestimmung, die Identität der verantwortlichen Stelle sowie Empfängerkategorien zu unterrichten. Im Falle einer – ausnahmsweise zulässigen – anderweitigen Erhebung bei der erstmaligen Speicherung ohne die Kenntnis des Betroffenen trifft die verantwortliche Stelle nach § 33 Abs. 1 Satz 1 BDSG eine vergleichbare Benachrichtigungspflicht. Im Rahmen des Cloud-Computing ist ein Betroffener somit mindestens einmal über die Umstände der Cloud-Nutzung ohne weiteres Zutun seinerseits zu informieren: als betroffener Dritter etwa bei der Datenerhebung durch den Cloud-Nutzer oder der Speicherung durch den Cloud-Anbieter oder als betroffener Nutzer im Rahmen der Buchung eines Dienstes.

Der Betroffene hat überdies nach § 34 BDSG auf sein Anfordern hin Anspruch auf kostenlose und umfassende Auskunft über die konkret¹⁵⁰ gespeicherten Daten, Empfänger (auch Unterauftragnehmer wie Serveranbieter) und Zwecke. Dabei muss eine Auskunft auch erteilt werden, wenn der Betroffene nicht namentlich bekannt ist, und sogar, wenn gar keine Daten über ihn vorliegen (Negativauskunft).¹⁵¹ Benachrichtigung und Auskunft könnten gegebenenfalls automatisiert, etwa mit Unterstützung einer Online-Plattform, erfolgen.

149 Roßnagel/Pfitzmann/Garstka 2001, 169.

150 Dix, in: Simitis 2014, § 34 Rn. 6; Meents/Hinzpeter, in: Taeger/Gabel 2013, § 34 BDSG, Rn. 4.

151 Statt vieler Meents/Hinzpeter, in: Taeger/Gabel 2014, § 33 BDSG, Rn. 16.

15.2.3.2 Gestaltungsrechte der Betroffenen

Stellt ein Betroffener, beispielsweise aufgrund einer Benachrichtigung oder Auskunft fest, dass die verantwortliche Stelle seine Daten erhebt, verarbeitet oder nutzt, kann er mit mehreren Mitteln darauf reagieren. Er kann gegebenenfalls eine Beschwerde oder einen Widerspruch einlegen oder die Berichtigung, Löschung oder Sperrung der Daten fordern sowie unter Umständen Schadensersatzansprüche geltend machen.

Als verantwortliche Stelle muss der Cloud-Nutzer (oder gegebenenfalls auch der Cloud-Anbieter) damit rechnen, dass sich der betroffene Dritte nach § 38 Abs. 1 Satz 8 in Verbindung mit § 21 BDSG an die Aufsichtsbehörde wendet, wenn er sich in seinen Datenschutzrechten verletzt fühlt.¹⁵² Für die verantwortliche Stelle ist hierbei wichtig zu wissen, welche Aufsichtsbehörde sich an sie wenden könnte und wie ein Verfahren nach solch einer Beschwerde abläuft.¹⁵³

Wenn die gespeicherten Daten unrichtig sind, müssen sie nach § 35 Abs. 1 BDSG berichtigt werden. Geht der Cloud-Nutzer als verantwortliche Stelle mit Daten des Betroffenen um, ohne hierfür berechtigt zu sein, müssen die Daten nach § 35 Abs. 2 BDSG gelöscht werden. Eine Löschung muss auch erfolgen, wenn die Speicherung nicht mehr erforderlich ist, etwa weil ein Vertrag mit dem Betroffenen erfüllt ist und die Daten nicht mehr benötigt werden. Ebenso führt es zu einer Löschpflicht, wenn sich Umstände, die für eine Abwägung nach § 28 Abs. 1 Abs. 1 Nr. 2 BDSG relevant sind, ändern oder eine Einwilligung widerrufen wird.¹⁵⁴ Unter Umständen ist eine Löschung aber auch verboten, etwa weil Aufbewahrungspflichten (z.B. für Rechnungsunterlagen nach dem Handels- und Steuerrecht) bestehen. In diesen Fällen müssen die Daten, statt gelöscht, nach § 35 Abs. 3 und 4 BDSG gesperrt werden.¹⁵⁵ Gesperrt werden die Daten auch dann, wenn ihre Richtig-

152 S. hierzu auch Roßnagel/Pfitzmann/Garstka 2001, 175; Wedde, in: Roßnagel 2003, Kap. 4.4 Rn. 96.

153 S. hierzu Gola/Schomerus 2012, § 38 Rn. 16.

154 Meents/Hinzpeter, in: Taeger/Gabel 2013, § 35 BDSG, Rn. 20; Dix, in: Simitis 2014, § 35 Rn. 26.

155 Bergmann/Möhrle/Herb 2013, § 35 BDSG, Rn. 91.

keit bestritten wird, weder der Betroffene noch die verantwortliche Stelle aber die Richtigkeit beweisen können.

15.3 Datenschutzrechtliche Anforderungen für Cloud-Anbieter

Neben dem Cloud-Nutzer kann auch der Cloud-Anbieter datenschutzrechtlichen Anforderungen gegenüber stehen. In der Dreieckskonstellation (Cloud-Anbieter, Cloud-Nutzer und betroffener Dritter)¹⁵⁶ ist der Cloud-Anbieter zwar als Auftragnehmer häufig nicht verantwortliche Stelle. In diesem Fall treffen ihn jedoch zumindest die Pflichten für Auftragnehmer wie etwa die Einhaltung technischer und organisatorischer Maßnahmen.¹⁵⁷ Eine größere Verantwortlichkeit kommt dem Cloud-Anbieter nur zu, sofern er als verantwortliche Stelle selbst Daten erhebt, verarbeitet oder nutzt. Eigene datenschutzrechtliche Pflichten treffen den Cloud-Anbieter etwa in einer Zwei-Personenkonstellation, in der der Cloud-Nutzer selbst Betroffener ist oder wenn der Cloud-Anbieter die ihm zur Cloud-Speicherung oder -Verarbeitung übertragenen Daten zu eigenen Geschäftszwecken verwendet.

15.3.1 Persönlicher Anwendungsbereich – der Cloud-Anbieter als verantwortliche Stelle

Der Cloud-Anbieter kann nur verantwortliche Stelle sein, wenn er im Sinne des § 3 Abs. 7 BDSG in Verbindung mit Art. 2 lit. d) Satz 1 DSRL allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Sinne der kollektiven Verantwortlichkeit ist der Cloud-Anbieter beispielsweise dann für einen Datenumgang verantwortlich, wenn er – je nach Bereitstellungsmodell – eigenständig personenbezogene Daten beim Cloud-Nutzer erhebt. Er ist auch verantwortlich, wenn er mit personenbezogenen Daten etwa im Rahmen eines Wartungsprozesses zur Bereitstellung oder bei der Erbringung des Dienstes umgeht. Schließlich wird er zur verantwortlichen Stelle für sein

156 S. Abschnitt 15.1.2.

157 Zu den Pflichten des Auftragnehmers s. z.B. Dammann, in: Simitis 2014, § 3 Rn. 228.

Handeln, wenn er vom Cloud-Nutzer übermittelte oder im Rahmen der Auftragsdatenverarbeitung weitergegebene Daten zweckentfremdet.¹⁵⁸ Verarbeitet der Cloud-Anbieter demgegenüber die Daten im Rahmen eines Auftragsverhältnisses nach den Weisungen des Cloud-Nutzers, ist er für die gesamte Datenverarbeitung im Auftrag nicht verantwortlich.¹⁵⁹

15.3.2 Räumliche Anwendbarkeit des Datenschutzrechts auf den Cloud-Anbieter

Da der Cloud-Anbieter nicht selten seinen Sitz im Ausland hat, stellt sich die Frage, ob das deutsche Datenschutzrecht in diesem Fall auf ihn überhaupt anwendbar ist. Wird der Cloud-Anbieter nach dem zuvor Genannten nicht verantwortliche Stelle, so bestimmt sich das für die Auftragsdatenverarbeitung oder für die jeweilige Handlung geltende Datenschutzrecht nach dem Cloud-Nutzer.¹⁶⁰ Auf Handlungen, für die demgegenüber der Cloud-Anbieter verantwortlich ist, finden, sofern nicht der Sitz und Datenumgang auf Deutschland beschränkt ist, die Kollisionsregelungen des § 1 Abs. 5 BDSG Anwendung. Insbesondere, soweit zwischen dem Cloud-Nutzer und dem Cloud-Anbieter keine Auftragsdatenverarbeitung vorliegt, könnte auf die Tätigkeit des Cloud-Anbieters ein anderes als das deutsche Datenschutzrecht anwendbar sein.

Hat der im jeweiligen Fall verantwortliche Cloud-Anbieter seinen Sitz oder eine Niederlassung in einem anderen EU/EWR-Mitgliedsstaat, kommt das abgeschwächte Sitzlandprinzip¹⁶¹ nach § 1 Abs. 5 Satz 1 BDSG zur Anwendung. Soweit der verantwortliche Cloud-Anbieter Daten an einer Niederlassung in einem anderen Mitgliedstaat erhebt, verarbeitet oder nutzt, tritt das Bundesdatenschutzgesetz hinter dem Datenschutzrecht dieses Mitgliedsstaates zurück. Hierzu muss der Standort aber eine „echte“ Niederlassung sein.

158 Kroschwald, ZD 2013, 389 ff.

159 Petri, in: Simitis 2014, § 11 Rn. 1; Wedde, in: Roßnagel 2003, Kap. 4.3 Rn. 11.

160 S. Abschnitt 15.2.1.3.

161 Wuermeling 2000, 76; Damann, in: Simitis 2014, § 1 Rn. 199.

Server allein gelten dabei noch nicht als Niederlassung.¹⁶² Stehen nur Server in einem anderen Mitgliedsstaat, ist die für den Datenumgang maßgebliche Niederlassung oder der Sitz aber in Deutschland, findet das Bundesdatenschutzgesetz Anwendung. Häufig ist jedoch der Cloud-Anbieter nicht in Deutschland, sondern in einem anderen Mitgliedsstaat der EU oder des EWR ansässig. Die Anwendung des Bundesdatenschutzgesetzes beschränkt sich dann auf den (wohl eher seltenen Fall), dass der Cloud-Anbieter Daten in einer „echten“ Niederlassung in Deutschland verarbeitet. Bei großen Cloud-Anbietern, die ihren Sitz nicht in Deutschland haben, werden jedoch, wenn überhaupt, wohl nur Server in Deutschland genutzt, die den Niederlassungsbegriff nicht erfüllen.

Hat der Cloud-Anbieter seinen Sitz in einem Drittland und keine Niederlassung innerhalb der EU oder des EWR, kommt es für die Anwendbarkeit des Datenschutzrechts nach § 1 Abs. 5 Satz 2 BDSG in Verbindung mit Art. 4 Abs. 1 lit. c) DSRL nur noch darauf an, ob der Cloud-Anbieter als verantwortliche Stelle zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedsstaats belegen sind. Als Mittel können alle technischen Einrichtungen, die dafür ausgelegt sind oder überwiegend dafür verwendet werden, personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen, angesehen werden. Für einen Rückgriff auf Mittel muss die verantwortliche Stelle einen Datenumgang auf diesen Mitteln betreiben. Die Verantwortlichkeit für den jeweiligen Datenumgang im Sinne einer Entscheidung über Zwecke wird als „Mindestvoraussetzung“ für einen solchen Rückgriff angesehen.¹⁶³ Eine im Drittstaat ansässige Stelle hat demnach das deutsche Datenschutzrecht zu berücksichtigen, wenn sie für den Datenumgang durch das im Inland belegene Mittel verantwortliche Stelle ist.

Liegt zwischen dem Cloud-Nutzer und dem Cloud-Anbieter keine Auftragsdatenverarbeitung vor, ist der Cloud-Anbieter regelmäßig zumindest für bestimmte Phasen der Datenverarbeitung in der Cloud verantwortlich. Bei

162 Damann, in: Simitis 2014, § 1 Rn. 204; Artikel 29-Datenschutzgruppe 2010, WP 179, 15; Scheja 2006, 84; Jotzo, MMR 2009, 235; a. A. Ehmann/Helfrich 1999, Art. 4 Rn. 8.

163 Wuermeling 2000, 78.

Infrastrukturdiensten ist er in der Regel zumindest für die Datensicherheit, aber auch den Datenumgang im Rahmen der technischen Dienstbereitstellung und -erbringung verantwortlich.¹⁶⁴ Da sich hier der Datenumgang des Cloud-Anbieters aber auf Phasen nach der Übertragung in die Cloud beschränkt, greift der Cloud-Anbieter hierbei nur auf Mittel „in der Cloud“ zurück, das heißt beispielsweise auf eigene Server oder Server anderer Anbieter. Für die Bestimmung des anwendbaren Rechts kommt es demnach darauf an, ob der Cloud-Anbieter mit Sitz im Drittstaat die Daten auf Servern in Deutschland oder einem anderen EU- oder EWR-Mitgliedsstaat verarbeitet oder speichert.

Zum gleichen Ergebnis gelangt man, wenn der Cloud-Anbieter im Rahmen von Softwarediensten keine eigenständige Datenerhebung durchführt. Erhebt der Cloud-Anbieter demgegenüber Daten vom Cloud-Nutzer oder betroffenen Dritten, beispielsweise durch adaptive Dienste in Nutzergeräten wie Smartphones, greift der Cloud-Anbieter auf diese Nutzergeräte als Mittel im Sinne der Datenschutzrichtlinie zurück.¹⁶⁵ In diesem Fall kommt das Datenschutzrecht des europäischen Nutzers zur Anwendung. Das deutsche Datenschutzrecht oder das eines anderen Mitgliedsstaates der EU oder des EWR ist folglich nur dann nicht anwendbar, wenn der Cloud-Anbieter mit Sitz in einem Drittland in keiner europäischen Niederlassung eine Datenverarbeitung verantwortet und auf keine Geräte im Inland zugreift. Ein ausländisches Datenschutzrecht ist auf den Cloud-Anbieter folglich nur dann anwendbar, wenn der Cloud-Nutzer Daten selbstständig in eine Drittlands-Cloud übermittelt und keine Auftragsdatenverarbeitung stattfindet.

15.3.3 Zulässigkeit des verantworteten Datenumgangs

Findet das deutsche Datenschutzrecht auf den Cloud-Anbieter Anwendung und ist der Cloud-Anbieter für den jeweiligen Datenumgang auch verantwortlich, bedarf es nach § 4 Abs. 1 BDSG auch hier einer gesetzlichen Erlaubnis oder einer Einwilligung des Betroffenen.

¹⁶⁴ Kroschwald, ZD 2013, 390.

¹⁶⁵ Kroschwald, ZD 2013, 391.

Einwilligungen von betroffenen Dritten sind praktisch für das Cloud-Computing nicht relevant.¹⁶⁶ Sie finden allerdings dort Verwendung, wo der Cloud-Nutzer selbst Betroffener ist und direkt gegenüber dem Cloud-Anbieter einwilligt. Vorstellbar ist beispielsweise eine Einwilligung zur Verarbeitung der Daten zum Zwecke der Dienstbereitstellung und Erbringung. So könnte etwa der Cloud-Nutzer einwilligen, dass der Cloud-Anbieter auf Standortdaten in einem Smartphone zur cloud-basierten Navigation des Nutzers zugreift. Er könnte auch darin einwilligen, dass seine Daten zusätzlich noch zu anderen Zwecken genutzt werden – etwa die Verwendung der Standortdaten zum Zwecke der Werbung. Im Rahmen dieser Einwilligungen muss der Cloud-Anbieter jedoch die gesetzlichen Anforderungen an wirksame Einwilligungen einhalten.¹⁶⁷ Hierbei ist danach zu differenzieren, ob sich die Einwilligung auf den Umgang des Cloud-Anbieters mit Bestands- und Nutzungsdaten oder auf Inhaltsdaten bezieht. Der Umgang mit Bestands- und Nutzungsdaten ist im Telemediengesetz geregelt. Einwilligungen, die sich beispielsweise auf die Verwendung der Adresse des Cloud-Nutzers als Bestandsdatum zu Werbezwecken oder auf die Verwendung von Standortdaten als Nutzungsdaten einer Smartphone-App beziehen, unterliegen den Anforderungen des § 13 Abs. 2 TMG. Anders als die Einwilligung für Inhaltsdaten nach § 4a BDSG unterliegt die Einwilligung nach § 13 Abs. 2 TMG keinem Schriftformerfordernis.¹⁶⁸ In Fällen, in denen sich die Einwilligung demgegenüber auf den Umgang mit Inhaltsdaten bezieht, ist nach § 4a BDSG die Schriftform erforderlich. Eine solche Einwilligung ist beim Cloud-Computing wenig praktikabel.

Gesetzliche Erlaubnistatbestände für die Erhebung, Verarbeitung und Nutzung von Daten durch den Cloud-Anbieter ergeben sich zum einen aus § 11 ff. TMG für Bestands- und Nutzungsdaten des Cloud-Nutzers.¹⁶⁹ Der Umgang mit diesen Daten durch einen Online-Dienst ist aber nicht cloud-

166 S. Kroschwald/Wicker, DSB-Newsletter zum 15. Datenschutzkongress 2014, 12.

167 S. Abschnitt 15.2.2.3.

168 S. hierzu Jandt/Schaar/Schulz, in: Roßnagel 2013, § 13 TMG, Rn. 66 f.

169 S. hierzu Abschnitt 15.2.1.5.

spezifisch und soll hier nicht näher beleuchtet werden.¹⁷⁰ Hinsichtlich des Umgangs mit Inhaltsdaten kann sich ein Erlaubnistatbestand aus § 28 BDSG ergeben.¹⁷¹ § 28 Abs. 1 Satz 1 Nr. 1 BDSG kann den Umgang mit den Daten des Nutzers erlauben, wenn es für die Begründung, Durchführung oder Beendigung eines Schuldverhältnisses mit dem Cloud-Nutzer erforderlich ist. Zweckändernde Nutzungen lassen sich dagegen nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG in der Regel nicht rechtfertigen. Da eine zweckgebundene Übermittlung von Daten betroffener Dritter durch den Cloud-Nutzer in die Cloud nur in Einzelfällen zulässig ist,¹⁷² kann § 28 Abs. 2 BDSG in Verbindung mit § 28 Abs. 1 Satz 1 Nr. 2 BDSG erst Recht nicht die Zweckänderung von Daten des Nutzers oder betroffener Dritter durch den Cloud-Anbieter rechtfertigen.

15.3.4 Zulässigkeit des Datenumgangs als Auftragnehmer

Die Zulässigkeit des Datenumgangs mit Daten betroffener Dritter beschränkt sich für den Cloud-Anbieter folglich weitgehend auf die Datenverarbeitung im Auftrag. Da er in dieser Konstellation aber keine verantwortliche Stelle ist, treffen ihn – zumindest im Rahmen der „innereuropäischen Auftragsdatenverarbeitung“ – ausschließlich die Pflichten aus dem Auftragsdatenverarbeitungsvertrag, also die Weisungen des Auftraggebers und die Vorgaben aus § 11 Abs. 4 BDSG sowie die technischen und organisatorischen Maßnahmen nach § 9 BDSG in Verbindung mit Anlage zu § 9 BDSG. Im Hinblick auf eine häufig bestehende Informationsasymmetrie zwischen (oftmals großem) Cloud-Anbieter und (oftmals kleinem) Cloud-Nutzer wird außerdem die Hinweispflicht aus § 11 Abs. 3 Satz 2 BDSG relevant sein. Ist der Cloud-Anbieter der Ansicht, dass eine Weisung des Auftraggebers gegen das Datenschutzrecht verstößt, hat er nach dieser Vorschrift den Auftraggeber unverzüglich darauf hinzuweisen.

170 S. hierzu auch Boos/Kroschwald/Wicker, ZD 2013, 206 ff.

171 S. Abschnitt 15.2.2.2.

172 So das Ergebnis in Abschnitt 15.2.2.2.

15.3.5 Technische und organisatorische Maßnahmen

Neben den Anweisungen des Auftraggebers hat der Cloud-Anbieter, unabhängig davon, ob als verantwortliche Stelle oder weisungsgebundener Auftragnehmer, insbesondere die technisch-organisatorischen Maßnahmen nach § 9 BDSG in Verbindung mit Anlage zu § 9 BDSG zu beachten. Die Infrastruktur des Cloud-Anbieters, in erster Linie seine Server, müssen danach über eine angemessene Zutritts-, Zugangs- und Zugriffskontrolle verfügen. Ferner muss die Ein- und Weitergabe von Daten technisch und organisatorisch sicher gestaltet und vor unbefugtem Zugriff und Veränderung geschützt sein. Außerdem müssen Daten nach der so genannten Verfügbarkeitskontrolle vor zufälliger Zerstörung oder Verlust gesichert werden. Vor einer besonderen Herausforderung wird der Cloud-Anbieter schließlich durch das Trennungsgebot gestellt. In der Cloud sind Daten gerade nicht physisch, sondern nur virtuell getrennt.¹⁷³ Entsprechend hoch ist daher die Anforderung an die Sicherheit der virtuellen Maschinen hinsichtlich der Verhinderung einer unbeabsichtigten Datenvermischung.¹⁷⁴

Weitere organisatorische Pflichten ergeben sich überdies aus den allgemeinen Bestimmungen des Bundesdatenschutzgesetzes. So ist der Cloud-Anbieter als datenverarbeitende Stelle regelmäßig zur Meldung an die Aufsichtsbehörden nach § 4d und § 4e BDSG verpflichtet. Er muss nach § 4f und § 4g BDSG gegebenenfalls einen Datenschutzbeauftragten bestellen sowie nach § 5 BDSG seine Mitarbeiter auf das Datengeheimnis verpflichten. Soweit der Cloud-Dienst ein automatisiertes Abrufverfahren, wie etwa eine selbstständig datenerhebende Anwendung, betreibt, muss darüber hinaus ein Abrufkonzept erstellt werden.

15.4 Gestaltungsvorschläge für einen Dienst zur Nutzerunterstützung

Ziel des Projekts Value4Cloud ist es, Anbieter und Nutzer durch dienstbasierte Werkzeuge zu unterstützen. Hierzu gehört auch, rechtliche Anforde-

173 Zur „hypervisor-basierten“ Virtualisierung Bedner 2013, 42.

174 S. hierzu Bedner 2013, 161 ff.

rungen darzustellen. Den Anbietern und Nutzern sollen jedoch auch Hilfsmittel an die Hand gegeben werden, ihre Dienste und die Nutzung der Dienste rechtsvertraglich zu gestalten. Auf der vorangehenden Anforderungsanalyse aufbauend sollen im Folgenden Gestaltungsvorschläge für einen nutzer- und anbieterunterstützenden Dienst entwickelt werden.

15.4.1 Unterstützung bei der Anonymisierung, Pseudonymisierung und Datenverschlüsselung

Ziel der Unterstützung durch den Value4Cloud-Dienst muss es sein, dass der Cloud-Nutzer Hinweise und Hilfsmittel erhält, wie er nach Möglichkeit im Rahmen der Cloud-Nutzung nur anonyme, nicht-personenbezogene Daten in eine Cloud übertragen kann. Hierzu kann er entweder schon von Anfang an nur anonyme Daten erheben oder diese so früh wie möglich anonymisieren.

Eine Möglichkeit, den Personenbezug von Daten zumindest aus Sicht von Dritten nachträglich zu entfernen oder zumindest die Kenntnisnahme des Inhalts und einen möglichen Missbrauch zu verhindern, ist die Verschlüsselung. Ein Cloud-Nutzer, der nur Daten in der Cloud speichern will, kann informativ unterstützt werden, indem er auf die Möglichkeit einer exklusiv nutzerseitigen Verschlüsselung hingewiesen wird. Darüber hinaus sollte der Cloud-Nutzer über die Anforderung an die Verwendung sicherer Schlüssel sowie an die erforderliche Risikoprognose aufgeklärt werden. Der Nutzer kann auch hinsichtlich der Auswahl sicherer Verschlüsselungsmechanismen oder der eines geeigneten des Cloud-Anbieters unterstützt werden. Hierbei müssten insbesondere solche Anbieter empfohlen werden, die Datenwege und Sicherungskopien eingrenzen und sicher verfolgbar machen, sodass die Daten bei unerwarteten Entwicklungssprüngen möglichst weitgehend zurückgeholt werden können. Plant der Cloud-Nutzer eine Datenverarbeitung in der Cloud (also vor allem die Nutzung von Softwarediensten), sollte er auf die Gefahr der Preisgabe des Schlüssels hingewiesen werden. Zusätzlich könnte ihm nahegelegt werden, nur Dienste zu verwenden,

- die eine Verarbeitung von Daten so ermöglichen, dass der Cloud-Anbieter sich selbst und Dritte wirksam von der Kenntnisnahme des Umstands

einer Verarbeitung, des Inhalts der Daten sowie deren Begleitinformationen zu jedem Zeitpunkt sicher ausschließt,¹⁷⁵

- bei denen die Selbstrestriktion und die technischen und organisatorischen Maßnahmen des Cloud-Anbieters nachweislich eingehalten werden und die Einhaltung durch eine neutrale Stelle, möglichst in einem staatlichen Verfahren, kontrolliert wird.

15.4.2 Unterstützung bei der Ermittlung des datenschutzrechtlichen Verantwortungsbereichs der Beteiligten

Liegt eine Auftragsdatenverarbeitung vor, erstreckt sich die Verantwortung des Cloud-Nutzers als Auftraggeber auf den gesamten Verarbeitungsprozess. Außerhalb einer Auftragsdatenverarbeitung ist der Cloud-Nutzer im Rahmen der kollektiven Verantwortung zumindest für die Übermittlung von Daten oder die Eröffnung eines Zugangs für einen Cloud-Anbieter die verantwortliche Stelle. Für seinen Umgang mit den personenbezogenen Daten muss er die Zulässigkeitsvoraussetzungen berücksichtigen.¹⁷⁶ Hierbei könnte der Cloud-Nutzer zunächst bei der Identifikation seines Verantwortungsspektrums unterstützt werden. Zu diesem Zweck müssten die Umstände des Einzelfalls mit den Abgrenzungskriterien der Verantwortlichkeit¹⁷⁷ abgeglichen werden. Geprüft werden könnte beispielsweise, ob ein potenzieller Cloud-Anbieter als Auftragnehmer eine Auftragsdatenverarbeitung akzeptieren und sich der Zweckfestlegung und den Weisungs- und Kontrollpflichten des Cloud-Nutzers unterwerfen würde. Ebenso ist relevant, ob der Cloud-Nutzer bei einem Cloud-Nutzungsverhältnis über Zwecke und Mittel der Datenverarbeitung bestimmen und die Anforderungen des § 11 BDSG einhalten könnte. Hierdurch lässt sich bestimmen, ob der Cloud-Nutzer Daten im Rahmen einer Auftragsdatenverarbeitung weitergeben kann oder ob er für eine Datenübermittlung einer gesetzlichen Erlaubnis oder einer Einwilligung des Betroffenen bedarf.

175 Beispielhaft sei hier die Versiegelung von Daten im Sinne des Konzepts des Trusted Cloud-Projekts „Sealed Cloud“ genannt, hierzu Jäger/Riecken 2014, 2 ff.; Kroschwald, in: Taeger 2013, 301.

176 Kroschwald, ZD 2013, 390 f.

177 S. hierzu Abschnitt 15.2.1.3.

15.4.3 Unterstützung bei der Feststellung des anwendbaren Datenschutzrechts

Eine weitere Unterstützungsleistung sollte darin bestehen, dem Cloud-Nutzer zu helfen, die für ihn einschlägigen Datenschutznormen zu finden. Hierzu müssten eventuell weitere konkrete Umstände des Datenumgangs ebenso abgefragt werden wie wesentliche Angaben zum Cloud-Dienst, zum Cloud-Nutzer und zur Art der Daten. Hieraus könnte dann ermittelt werden, ob für den Datenumgang durch den Cloud-Nutzer nur das Bundesdatenschutzgesetz oder vorrangig weitere bereichsspezifische Datenschutzgesetze zu beachten sind. Zusätzlich könnte der Nutzer darauf hingewiesen werden, dass bei der Nutzung eines Cloud-Online-Dienstes wie bei jedem Online-Dienst Bestands- und Nutzungsdaten anfallen, die vom Cloud-Anbieter verarbeitet werden könnten. Gegenüber Cloud-Nutzern könnten auf Basis solcher Abfragen Hinweise zu Anbietern geliefert werden, die beim Umgang mit diesen Daten den Anforderungen der §§ 11 ff. TMG unterliegen. Es könnte auch vor solchen Anbietern gewarnt werden, die ohne Beachtung des Telemediengesetzes Bestands- und Nutzungsdaten erheben, verarbeiten oder nutzen – etwa bestimmte ausländische Angebote. Auch könnten Angebote hervorgehoben werden, die eine besondere Transparenz, Seriosität oder Selbstbeschränkung, die möglicherweise sogar über die Anforderungen des Telemediengesetzes hinausgeht, bieten und insofern als besonders datenschutzfreundlich und vertrauenswürdig angesehen werden können.

15.4.4 Unterstützung bei der Bestimmung der Zulässigkeit der Cloud-Nutzung

Darüber hinaus muss der Dienst den Nutzer auf die Anforderungen einer gesetzlichen Erlaubnis oder einer Einwilligung hinweisen. Er könnte anhand der Angaben des Cloud-Nutzers prüfen, inwieweit die Einholung von Einwilligungen realistisch ist und welche Voraussetzungen für ihre Wirksamkeit gegeben sein müssen. Auch kann er anhand der Angaben im Einzelfall grob prüfen, ob ein Zulässigkeitstatbestand vorliegen könnte und ob alternativ auch die Möglichkeit einer Auftragsdatenverarbeitung besteht. Hieraus kann er Empfehlungen zu einzelnen bestehenden Cloud-Angeboten ableiten.

Im Einzelfall kann die Nutzung eines Cloud-Dienstes für den Cloud-Nutzer aufgrund der Abwägung im Rahmen der Erlaubnistatbestände zulässig sein. Der Dienst sollte den Cloud-Nutzer allgemein auf die Schwierigkeit einer Einzelfallabwägung und die geringen Erfolgsaussichten im Rahmen der Interessenabwägung aus Sicht des Cloud-Nutzers hinweisen. Vor allem aber könnte er den Cloud-Nutzer bei der Abwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG unterstützen, indem er aus den ihm bekannten Informationen über die geplante Cloud-Nutzung Argumente zugunsten der Nutzer- und der Betroffeneninteressen ableitet und gewichtet. Diese Interessen sollte er dann den verfügbaren Cloud-Angeboten unter Berücksichtigung oben genannter Kriterien¹⁷⁸ gegenüberstellen. Im Einzelnen könnte er es beispielsweise positiv oder negativ hervorheben, wenn

- ein Cloud-Nutzer offenbar nur wenig sensitive Daten in die Cloud einbringen will oder andererseits etwa plant, auch besondere Arten personenbezogener Daten zu übermitteln,
- ein Cloud-Nutzer in seiner Person einem besonderen Vertrauensverhältnis und einer besonderen Verschwiegenheitspflicht unterliegt, sodass die Daten in Verbindung zu dieser Person das Persönlichkeitsrecht im besonderen Maße betreffen,
- ein Cloud-Nutzer nur wenige oder nur Daten aus dem privaten Umfeld von wenigen Betroffenen speichern möchte oder andererseits erhebliche Datenmengen von vielen Betroffenen zu Geschäftszwecken in die Cloud einbringt,
- ein Cloud-Nutzer durch technisch-organisatorische Maßnahmen die Kenntniserlangung des Dateninhalts durch den Cloud-Anbieter und Dritte wirksam ausschließt – beispielsweise indem er die Daten nutzerseitig verschlüsselt,
- ein Cloud-Dienst ausschließlich die Verarbeitung innerhalb der Europäischen Union und damit im Geltungsbereich des europäischen Datenschutzrechts garantiert oder aber andererseits hierzu keine Angaben

178 S. zu diesen Kriterien Abschnitt 15.2.2.2.

macht oder in einem nachweislich „unsicheren“ Drittland seinen Sitz oder seine Server hat,

- ein Cloud-Dienst durch technisch-organisatorische Maßnahmen den Zugriff durch Dritte verhindert und sich selbst nachweislich und kontrollierbar technisch und organisatorisch von einer Kenntnisnahme ausschließt,¹⁷⁹
- ein Cloud-Dienst einer Überwachung durch Aufsichtsbehörden unterliegt und geeignete, vergleichbare und seriöse Zertifikate, die eine Kontrolle der technischen und organisatorischen Maßnahmen sowie des Cloud-Datenschutzes nachweisen, vorweisen kann,
- ein Cloud-Dienst eine gute oder schlechte Bewertung durch andere Nutzer erhalten hat.

15.4.5 Unterstützung bei der Abwägung von Einwilligungslösungen

Auf die Problematik einer informierten, freiwilligen, bestimmten und formal richtigen Einwilligung sollte der Dienst hinweisen. Er könnte die Ausnahmen hervorheben, bei denen eine Einwilligung im Einzelfall umsetzbar erscheint – etwa, wenn nur ein überschaubarer Kreis betroffener Dritter besteht, zu denen der Cloud-Nutzer einen persönlichen Kontakt hat, oder wenn der Datenbestand sich nicht häufig ändert. Im Übrigen sollte der Dienst jedoch von der Einwilligungslösung im Hinblick auf praktische Erwägungen tendenziell abraten.

15.4.6 Unterstützung bei der Einhaltung der Vorgaben zur Auftragsdatenverarbeitung

Der Cloud-Nutzer benötigt auch als Auftraggeber einer Auftragsdatenverarbeitung bei der Auswahl und Kontrolle des Cloud-Anbieters Unterstützung. Hierzu könnte der Dienst bereits bei der Erstellung eines Risikoprofils der geplanten Auftragsdatenverarbeitung anhand der konkreten Angaben und Anforderungen des Cloud-Nutzers mitwirken. Auf diesem Risikoprofil auf-

179 S. hier das Konzept des Trusted-Cloud-Projekts „Sealed Cloud“, hierzu Jäger/Riecken 2014, 2 ff.; hierzu auch Kroschwald, in: Taeger 2013, 301 ff.

bauend könnte er durch eine dynamische Checkliste dem Cloud-Nutzer bei der Erstellung von Sicherheitsanforderungen gegenüber dem Anbieter Hilfestellung geben. Diese Sicherheitsanforderungen könnte er dann mit Angaben von bestehenden Anbietern etwa zu deren Sitz und Serverstandort, deren Sicherheitskonzept, den Kontrollmöglichkeiten, Zertifizierungsstatus, zur Qualität der Zertifikate sowie zu weiteren technischen und organisatorischen Maßnahmen abgleichen. Im Ergebnis könnte dann eine Auswahl zwischen geeigneten Anbietern übrig bleiben.

Der Dienst könnte den Cloud-Nutzer in seiner Kontrollpflicht als Auftraggeber unterstützen, indem er die von den verschiedenen Cloud-Anbietern verwendeten Vertragsklauseln vorab prüft und dann für den Nutzer bezogen auf seine Bedürfnisse und seine Situation als geeignet oder nicht geeignet bewertet. Unterstützung des Cloud-Nutzers könnte auch hinsichtlich der weiteren Vertragsgestaltung oder Auswahl erfolgen. So könnte der Dienst Vertragsklauseln von Cloud-Anbietern auf die Einhaltung der Vorgaben aus § 11 Abs. 2 Satz 2 Nr. 1 bis 10 BDSG in diesen Klauseln überprüfen. Er könnte dem Cloud-Nutzer außerdem bei der Erstellung und Prüfung eines entsprechenden Vertrages automatisiert oder manuell Hilfestellung anbieten. Vorstellbar ist beispielsweise, dass er aus den ihm bekannten Informationen über die Präferenzen und Erfordernisse des Nutzers ein personalisiertes Vertragsmuster erstellt, das dem gesetzlichen Klauselkatalog des § 11 Abs. 2 Satz 2 Nr. 1 und 2 BDSG entspricht.¹⁸⁰

Der Dienst könnte den Cloud-Nutzer auch bei der Ausübung seines Weisungsrechts nach § 11 Abs. 3 Satz 1 BDSG unterstützen. In der Praxis wäre ein Cloud-Nutzer wohl kaum in der Lage, substantiierte Anweisungen hinsichtlich des konkreten Datenumgangs sowie den erforderlichen technischen und organisatorischen Maßnahmen zu geben. Auch könnte der Cloud-Anbieter entsprechend unmöglich differenzierte Weisungen von jedem einzelnen Auftraggeber in Empfang nehmen. Ein entsprechender Dienst kann diese Weisungen jedoch derart standardisieren, dass der Cloud-Nutzer bei-

180 S. Abschnitt 15.2.2.1.

spielsweise nur noch zwischen vordefinierten Alternativen zu wählen braucht.¹⁸¹

Unterstützend könnte ein Dienst auch den Cloud-Anbieter über das Vorliegen einer Auftragsdatenverarbeitung informieren und ihn mit passenden Informationen zu den Auftragnehmerpflichten versorgen. Hierzu zählen insbesondere die Weisungsbindung, die Kontrollpflichten und Zertifizierungsmöglichkeiten, aufsichtsbehördliche Kontrollen, die technischen und organisatorischen Maßnahmen sowie die Hinweispflichten bei Datenschutzverstößen.

15.4.7 Unterstützung beim grenzüberschreitenden Cloud-Computing

Aufgabe des Dienstes könnte auch sein, mit Hilfe der Informationen über den Cloud-Nutzer eine Prüfung vorzunehmen, inwiefern eine Cloud-Nutzung, die sich auf ein Drittland erstreckt, überhaupt im Einzelfall erforderlich ist. Gegebenenfalls könnte dem Cloud-Nutzer zu einem entsprechenden Anbieter geraten werden, der einen exklusiven Datenumgang innerhalb der EU und des EWR anbietet. In manchen Fällen kann sich die Erforderlichkeit ergeben, einen Dienst zu wählen, bei dem Daten auch in Drittländer übermittelt werden. Beispielsweise könnte die Nutzung aus Kosten- oder Verfügbarkeitsgründen oder für die Zusammenarbeit mit weiteren Nutzern in Drittländern erforderlich sein. In solch einem Fall müsste der Dienst den Nutzer auf die spezifischen datenschutzrechtlichen Risiken einer internationalen Cloud-Nutzung sowie die Voraussetzungen der Zwei-Stufen-Prüfung für einen Datenexport hinweisen.¹⁸² Der Dienst könnte Angaben über Anbieter hinsichtlich ihrer Standorte und Unterauftragnehmer berücksichtigen und so dann dem Cloud-Nutzer beispielsweise Zielländer mit angemessenem Datenschutzniveau vorschlagen. Auch könnte die Nutzung von Standardvertragsklauseln sowie PBCR vorgeschlagen werden.¹⁸³ Hierfür könnte der Dienst entsprechende Klauseldokumente und Informationen zu den Genehmigungsverfahren vorhalten.

181 Weichert, DuD 2010, 685; Niemann/Hennrich, CR 2010, 692; Opfermann, ZeuS 2012, 135.

182 S. zu den Voraussetzungen Abschnitt 15.2.2.4.1.

183 S. hierzu Abschnitt 15.2.2.4.4.

15.4.8 Unterstützung bei der Einhaltung von Betroffenenrechten und technisch-organisatorischen Maßnahmen

Der Dienst könnte auch Informationen über Betroffenenrechte anbieten. Gegebenenfalls könnte er die Informationen über beteiligte Stellen automatisiert zusammentragen und dem Cloud-Nutzer gebündelt und aufgearbeitet zur Verfügung stellen. Zur Herstellung von Transparenz könnte er beispielsweise Informationen zum Cloud-Anbieter als Empfänger und den Umständen der Cloud-Nutzung, die der Nutzer später im Rahmen der Benachrichtigung und Auskunft an den Betroffenen weitergeben muss, vorhalten. Unter Umständen kann er den verantwortlichen Nutzer sogar dahingehend unterstützen, den Betroffenen diese Informationen mit (automatisiert) erstellten Benachrichtigungs- oder Auskunftsschreiben zukommen zu lassen. Dabei ist von zentraler Bedeutung, dass die Informationen individualisiert erfolgen – abstrakte Datenschutzerklärungen reichen nicht.¹⁸⁴ Auch müssen die Informationen auf Online-Plattformen zur dauerhaften Wiedergabe¹⁸⁵ vorhanden sein. Sie könnten beispielsweise zusätzlich als E-Mail an den Betroffenen versendet sowie – aufgrund ihres hohen Missbrauchspotenzials – sicher verschickt oder dargestellt werden.

Der Dienst könnte den Cloud-Nutzer auch darin unterstützen, der Berichtigungs-, Lösch- und Sperrpflicht nachzukommen. Er kann dem Cloud-Nutzer helfen zu erkennen, wann er berichtigungs-, lösch- und wann sperrpflichtig ist. Auch kann er ihn unterstützen, die jeweilige Berichtigung, Löschung oder Sperrung von Daten tatsächlich durchzuführen. Dies ist in der Cloud besonders schwierig, weil die im Internet gespeicherten oder auch nur versendeten Daten häufig in Zwischenspeichern abgelegt oder aus Redundanzgründen gespiegelt und archiviert werden. Diese Datenkopien lassen sich weder vollständig zurückholen noch vollständig löschen oder berichtigen.¹⁸⁶ Lösungsansätze, die Daten mit einer Art Selbstzerstörungsmechanis-

184 Dix, in: Simitis 2014, § 33 Rn. 42; Gola/Schomerus 2012, § 33 Rn. 18.

185 Dix, in: Simitis 2014, § 34 Rn. 49; Meents/Hinzpeter, in: Taeger/Gabel 2013, § 34 Rn. 41.

186 Däubler, in: Däubler/Klebe/Wedde/Weichert 2014, § 35 BDSG, Rn. 15a; Dix, in: Simitis 2014, § 35 Rn. 8; Hansen, in: Borges/Schwenk 2012, 90; zur Unmöglichkeit einer Löschung von im Netz veröffentlichten Daten Weichert, DuD

mus versehen und so einen „digitalen Radiergummi“ schaffen wollen, lassen sich technisch (noch) nicht umsetzen.¹⁸⁷ Vorerst müssen deshalb Daten und Backups so gut wie möglich verfolgt und ihre Wege protokolliert werden, um sie gegebenenfalls gezielt löschen zu können.¹⁸⁸ Der Dienst könnte den Cloud-Nutzer deshalb darin unterstützen, Cloud-Angebote zu identifizieren, die eine Verfolgbarkeit von Daten erleichtern oder selbst ein Werkzeug bereitstellen, mit dem sich Datenwege und Backups nachvollziehen lassen. Am wirksamsten ist auch hier die nutzerseitige Verschlüsselung, auf die der Dienst hinweisen sollte.

Zuletzt kann der Dienst auch zur Einhaltung von technischen und organisatorischen Maßnahmen beitragen. Möglich ist beispielsweise die Zurverfügungstellung von – gegebenenfalls individualisierten – Checklisten, anhand derer der Cloud-Anbieter prüfen kann, ob seine Infrastruktur die Maßnahmenanforderungen nach § 9 BDSG in Verbindung mit Anlage zu § 9 BDSG hinreichend berücksichtigt und ob er die weiteren organisatorischen Anforderungen aus den allgemeinen Bestimmungen des Bundesdatenschutzgesetzes einhält.

15.5 Literaturverzeichnis

Art. 29 Datenschutzgruppe: Zur Verarbeitung von personenbezogenen Daten von Beschäftigten. WP 48, Brüssel 2001.

Art. 29 Datenschutzgruppe: Stellungnahme 4/2007 zum Begriff „personenbezogener Daten“. WP 136, Brüssel 2007.

2009, 12; zum „Backup-Problem“ bei Verschlüsselungen, Kroschwald, ZD 2014, 79 f.

187 Der Ansatz eines den Daten anheftenden Verfallsdatums wurde unter dem (allerdings irreführenden) Begriff „digitaler Radiergummi“ diskutiert. Zum Gegenstand und technischen Details s. Federrath/Fuchs/Herrmann/Maier/Scheuer/Wagner, DuD 2011, 403; Jandt/Kieselmann/Wacker, DuD 2013, 239 f.

188 S. hierzu International Working Group on Data Protection in Telecommunications 2012 (Sopot Memorandum): „An automatically recorded copying and deletion audit trail should be established, showing clearly which copies of personal data the processor or its subcontractors have created and deleted.“; s. auch Hansen, in: Borges/Schwenk 2012, 90.

- Art. 29 Datenschutzgruppe:** Arbeitsdokument zu „Häufig gestellten Fragen“ über verbindliche unternehmensinterne Datenschutzregelungen (BCR). WP 155, Brüssel 2009.
- Art. 29 Datenschutzgruppe:** Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsdatenverarbeiter“. WP 169, Brüssel 2010.
- Art. 29 Datenschutzgruppe:** Stellungnahme 8/2010 zum anwendbaren Recht. WP 179, Brüssel 2010.
- Art. 29 Datenschutzgruppe:** Stellungnahme 5/2012 zum Cloud Computing. WP 196, Brüssel 2012
- Art. 29 Datenschutzgruppe:** Erläuterndes Dokument zu verbindlichen Unternehmensinternen Datenschutzregelungen für Auftragsdatenverarbeiter. WP 204, Brüssel 2013.
- Bedner, M.:** Cloud Computing – Technik, Sicherheit und rechtliche Gestaltung. Kassel 2013.
- Bergmann, L./Möhrle, R./Herb, A.:** Datenschutzrecht – Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und zum Bereichsspezifischen Datenschutz. 46. Ergänzungslieferung, Stuttgart/München 2013.
- Bizer, J.:** Rechtliche Bedeutung der Kryptographie. In: Datenschutz und Datensicherheit (DuD) 1997, S. 203-208.
- Boos, C.; Kroschwald, S.; Wicker, M.:** Datenschutz bei Cloud Computing zwischen TKG, TMG und BDSG – Datenkategorien bei der Nutzung von Cloud Diensten. In: Zeitschrift für Datenschutz (ZD), 2013, S. 205-210.
- Borges, G.; Schwenk, J.:** Daten- und Identitätsschutz in Cloud-Computing, E-Government und E-Commerce. Heidelberg 2012.
- Brennscheidt, K.:** Cloud Computing und Datenschutz. Baden-Baden 2013.
- Däubler, W.; Klebe, T.; Wedde, P.; Weichert, T.:** Bundesdatenschutzgesetz – Kompaktkommentar zum BDSG. 4. Auflage, Frankfurt am Main 2014.
- Deussen, P. H.; Strick, L.; Peters, J.:** Cloud-Computing für die öffentliche Verwaltung (ISPRAT-Studie). Berlin 2010.
- Düsseldorfer Kreis:** Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 19./20. April 2007, Fallgruppen zur Internationalen Auftragsdatenverarbeitung – Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung. Hamburg 2007.
- Düsseldorfer Kreis:** Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 28./29. April 2010, Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen. Hannover 2010.
- Eckhardt, J.:** Auftragsdatenverarbeitung. In: Datenschutz und Datensicherheit (DuD), 2013, S. 585-591.
- Eckhardt, J.:** BDSG: Neuregelungen seit 01.09.2009. In: Datenschutz und Datensicherheit (DuD), 2009, S. 587-595.
- Ehmann, E.; Helfrich, M.:** EG-Datenschutzrichtlinie: Kurzkommentar. 1. Auflage, Köln 1999.

- Engels, T.:** Datenschutz in der Cloud – Ist hierbei immer eine Auftragsdatenverarbeitung anzunehmen? In: Kommunikation und Recht (K&R), 2011, S. 548-551.
- Enzmann, M.; Roßnagel, A.:** Realisierter Datenschutz für den Einkauf im Internet. In: Computerrecht (CR), 2002, S. 141-150.
- Federrath, H.; Fuchs, K.-P.; Herrmann, D.; Maier, D.; Scheuer, F.; Wagner, K.:** Grenzen des digitalen Radiergummis. In: Datenschutz und Datensicherheit (DuD), 2011, S. 403-407.
- Gaul, B.; Koehler, L.-M.:** Mitarbeiterdaten in der Computer Cloud: Datenschutzrechtliche Grenzen des Outsourcing. In: Betriebs-Berater (BB), 2011, S. 2229-2236.
- Geppert, M.; Schütz, R.:** Beck'scher TKG-Kommentar. 4. Auflage, München 2013.
- Geppert, M.; Piepenbrock, H.-J.; Schütz, R.; Schuster, F.:** Beck'scher TKG Kommentar. 3. Auflage, München 2006.
- Gola, P.; Schomerus, P.:** BDSG Bundesdatenschutzgesetz. 11. Auflage, München 2012.
- Götz, C.:** Grenzüberschreitende Datenübermittlung im Konzern Zulässigkeit nach BDSG und Entwurf der EU-DS-GVO. In: Datenschutz und Datensicherheit (DuD), 2013, S. 631-637.
- Hansen, M.:** Datenschutz im Cloud Computing. In: Daten-Identitätsschutz in Cloud Computing, E-Government und E-Commerce. Hrsg.: Borges, G.; Schwenk, J., Heidelberg 2012, S. 79-95.
- Heidrich, J.; Wegener, C.:** Sichere Datenwolken Cloud Computing und Datenschutz. In: Multimedia und Recht (MMR), 2010, S. 803-805.
- Hennrich, T.:** Compliance in Clouds. In: Computerrecht (CR), 2011, S. 546-552.
- Hilber, M.:** Handbuch Cloud Computing. 1. Auflage, Köln 2014.
- Hoeren, T.:** Anonymität im Web – Grundfragen und aktuelle Entwicklung. In: Zeitschrift für Rechtspolitik (ZRP), 2010, S. 251-253.
- Hornung, G.; Sädler, S.:** Europas Wolken – Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing. In: Computerrecht (CR), 2012, S. 638-645.
- International Working Group on Data Protection in Telecommunications 2012:** An automatically recorded copying and deletion audit trail should be established, showing clearly which copies of personal data the processor or its subcontractors have created and deleted. Brüssel 2012.
- Jandt, S.; Kieselmann, O.; Wacker, A.:** Recht auf Vergessen im Internet. In: Datenschutz und Datensicherheit (DuD), 2013, S. 235-241.
- Jandt, S.; Roßnagel, A.:** Datenschutz in Social Networks – Kollektive Verantwortlichkeit für die Datenverarbeitung. In: Zeitschrift für Datenschutz (ZD), 2011, S. 160-166.
- Jäger, H.; Rieken, R.:** IDGARD Sealed Cloud – das erste vollfunktionale Kommunikationsnetz, das sowohl Inhalte als auch Metadaten schützt. München 2014.
- Jotzo, F.:** Gilt deutsches Datenschutzrecht auf für Google, Facebook & Co. Bei grenzüberschreitendem Datenverkehr? In: Multimedia und Recht (MMR), 2009, 232-237.

- Jotzo, F.:** Der Schutz personenbezogener Daten in der Cloud. Baden-Baden 2013.
- Kamp, M.; Rost, M.:** Kritik an der Einwilligung. In: Datenschutz und Datensicherheit (DuD), 2013, S. 80-84.
- Kappes, M.:** Netzwerk- und Datensicherheit. 1. Auflage, Wiesbaden 2007.
- Karg, M.:** Die Rechtsfigur des personenbezogenen Datums – Ein Anachronismus des Datenschutzes. In: Zeitschrift für Datenschutz (ZD), 2012, S. 255-261.
- Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“:** Lizenzierungsbedarf beim Cloud Computing – Welche Rechte zur Nutzung von Software benötigen Anbieter und Nutzer von Cloud Computing. 1. Auflage, Berlin 2012.
- Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“:** Datenschutzrechtliche Lösungen für Cloud Computing – Ein rechtspolitisches Thesenpapier der AG Rechtsrahmen des Cloud Computing. 1. Auflage, Berlin 2012.
- Konferenz der Datenschutzbeauftragten des Bundes und der Länder:** Datenschutzkonferenz: Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und osteuropäischen Staaten. Bremen 2013. In: http://www.bfdi.bund.de/DE/Home/homepage_Kurzmeldungen2013/PMDerDSK_SafeHarbor.html, zugegriffen am 30.07.2013.
- Kroschwald, S.; Wicker, M.:** Einwilligung des Betroffenen in den Umgang mit seinen Daten als Lösung für das Cloud Computing. In: Datenschutzberater (DSB), Newsletter zum 15. Euroforum Datenschutzkongress 2014, S. 12-13.
- Kroschwald, S.:** Kollektive Verantwortung für den Datenschutz in der Cloud – Datenschutzrechtliche Folgen einer geteilten Verantwortlichkeit beim Cloud Computing. In: Zeitschrift für Datenschutz (ZD), 2013, S. 388-394.
- Kroschwald, S.:** Verschlüsseltes Cloud Computing – Auswirkungen der Kryptografie auf den Personenbezug in der Cloud. In: Zeitschrift für Datenschutz (ZD), 2014, S. 75-80.
- Kroschwald, S.:** Verschlüsseltes Cloud Computing – Anwendung des Daten- und Geheimnisschutzrechts auf „betreibersichere“ Clouds am Beispiel der „Sealed Cloud“. In: Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter (Tagungsband DSRI Herbstakademie 2013). Hrsg.: Taeger, J., Oldenburg 2013, S. 289-308.
- Kühling, J.; Klar, M.:** Unsicherheitsfaktoren Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität. In: Neue Juristische Wochenschrift (NJW), 2013, S. 3611-3617.
- Kunz, T.; Niehues, P.; Walmann, U.:** Technische Unterstützung von Audits bei Cloud-Betreibern. In: Datenschutz und Datensicherheit (DuD), 2013, S. 521-525.
- Masing, J.:** Herausforderung des Datenschutzes. In: Neue Juristische Wochenschrift (NJW), 2012, S. 2305-2311.
- Moos, F.:** Die EU-Standardvertragsklauseln für Auftragsverarbeiter 2010. In: Computerrecht (CR), 2010, S. 281-286.
- Müller-Broich, J. D.:** Telemediengesetz. 1. Auflage, Baden-Baden 2012.
- Nägele, T.; Jacobs, S.:** Rechtsfragen des Cloud Computing. In: ZUM 2010, S. 281-292.

- Niemann, F.; Hennrich, T.:** Kontrolle in den Wolken?. In: Computerrecht (CR), 2010, S. 686-692.
- Niemann, F.; Paul, J.-A.:** Bewölkt oder wolkenlos – rechtliche Herausforderung des Cloud Computing. In: Kommunikation und Recht (K&R), 2009, S. 444-452.
- Opfermann, E.:** Datenschutzkonforme Vertragsgestaltung im „Cloud Computing“. In: Zeitschrift für Europäisches Privatrecht (ZEuS), 2012, S. 121-160.
- Plath, K.-U.:** Bundesdatenschutzgesetz (BDSG). 1. Auflage, Köln 2013.
- Räther, P. C.; Seitz, N.:** Übermittlung personenbezogener Daten in Drittstaaten – Angemessenheitsklausel, Safe Harbor und die Einwilligung. In: Multimedia und Recht (MMR), 2002, S. 425-433.
- Räther, P.C.:** Datenschutz und Outsourcing. In: Datenschutz und Datensicherheit (DuD), 2005, S. 461-466.
- Reindl, M.:** Cloud Computing und Datenschutz. In: Inside the cloud – Neue Herausforderungen für das Informationsrecht. Hrsg.: Taeger, J.; Wiebe, A., Edewecht 2009, S. 445.
- Rittweger, C.; Schmidl, M.:** Einwirkung von Standardvertragsklauseln auf § 28 BDSG. In: Datenschutz und Datensicherheit (DuD), 2004, S. 617-620.
- Roßnagel, A.:** Beck'scher Kommentar zum Recht der Telemediendienste, Kommentar zum TMG, SigG, SigV, JMSStV, BGB (Auszüge), VwVfG (Auszüge), ZPO (Auszüge). München 2013.
- Roßnagel, A.:** Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht. In: Zeitschrift für Datenschutz (ZD), 2013, S. 562-567.
- Roßnagel, A.:** Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirk-samen technikbasierten Persönlichkeitsschutzes? In: Innovation, Recht und öffent-liche Kommunikation. Hrsg.: Eifert, M.; Hoffmann-Riem, W., Berlin 2011, S. 41-66.
- Roßnagel, A.:** Handbuch Datenschutzrecht. München 2003.
- Roßnagel, A.:** Modernisierung des Datenschutzes – Nicht die Definition von Perso-nendaten muss geändert werden, sondern die Anforderungen an ihren Schutz, In: Zeitschrift für Datenrecht und Informationssicherheit (digma), 2011, S. 160-165.
- Roßnagel, A.; Jandt, S.; Richter, P.:** Die Zulässigkeit der Übertragung personenbe-zogener Daten in die USA im Kontext der NSA-Überwachung. In: Datenschutz und Datensicherheit (DuD), 2014, S. 545-551.
- Roßnagel, A.; Pfitzmann, A.; Garstka, H.:** Modernisierung des Datenschutzrechts – Gutachten im Auftrag des Bundesministeriums des Inneren. Berlin 2001.
- Roßnagel, A.; Scholz, P.:** Datenschutz durch Anonymität und Pseudonymität – Rechtsfolge der Verwendung anonymer und pseudonymer Daten. In: Multimedia und Recht (MMR), 2000, S. 721-731.
- Roßnagel, A.:** Handbuch Datenschutzrecht. 1. Auflage, München 2003.
- Schaar, P.:** Datenschutz im Internet – Die Grundlagen. 1. Auflage, München 2002.
- Schaffland, H.-J.; Wiltfang, N.:** Bundesdatenschutzgesetz BDSG. Stand: 31.12.2013, Berlin 2013.
- Scholz, M.; Lutz, H.:** Standardvertragsklauseln für Auftragsverarbeiter und § 11 BDSG. In: Computerrecht (CR), 2011, S. 424-428.

- Schröder, C.; Haag, N. C.:** Neue Anforderungen an Cloud Computing für die Praxis. In: Zeitschrift für Datenschutz (ZD), 2011, S. 147-152.
- Schulz, S. E.:** Cloud Computing in der öffentlichen Verwaltung Chancen – Risiken – Modelle. In: Multimedia und Recht (MMR), 2010, 75-80.
- Schuster, F.; Reichl, W.:** Cloud Computing & SaaS: Was sind die wirklich neuen Fragen? In: Computerrecht (CR), 2010, S. 38-42.
- Selzer, A.:** Die Kontrollpflicht nach § 11 Abs. 2 Satz 4 BDSG im Zeitalter des Cloud-Computings. In: Datenschutz und Datensicherheit (DuD), 2013, S. 215-219.
- Simitz, S.:** Bundesdatenschutzgesetz. 8. Auflage, Baden-Baden 2014.
- Spies, A.:** Cloud Computing: Keine personenbezogenen Daten bei Verschlüsselung. In: Multimedia und Recht Aktuell (MMR-Aktuell), 2011, 313727.
- Spindler, G.; Schuster, F.:** Recht der Elektronischen Medien. 2. Auflage, München 2011.
- Splittgerber, A.; Rockstroh, S.:** Sicher durch die Cloud navigieren – Vertragsgestaltung beim Cloud Computing. In: Betriebs-Berater (BB), 2011, 2179-2185.
- Stiemerling, O.; Hartung, J.:** Datenschutz und Verschlüsselung. In: Computerrecht (CR), 2012, S. 60-68.
- Taeger, J.; Gabel, D.:** BDSG und Datenschutzvorschriften des TKG und TMG. 2. Auflage, Frankfurt am Main 2013.
- Taeger, J.; Wiebe, A.:** Inside the Cloud – Neue Herausforderungen für das Informationsrecht. Edeweicht 2009.
- Taeger, J.:** Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter: Tagungsband DSRI Herbstakademie 2013. 1. Auflage, Band 1, Edeweicht 2013.
- Thalhofer, T.:** Grenzenlos: Compliance bei Cloud Computing. In: Corporate Compliance Zeitschrift (CCZ), 2011, S. 222-225.
- Vander, S.:** Auftragsdatenverarbeitung 2.0? – Neuregelungen der Datenschutznovelle II im Kontext von § 11 BDSG. In: Kommunikation und Recht (K&R), 2010, S. 293-298.
- Weber, M. P.; Voigt, P.:** Internationale Auftragsdatenverarbeitung – Praxisempfehlung für die Auslagerung von IT-Systemen in Drittstaaten mittels Standardvertragsklauseln. In: Zeitschrift für Datenschutz (ZD), 2011, S. 74-79.
- Weichert, T.:** BDSG-Novelle zum Schutz von Internet-Inhaltsdaten. In: Datenschutz und Datensicherheit (DuD), 2009, S. 7-14.
- Weichert, T.:** Cloud Computing und Datenschutz. In: Datenschutz und Datensicherheit (DuD), 2010, S. 679-687.
- Wuermeling, U.:** Handelshemmnis Datenschutz. 1. Auflage, Köln 2000.

16 Vertragliche Aspekte des Cloud-Computing

S. Jandt, S. Kroschwald, A. Roßnagel, M. Wicker

Die Beziehung zwischen dem Cloud-Nutzer und dem Cloud-Anbieter ist ein zivilrechtlicher Vertrag, auf den das Bürgerliche Gesetzbuch (BGB) anwendbar ist. Die richtige Vertragsgestaltung beim Cloud-Computing dient vor allem der angemessenen Risikoverteilung zwischen den beteiligten Cloud-Akteuren. So kann im Wege des Cloud-Vertrages neben der Hauptleistung des Cloud-Dienstes beispielsweise geregelt werden, wie der Vertrag zu kündigen ist oder in welchen Konstellationen Schadensersatz zu leisten ist.

Im Folgenden werden die wesentlichen Regelungsbereiche für einen Cloud-Vertrag dargestellt, die geregelt werden sollten, um eine angemessene Verteilung der rechtlichen Risiken zwischen den Cloud-Akteuren zu erreichen.

16.1 Allgemeine Geschäftsbedingungen beim Cloud-Vertrag

Auch wenn die Vertragsparteien grundsätzlich einen Vertrag individuell aushandeln könnten, ist dies bei den standardisierten Angeboten aus der Cloud häufig nicht der Fall.¹ Vielmehr bietet der Cloud-Anbieter verschiedene Cloud-Lösungen an und hält für den möglichen Cloud-Nutzer seine Allgemeinen Geschäftsbedingungen (AGB) gemäß § 305 Abs. 1 BGB bereit, die im Fall des Vertragsschlusses gemäß § 305 Abs. 2 BGB Anwendung finden sollen.

Die Vorschriften über die AGB in den §§ 305 ff. BGB schützen überwiegend die Verbraucher, sie finden aber gemäß § 310 Abs. 1 Satz 2 BGB auch für Verträge zwischen Unternehmen Anwendung. Ziel der Normen ist vor allem, intransparente, überraschende und unangemessene Klauseln in den AGB zu verhindern. Möglich ist, dass die Regelungen innerhalb der AGB

1 S. zu der Definition von Cloud-Computing als IT-Bereitstellungsmodell bereits Kapitel 2.

von dem gesetzlichen Leitbild im Bürgerlichen Gesetzbuch abweichen und eine andere Risikoverteilung zwischen den Vertragsparteien vorsehen. Sofern der Vertragspartner die AGB-Regelungen vor Gericht angreift, stellt das Gericht in einem solchen Fall meist die Unwirksamkeit der gesamten vertraglich vereinbarten AGB fest. Diese gilt insbesondere für Haftungsregelungen, die den Cloud-Anbieter weitgehend zu Lasten des Cloud-Nutzers von einer Haftung freistellen. An die Stelle der AGB treten in diesem Fall die gesetzlich vorgesehenen Regelungen des Bürgerlichen Gesetzbuches für vergleichbare Vertragskonstellationen.

16.2 Cloud-Ressourcen als Mietgegenstand

Verträge über Cloud-Leistungen sind, wie die meisten Verträge im Zusammenhang mit Informationstechnik, nur schwer einem im Gesetz ausdrücklich geregelten Vertragstyp zuzuordnen. Vielmehr ist bei der vertragstypologischen Einordnung von Cloud-Verträgen die vorgesehene Hauptleistung mit dem gesetzlichen Leitbild der typischen Verträge des Bürgerlichen Gesetzbuchs zu vergleichen.

Die Bereitstellung von Informationstechnik aus dem Internet entspricht am ehestens einem Mietvertrag,² soweit die Vertragsparteien keine abweichenden Regelungen treffen.³ Beim Mietvertrag ist der Vermieter gemäß § 535 Abs. 1 Satz 1 BGB „verpflichtet, dem Mieter den Gebrauch der Mietsache während der Mietzeit zu gewähren“. Dabei hat der Vermieter gemäß § 535 Abs. 1 Satz 1 BGB „die Mietsache dem Mieter in einem zum vertragsgemäßen Gebrauch geeigneten Zustand zu überlassen und sie während der Mietzeit in diesem Zustand zu erhalten.“ Gemäß § 535 Abs. 2 BGB ist der Mieter „verpflichtet, dem Vermieter die vereinbarte Miete zu entrichten“. Legt man folglich zu Grunde, dass mit Hilfe von Cloud-Angeboten IT-Ressourcen ständig vorgehalten werden müssen, damit der Cloud-Nutzer

2 Wicker, MMR 2012, 783; BGH, NJW 2007, 2394, für Bereitstellung von Software im Rahmen eines Application-Service-Provider-Vertrages; LG Mannheim, Ur. v. 7.12.2010, Az: 11 O 273/10 für Kündigungsfristen bei Webhosting.

3 S. hierzu bereits Abschn. 15.1, so dass vor dem Hintergrund des AGB-Rechts Abweichungen zu Lasten des Cloud-Nutzers unbeachtlich bleiben können.

diese IT-Leistungen jederzeit bedarfsgerecht beziehen kann, ist eine mietrechtliche Einordnung der Beziehung zwischen den Cloud-Akteuren angemessen.⁴ Die ständige Verfügungsmöglichkeit über IT-Leistungen aus der Cloud stellt folglich einen Mietvertrag gemäß §§ 535 ff. BGB dar.

Dabei muss der „Cloud-Vermieter“ dem „Cloud-Mieter“ die IT-Ressource zum Gebrauch überlassen. Auf eine tatsächliche Besitzverschaffung kommt es nicht an. In der Cloud wählt der Nutzer entsprechend seinem Bedarf seine Komponenten aus und der Cloud-Anbieter hält diese fortwährend bereit und gewährt deren Nutzung.⁵

Die mietvertragliche Einordnung des Cloud-Computing führt zur Anwendbarkeit der Vorschriften des Mietrechts in den §§ 535 ff. BGB, soweit die Parteien keine eigenen Regelungen individuell ausgehandelt haben oder wenn die Regelungen in den AGB unangemessen vom Leitbild des Mietrechts abweichen. Die Cloud-Akteure sollten daher genaue Leistungsbeschreibungen, welche Cloud-Leistungen der Cloud-Anbieter erbringen muss, vornehmen.⁶

16.3 Notwendige Regelungen im Cloud-Vertrag

Um eine angemessene Risikoverteilung zu erreichen, sollten die Cloud-Akteure insbesondere Regelungen zur Verfügbarkeit,⁷ zur Gewährleistung im Fall von Mängeln⁸ und zur Beendigung des Vertrages und der Rückabwicklung⁹ treffen. Darüber hinaus sind weitere vertragliche Regelungen für den Streitfall sinnvoll.¹⁰

4 Wicker, MMR 2012, 783.

5 Wicker, MMR 2012, 783, 786.

6 S. hierzu Bitkom 2010, 15 ff.

7 S. Abschnitt 16.3.1.

8 S. Abschnitt 16.3.2.

9 S. Abschnitt 16.3.3.

10 S. Abschnitt 16.3.4.

16.3.1 Verfügbarkeit

Das Mietrecht verlangt eine vollständige Verfügbarkeit der Mietsache ab Beginn der Vertragslaufzeit.¹¹ Der Cloud-Nutzer muss also die Möglichkeit haben, ununterbrochen auf seine IT-Ressourcen in der Cloud zuzugreifen. Aufgrund der Verbindung zwischen Cloud-Anbieter und Cloud-Nutzer über das Internet ist für die Cloud-Nutzung zwischen drei Phasen zu unterscheiden. Zum einen muss der Cloud-Nutzer eine Verbindung über das Internet zur Cloud haben, über die er Daten in die Cloud übertragen und Leistungen aus der Cloud abrufen kann (Phase 1). Zweitens müssen die Cloud-Server funktionieren, um die Cloud-Leistungen erbringen zu können (Phase 2). Schließlich muss der Cloud-Anbieter eine funktionierende Verbindung über das Internet zur Cloud haben, um die Cloud-Leistungen administrieren und auf die Server in seiner Cloud verteilen zu können (Phase 3).

Während die Risiken einer funktionierenden Internetverbindung des Cloud-Nutzers zur Cloud (Phase 1) in dessen Sphäre fallen, muss der Cloud-Anbieter das Ausfallrisiko der Cloud-Server (Phase 2) und seiner Verbindung zum Internet (Phase 3) allein tragen.¹² Rechtliche Folgen eines Ausfalls in der Sphäre des Cloud-Anbieters können neben Minderung der Miete für die Zeit der gestörten Verfügbarkeit weitere Schadensersatzansprüche für die entstandenen Nachteile beim Cloud-Nutzer sein.¹³ Das Haftungsrisiko des Cloud-Anbieters ist bei der Vereinbarung einer Verfügbarkeit von 100 % schwierig abzuschätzen und unter Umständen sehr hoch, wenn der Cloud-Nutzer beispielsweise Schadensersatz wegen entgangenen Gewinns für Umsätze, die in der Zeit der Störung nachweislich hätten tätigen können, verlangt.

Dem Cloud-Nutzer kommt es darauf an, dass ihm die Leistung, die er benötigt und mietet,¹⁴ von Anfang an und während der gesamten Vertragsdauer fehlerfrei zur Verfügung steht. Der Cloud-Anbieter demgegenüber will Risiken der Verfügbarkeit nur in dem Umfang tragen, in dem er auch Einfluss

11 S. hierzu die Garantieverpflichtung des § 535 Abs. 1 Satz 2 BGB; s. dazu Pohle/Amann, CR 2009, 275.

12 S. hierzu den Wortlaut des § 535 Abs. 1 Satz 2 BGB; BGH, NJW 2001, 751 ff.

13 S. für Grid-Computing Niemann/Paul, K&R 2009, 446.

14 Wicker, MMR 2012, 783.

auf die Funktionsweise, beispielsweise für Wartung oder Updates, nehmen kann. Die Verfügbarkeit sollte daher im Cloud-Vertrag in einem Service Level Agreement (SLA)¹⁵ sehr detailliert ausgestaltet werden.¹⁶ So sollten die Vertragspartner beispielsweise Regelungen zu Entstörzeiten vereinbaren und etwaige Mitwirkungspflichten des Cloud-Nutzers festlegen.

16.3.2 Haftung und Gewährleistung

Hält der Cloud-Anbieter seine versprochene Leistung nicht ein, so kann der Cloud-Nutzer gemäß § 536 Abs. 1 Satz 1 BGB von der Zahlungspflicht befreit sein oder zumindest die Vergütung gemäß § 536 Abs. 1 Satz 2 BGB mindern. Das Mietrecht verlangt dabei kein Verschulden des Cloud-Anbieters für den Leistungsausfall. Vielmehr ist der Cloud-Anbieter dauerhaft zur Bereitstellung der Leistung aus der Cloud verpflichtet. Auch soweit der Leistungsausfall durch einen Dritten verursacht wurde, kann der Cloud-Nutzer von der Zahlungspflicht befreit sein.¹⁷

Hat darüber hinaus die Nicht-Verfügbarkeit zu wirtschaftlichen Nachteilen geführt, kann der Cloud-Nutzer gemäß §§ 280 ff. und §§ 536a ff. BGB auch Schadensersatz verlangen. Hier ist der Cloud-Anbieter allerdings nur dann zur Haftung verpflichtet, wenn er gemäß §§ 536a Abs. 1 und 280 Abs. 1 Satz 2 BGB den Ausfall zu vertreten hat.

Der Cloud-Anbieter wird sein Ausfallrisiko in der Regel standardisiert begrenzen und dementsprechend Haftungsbeschränkungen durchsetzen wollen.¹⁸ Allerdings sind solche Begrenzungen in den AGB nur in engen Grenzen möglich.¹⁹ Beispielsweise scheiden Haftungsfreistellungen für die vorsätzliche oder grob fahrlässige Verursachung von Schäden gemäß § 309 Nr. 7 b) BGB aus.

15 Von dem Bussche/Schelinski, in: Leupold/Glossner 2013, Teil 1, Rn. 384 ff.

16 Trusted Cloud, AG Rechtsrahmen 2014a, 18 f.

17 Gesetzliche Haftungsprivilegien, wie §§ 44 TKG oder §§ 8 ff. TMG, kommen dem Cloud-Anbieter in der Beziehung zum Cloud-Nutzer nicht zugute.

18 Duisburg, in: Picot/Hertz/Götz 2011, 49, 54.

19 Kompetenzzentrum Trusted Cloud, AG Rechtsrahmen des Cloud Computing (Hrsg.), 2014a, 24 ff.

16.3.3 Beendigung und Rückabwicklung

Für einen Cloud-Vertrag sind Regelungen zur Beendigung und zur Rückabwicklung erforderlich. Soweit die Cloud-Akteure nichts anderes vereinbaren, gelten die Kündigungsfristen des Mietrechts. Das gesetzliche Leitbild des Mietvertrags bietet Kündigungsfristen, die insbesondere dem Cloud-Nutzer ausreichend Zeit belassen, um nach einer Kündigung adäquaten Ersatz der Ressourcen zu besorgen. Gemäß § 580a Abs. 2 BGB gilt insbesondere für Gewerberaummietverhältnisse eine Kündigungsfrist von sechs Monaten.²⁰ Somit ermöglicht Cloud-Computing auf der einen Seite, IT-Ressourcen kurzfristig und schnell aus der Cloud verfügbar zu machen, und auf der anderen Seite eine Sicherheit, dass die IT-Ressourcen dem Cloud-Nutzer auch nicht kurzfristig entzogen werden können.

Im Cloud-Vertrag können jedoch auch andere Kündigungsfristen vereinbart werden, wobei hier der Cloud-Anbieter beachten muss, dass eine gegenüber dem Cloud-Nutzer deutlich nachteilige Regelung in den Allgemeinen Geschäftsbedingungen einer gerichtlichen Überprüfung nicht standhalten wird. Es ist jedoch ebenfalls anzunehmen, dass sich kurze Kündigungsfristen für den Cloud-Nutzer als ein besonderer Vorteil darstellen können, weil er sich nicht an lange Verträge binden muss.

Neben der Bestimmung der Vertragslaufzeit, automatischer Vertragsverlängerungen, Kündigungsfristen und Voraussetzungen für außerordentliche Kündigungen²¹ sollten die Cloud-Akteure auch die Rückabwicklung nach Beendigung regeln.²²

Das Mietrecht hält die passenden Vorschriften bereit, wenn das Vertragsverhältnis in der Cloud beendet ist. So ist die IT-Ressource dem Cloud-Anbieter nach Ablauf der Vertragsbeziehung gemäß § 546 BGB „zurückzugewähren“. Hierzu muss der Cloud-Nutzer grundsätzlich nichts unternehmen

20 Anwendbarkeit der Kündigungsfristen für gewerbliche Mietverträge bei Webhosting, LG Mannheim, Urt. v. 7.12.2010, Az: 11 O 273/10.

21 So können die Parteien für den Fall einer wesentlichen Nichteinhaltung der SLA eine außerordentliche Kündigungsmöglichkeit entsprechend dem gesetzlichen Leitbild vereinbaren.

22 Kompetenzzentrum Trusted Cloud, AG Rechtsrahmen des Cloud Computing (Hrsg.), 2014a, 27 f.

außer, die Nutzung der Cloud-Ressource einzustellen. Im eigenen Interesse sollte der Cloud-Nutzer beispielsweise gespeicherte Daten auf lokale IT-Ressourcen zurückholen.

Der Cloud-Anbieter könnte rein faktisch ab dem Zeitpunkt des Vertragsendes den Zugang für den Cloud-Nutzer sperren. Allerdings ist er nicht berechtigt, die dem Cloud-Nutzer gehörenden Daten zu behalten, er muss eine Datenüberführung ermöglichen oder die Daten im Einverständnis mit dem Cloud-Nutzer löschen.²³

Löscht der Cloud-Anbieter beispielsweise nach Ablauf des Vertrages die Daten des Cloud-Nutzers, ohne dass dieser die Daten sichern konnte, kann der Cloud-Anbieter zum Schadensersatz verpflichtet sein.²⁴ Der Cloud-Vertrag sollte daher Regelungen enthalten, wann beispielsweise Daten nach Ablauf des Vertragsverhältnisses durch den Cloud-Anbieter gelöscht werden dürfen.

16.3.4 Streitvermeidende Vertragsinhalte

Darüber hinaus sollten die Vertragsparteien verschiedene potenzielle Streitpunkte im Cloud-Vertrag regeln. Hierzu kann beispielsweise eine Vereinbarung zum Gerichtsstand getroffen werden, um für den Fall einer gerichtlichen Auseinandersetzung vorab festzulegen, wo ein eventueller Prozess durchgeführt werden soll. Denkbar sind auch Schiedswahlklauseln, mit deren Hilfe ein Streit vor einem (internationalen) Schiedsgericht geklärt werden kann, um Zeit und Kosten zu sparen.²⁵

Neben der Vereinbarung über Verfügbarkeitswerte in einem SLA sowie der Vereinbarung über die Auftragsdatenverarbeitung gemäß § 11 BDSG²⁶ können auch Voraussetzungen für die Änderung der vertraglichen Bedingungen festgelegt werden, beispielsweise also Voraussetzungen für Preiserhö-

23 Koch, CR 2006, 48 in Bezug auf Datenspeicherung im Rahmen von Grid Computing.

24 OLG Dresden, NJW-RR 2013, 27, in Bezug auf E-Mails im gekündigten E-Mail-Account.

25 Trusted Cloud, AG Rechtsrahmen 2014a, 12 f.

26 S. zu den datenschutzrechtlichen Anforderungen Kapitel 15.

hungen oder Softwareänderungen.²⁷ Die Cloud-Akteure können ebenfalls vereinbaren, dass der Cloud-Anbieter den Cloud-Nutzer über die Qualität der Leistungserbringung im Kontext der SLA informiert, um auf diese Weise das Vertrauen in der Cloud-Beziehung zu stärken.

Soweit der Cloud-Anbieter nicht selbst sämtliche Leistungen erbringt, sondern diesbezüglich Subunternehmer in Anspruch nimmt, sind die vertraglichen Beziehungen in solchen Ketten zu klären.²⁸ Urheberrechtliche Nutzungsfragen sowie zu beachtende Regelungen im Kontext der Verwendung von Open-Source-Software bereiten beim Cloud-Computing keine grundlegenden Schwierigkeiten, soweit rechtliche Anforderungen beachtet werden.²⁹

16.4 Gestaltungsempfehlungen für Cloud-Verträge

Die Kosteneinsparung, die mit Hilfe von Cloud-Computing erreicht werden kann, verlangt eine aufwändige vertragliche Vorarbeit zwischen den Cloud-Akteuren, um die Risikoverteilung für einen möglichen Leistungsausfall und für eventuelle Schäden angemessen zu verteilen und dadurch die Wirtschaftlichkeit für beide Vertragsseiten sicherzustellen.

Soweit der Cloud-Vertrag individuell ausgehandelt wird, können die Vertragsparteien eine eigene Risikoverteilung vereinbaren. Da jedoch das Cloud-Computing auf einem Modell standardisierter IT-Bereitstellung beruht, bietet in der Regel der Cloud-Anbieter sowohl sein Cloud-Produkt als auch seine Vertragsbedingungen in Form von AGB an. Dabei unterliegt der Cloud-Anbieter den AGB-rechtlichen Anforderungen, die eine übermäßige Benachteiligung des Cloud-Nutzers verhindern. Gleichzeitig will der Cloud-Anbieter sein Cloud-Produkt erfolgreich vermarkten und kann durch faire vertragliche Standardlösungen das Vertrauen der Cloud-Nutzer fördern.

27 *Trusted Cloud, AG Rechtsrahmen* 2014a, 15 ff. und 20 ff.

28 S. Kapitel 15 zu den datenschutzrechtlichen Voraussetzung von Unteraufträgen.

29 S. dazu bereits *Trusted Cloud, AG Rechtsrahmen* 2012 und 2014b.

16.4.1 Anforderungen an einen Cloud-Vertrag

In einem Cloud-Vertrag³⁰ sollten, soweit keine individualvertraglichen Vereinbarungen vorliegen, folgende Inhalte unter Beachtung der AGB-rechtlichen Voraussetzungen enthalten sein:

- Vereinbarung zum anwendbaren Recht und Gerichtsstand
- vollständige, differenzierte und wirksame Leistungsbeschreibung
- Beendigung
 - Laufzeit
 - Kündigungsfristen
- Exit-Management (Rückabwicklung nach Vertragsende)
- Haftung
 - Haftungsbegrenzungen
 - Vertragsstrafen
 - pauschalierter Schadensersatz
- Change Management (Änderungsmöglichkeiten während der Vertragslaufzeit)
 - Preisanpassungsklauseln
 - Vertragsverlängerung

Zusätzlich sind folgende Regelungen in einem Cloud-Vertrag empfehlenswert:

- urheberrechtliche Nutzungsrechte (unter Berücksichtigung von Open-Source-Software)
- Vereinbarung über die Auftragsdatenverarbeitung
- Einsatz von Subauftragnehmern
- Geheimhaltungspflichten

30 S. hierzu ebenfalls die Checkliste zum Cloud-Vertrag in *Trusted Cloud, AG Rechtsrahmen* 2014a, 32 f.

- SLA
 - Verfügbarkeit
 - Entstörzeiten
 - Möglichkeiten der Minderung
 - Informationen über Erreichen der Verfügbarkeit
- branchenspezifische Vorgaben (beispielsweise bei Banken, Versicherungen und im Finanzsektor, Exportkontrollrecht oder Steuerrecht)
- Datensicherheit
- Kommunikationswege zwischen Cloud-Anbieter und Cloud-Nutzer

16.4.2 Empfehlungen an den Cloud-Anbieter

Auch soweit der Cloud-Anbieter die Ressourcen aus der Cloud unter Rückgriff auf seine AGB anbietet und dabei Standard-Angebote zur Verfügung stellt, hat er die Möglichkeit, den Cloud-Vertrag rechtsverträglicher zu gestalten.

So kann er die Anforderungen anerkennen, denen der Cloud-Nutzer – etwa als Angehöriger eines geheimhaltungspflichtigen freien Berufes – unterliegt, indem er im Cloud-Computing-Vertrag die Einhaltung anerkannter Sicherheitsstandards zusagt. Auch kann er dem Cloud-Nutzer helfen, bestimmte (datenschutz-)rechtlichen Vorgaben einzuhalten. Soweit der Cloud-Anbieter auf entsprechende Kunden-Anforderungen eingeht und diese beispielsweise vor Vertragsschluss abfragt und entsprechende Vertragsmodalitäten bereithält, kann er seine Vertrauenswürdigkeit und die Nutzung seines Cloud-Dienstes steigern. Beispiele hierfür können besondere Cloud-Angebote für Berufsheimnisträger wie Rechtsanwälte und Ärzte sein, die einem Strafbarkeitsrisiko gemäß § 203 StGB unterliegen,³¹ Angebote, die eine client-seitige Verschlüsselung der Daten vorsehen, oder die Bereitstellung eines Vertrages über die Auftragsdatenverarbeitung, dessen Abschluss grundsätzlich im Verantwortungsbereich des Cloud-Nutzers liegt.³²

31 S. Abschnitt 17.1.1.2.1 zur Strafbarkeit nach § 203 StGB.

32 S. Kapitel 15 zu den datenschutzrechtlichen Anforderung der Cloud-Nutzung.

16.5 Literaturverzeichnis

- BITCOM:** Cloud-Computing – Was Entscheider Wissen müssen, Berlin 2010.
- Duisberg, A.:** Gelöste und ungelöste Rechtsfragen im IT-Outsourcing und Cloud Computing. Hrsg.: Picot, A.; Hertz, U.; Götz, T., Heidelberg 2011, S. 49-71.
- Koch, F. A.:** Weltweit verteiltes Rechnen im Grid Computing. In: Computerrecht (CR) 2006, S. 52-50.
- Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“:** Leitfaden – Vertragsgestaltung beim Cloud Computing, 1. Auflage, Berlin 2014a.
- Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“:** Cloud Computing und Open Source Software, 1. Auflage, Berlin 2014b.
- Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“:** Lizenzierungsbedarf beim Cloud Computing – Welche Rechte zur Nutzung von Software benötigen Anbieter und Nutzer von Cloud Computing, 1. Auflage, Berlin 2012.
- Leupold, A.; Glossner, S.:** Münchener Anwaltsbuch für IT-Recht. 3. Auflage, München 2013.
- Niemann, f.; Paul, J.-A.:** Bewölkt oder wolkenlos – rechtliche Herausforderung des Cloud Computing, In: Kommunikation und Recht (K&Rn.), 2009, S. 444-452.
- Picot, A.; Hertz, U.; Götz, T.:** Trust in IT – Wann vertrauen Sie Ihr Geschäft der Internet-Cloud an?, Heidelberg 2011.
- Pohle, J.; Ammann, T.:** Über den Wolken... – Chancen und Risiken des Cloud Computing. In: Computerrecht (CR), 2009, S. 273-278.
- Schulz, C.; Rosenkranz, T.:** Cloud Computing – Bedarfsorientierte Nutzung von IT-Ressourcen, In: IT-Rechts-Berater (ITRB), 2009, S. 232-236.
- von dem Bussche, A.; Schelinski, T.:** IT-Vertragsgestaltung. Hrsg.: Leupold, A.; Glossner, S., München 2013.
- Wicker, M.:** Die Neuregelung des § 100j StPO auch beim Cloud Computing? Zugriff auf Zugangsdaten zur Cloud nach der neuen Bestandsdatenauskunft?. In: Multimedia und Recht (MMR), 2014, S. 298-302.
- Wicker, M.:** Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln. In: Multimedia und Recht (MMR), 2012, S. 783-788.

17 Strafrechtliche Risiken beim Cloud-Computing

S. Kroschwald, A. Roßnagel, M. Wicker

17.1 Einleitung

Cloud-Computing erhöht die Gefahr eines heimlichen und unerlaubten Zugriffs auf gespeicherte Daten, da die Daten nicht mehr lokal beim Nutzer gespeichert sind, sondern über externe Cloud-Server verwaltet werden, auf die ein Zugriff über das Internet grundsätzlich möglich ist. Die Nutzung der Cloud kann für den Cloud-Nutzer eine Strafbarkeit auslösen, weil die Sicherheitsmöglichkeiten in der Cloud geringer sind als auf lokalen Rechnern. Ebenso können die Bereitstellung oder der Umgang mit Daten in der Cloud für den Cloud-Anbieter eine Straftat darstellen, wenn er dadurch die Interessen des Cloud-Nutzers oder Betroffener verletzt.

Dabei handelt es sich teilweise um Strafbarkeitsrisiken, die sich unbeabsichtigt aus dem Charakter der Cloud ergeben, oder auch um strafrechtlich relevantes Verhalten, das durch die Cloud ermöglicht oder erleichtert wird. Um eine erlaubte Bereitstellung und Nutzung der Cloud-Angebote zu erreichen, muss zum einen das Risiko der Strafbarkeit bekannt sein,¹ zum anderen ist den Cloud-Akteuren eine Möglichkeit zur Vermeidung der Strafbarkeit an die Hand zu geben.²

1 S. Abschnitt 17.2 zur den Strafbarkeitsrisiken der Cloud-Akteure.

2 S. Abschnitt 17.4 zu den Gestaltungsempfehlungen für die Cloud-Akteure.

17.2 Strafrechtlich relevantes Verhalten der Cloud-Akteure

Das Strafrecht erfasst nur das Verhalten natürlicher Personen.³ Der Cloud-Nutzer und vor allem der Cloud-Anbieter sind jedoch meist juristische Personen. Strafbarkeitsrisiken bestehen daher insbesondere für die Verantwortlichen der juristischen Personen, wie den Geschäftsführer einer Gesellschaft mit beschränkter Haftung oder den Leiter einer Behörde, aber auch für einzelne Mitarbeiter der Cloud-Anbieter oder Cloud-Nutzer.

Einzelnen natürlichen Personen, die im privaten Kontext ein Angebot aus der Cloud in Anspruch nehmen, kann die eventuell strafrechtlich relevante Handlung eindeutig zugeordnet werden. Anders kann dies jedoch sein, wenn ein Unternehmen oder eine Behörde Angebote aus der Cloud nutzen. In diesem Fall können die Entscheidung über die Cloud-Nutzung und die tatsächliche Nutzung der Cloud personell auseinanderfallen. Zu denken ist hier an den Einsatz von Cloud-Computing in einem Unternehmen, der auf einer Entscheidung der Unternehmensleitung beruht. Der spätere Cloud-Nutzer, also ein Mitarbeiter im Unternehmen, hat die eingesetzte Informationstechnik nicht ausgewählt und greift nur auf die Angebote zurück, die ihm seitens der IT-Abteilung zur Verfügung gestellt werden. Darüber hinaus kann es auch vorkommen, dass Beschäftigte in einem Unternehmen ohne oder gegen den Willen des Arbeitsgebers Angebote aus der Cloud zur Erledigung ihrer Arbeit nutzen, beispielsweise weil diese ihnen praktisch erscheinen.

Im Strafrecht ist die Zurechnung von Kenntnissen, Tatbeiträgen und Absichten äußerst restriktiv vorzunehmen, so dass eine Strafbarkeit nur denjenigen treffen kann, der sämtliche Voraussetzungen in seiner Person verwirklicht. Dies bedeutet zum einen, dass fremde Handlungen kaum zugerechnet werden. Zum anderen kann jedoch die Billigung eines fremden Verhaltens im eigenen Verantwortungsbereich, ohne zumutbare Gegenmaßnahmen zu ergreifen, einen Straftatbestand erfüllen.

3 Fischer 2014, Vor § 13 StGB, Rn. 3.

17.3 Strafbarkeitsrisiken der Cloud-Akteure

Um die Nutzung und die Bereitstellung von Cloud-Angeboten zu fördern, ist sowohl für den Cloud-Anbieter als auch für den Cloud-Nutzer die Kenntnis der jeweils spezifischen Strafbarkeitsrisiken notwendig.

17.3.1 *Strafbarkeitsrisiko des Cloud-Nutzers*

Der Cloud-Nutzer unterliegt insbesondere dann einem Strafbarkeitsrisiko, wenn durch die Nutzung von Cloud-Angeboten das Risiko besteht, dass geheim zu haltende Inhalte von Unberechtigten wahrgenommen werden.

17.3.1.1 Berufsgeheimnisträger

Die Nutzung einer Cloud kann beispielsweise für Anwälte und Ärzte eine interessante Möglichkeit bieten, auf notwendige IT-Ressourcen einfach, kostengünstig und flexibel zuzugreifen.⁴ Berufsgeheimnisträger unterliegen jedoch dem strafrechtlichen Risiko der Verletzung von Privatgeheimnissen gemäß § 203 Abs. 1 StGB. Diese Vorschrift verbietet den in ihr genannten Berufsgeheimnisträgern Geheimnisse, die ihnen anvertraut worden sind, unbefugt zu offenbaren. Das besondere Vertrauensverhältnis beispielsweise zwischen Arzt und Patient oder Anwalt und Mandant schützt jede ihnen in dieser Funktion anvertraute oder bekannt gewordene Information.⁵

Die Tathandlung des § 203 StGB, das Offenbaren, wird durch den Cloud-Nutzer bereits dadurch verwirklicht, dass er dem Cloud-Anbieter ermöglicht, die Patienten- und Mandantengeheimnisse, die sich bei ihm in der Cloud befinden, zur Kenntnis zu nehmen.⁶

Verschiedene Ansätze, das Strafbarkeitsrisiko auszuräumen und Berufsgeheimnisträgern die Cloud-Nutzung zu ermöglichen, werden zwar diskutiert, sorgen jedoch nicht für ausreichende Rechtssicherheit.⁷ So wird beispielsweise der Cloud-Anbieter entsprechend § 203 Abs. 3 Satz 2 StGB als berufsmäßig tätiger Gehilfe, vergleichbar mit dem Kanzleipersonal oder

4 Härting, AnwBl 2012, 486.

5 Kroschwald/Wicker, in: Taeger 2012, 733 ff.

6 Fischer 2014, § 203 StGB, Rn. 30a, 30b.

7 So beispielsweise Conrad/Fechner, CR 2013, 137.

Sprechstundenhilfen, eingeordnet, um so eine strafbare Weitergabe von Geheimnissen auszuschließen.⁸ Die Behandlung des Cloud-Anbieters als Gehilfen des Cloud-Nutzers ist jedoch nicht möglich, da Hilfe nur sein kann, wer weisungsgebunden beim Berufsgeheimnisträger tätig ist.⁹ Der Cloud-Anbieter ist jedoch nicht beim Cloud-Nutzer abhängig beschäftigt.

Auch wird vertreten, dass beim Vorliegen einer Auftragsdatenverarbeitung nach § 11 BDSG eine Strafbarkeit nach § 203 StGB ausscheide, weil aufgrund der datenschutzrechtlichen Weisungsbedingung eine ausreichende Kontrolle des Cloud-Anbieters möglich sei.¹⁰ Auch dieses Argument überzeugt nicht, da das Strafrecht nicht mithilfe des Datenschutzrechts ausgelegt werden kann. Während das Datenschutzrecht nämlich den Schutz personenbezogener Daten vornimmt, schützt § 203 StGB darüber hinaus auch das besondere Vertrauensverhältnis zwischen dem Berufsgeheimnisträger und seinen Patienten und Mandanten.¹¹

Eine Zustimmung aller Patienten oder Mandaten zur Cloud-Nutzung kann eine Lösung hinsichtlich des Strafbarkeitsrisikos darstellen,¹² stößt aber auf praktische Grenzen.¹³ Deshalb ist eine gesetzliche Klarstellung zur strafrechtssicheren Nutzung von Cloud-Computing durch Berufsgeheimnisträger erforderlich.¹⁴

Der Cloud-Nutzer muss, um eine Strafbarkeit gemäß § 203 Abs. 1 StGB zu vermeiden, die Möglichkeit der Kenntnisnahme durch technische Sicherungsmechanismen wie beispielsweise Verschlüsselung verhindern. Dies ist jedoch bei der Verarbeitung von Daten in der Cloud (bis jetzt) nicht mög-

8 Kroschwald/Wicker, CR 2012, 758 ff.

9 Hoenike/Hülsdunk, MMR 2004, 788, 789.

10 Hartung, VersR 2012, 400, 409; s. hierzu auch Heghmanns/Niehaus, NStZ 2008, 57, 59 ff.; Hoenike/Hülsdunk, MMR 2004, 788, 791 f.; Jahn/Palm, AnwBl 2011, 613, 620; s. zum Cloud Computing Maisch/Seidl, DSB 2012, 127; ähnlich auch Giesen, NStZ 2012, 122, 127, der die externen Dienstleister entsprechend der Auftragsdatenverarbeitung der Stelle des Geheimnisträgers zuordnet.

11 Fischer 2014, § 203 StGB, Rn. 7.

12 Buchner, MedR 2013, 337 ff.

13 So auch Kroschwald/Wicker, DSB Newsletter 2014, 12 f. zur datenschutzrechtlichen Einwilligung.

14 So auch Härtling, AnwBl 2012, 486.

lich.¹⁵ Zumindest die Nutzung der Cloud als Backup-Speicher ist aber bereits heute straflos möglich, sofern die Daten nutzerseitig nach dem Stand von Wissenschaft und Technik verschlüsselt werden.¹⁶

17.3.2 Telekommunikationsdiensteanbieter

Ein weiteres Strafbarkeitsrisiko für Cloud-Nutzer kann aus der Verletzung des Fernmeldegeheimnisses gemäß § 206 StGB resultieren, soweit beispielsweise ein Telekommunikationsdiensteanbieter¹⁷ Angebote aus der Cloud zur Verwaltung seiner Kundendaten nutzt.

Gemäß § 206 Abs. 1 StGB macht sich strafbar, wer „unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt“. Inhaber oder Beschäftigte von Telekommunikationsunternehmen können sich bei der Cloud-Nutzung gemäß § 206 Abs. 1 StGB strafbar machen, soweit ihnen fernmeldegeheimnisrelevante Tatsachen ihrer Kunden – also Bestands- und Verkehrsdaten¹⁸ – persönlich tatsächlich bekannt geworden sind und sie diese zur Datenspeicherung unverschlüsselt in einer Cloud ablegen oder Angebote zur Datenverarbeitung in der Cloud in Anspruch nehmen.¹⁹

Dem Telekommunikationsgeheimnis können auch Arbeitgeber im Verhältnis zu ihren Mitarbeitern unterfallen, wenn sie beispielsweise eine Tele-

15 Kroschwald, ZD 2014, 75 ff.

16 Kroschwald, ZD 2014, 75 ff.

17 Zum Begriff des Telekommunikationsanbieters oder Access-Providers Ballhausen/Roggenkamp, in: Kilian/Heussen 2013, 1. Abschnitt, Teil 2, Providerverträge, Rn. 5; eine stets aktuelle Liste der meldepflichtigen Anbieter gemäß § 6 TKG, die gewerblich öffentliche Telekommunikationsnetze betreiben oder gewerblich öffentlich zugängliche Telekommunikationsdienste erbringen, stellt die Bundesnetzagentur zur Verfügung, http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/TKDiensteanbieterPDF.pdf?__blob=publicationFile&v=16.

18 Zu den Datenkategorien beim Cloud-Computing Boos/Kroschwald/Wicker, ZD 2013, 205.

19 Fischer 2014, § 206 StGB, Rn. 6 ff.

fonanlage betreiben, die Mitarbeiter auch zum privaten Gebrauch nutzen dürfen.²⁰ Insofern können auch die Bestands- und Verkehrsdaten aus dieser Telefonanlage dem Telekommunikationsgeheimnis unterliegen. Speichert ein Arbeitgeber diese Daten in einer Cloud oder verarbeitet er sie dort, kann er dadurch den Straftatbestand des § 206 Abs. 1 StGB erfüllen.²¹

17.3.3 Öffentliche Verwaltung

Soweit die öffentliche Verwaltung für ihre Datenverarbeitung oder die Speicherung Cloud-Angebote nutzen will, besteht ein Strafbarkeitsrisiko wegen der Verletzung des Dienstgeheimnisses gemäß § 353b StGB.²²

Dienstgeheimnisse²³ sind alle Informationen, die einem Amtsträger als private Geheimnisse oder Betriebs- und Geschäftsgeheimnisse bekannt geworden sind oder aufgrund einer Rechtsnorm einer Geheimhaltung bedürfen.²⁴ Beispiele für Geheimnisse im Sinne des § 353b StGB sind Informationen über einen Haftbefehl, die in den Fahrzeugregistern abgespeicherten Fahrzeug- und Halterdaten, Hinweise aus einem Computerausdruck mit polizeilichen Erkenntnissen über eine Person sowie eine Liste von zugelassenen Mitbewerbern bei einer behördlichen Ausschreibung an daran beteiligte Unternehmen.²⁵

Die Nutzung von Cloud-Angeboten kann das Tatbestandsmerkmal der Offenbarung erfüllen, wenn der Amtsträger die Daten, ohne sie zu verschlüsseln, an den Cloud-Anbieter überträgt, um sie dort zu speichern oder zu ver-

20 S. ausführlich Schuster, CR 2014, 21.

21 S. ausführlich dazu Vietmeyer/Byers, MMR 2010, 807.

22 Der von § 353b StGB Abs. 1 StGB neben der Tathandlung geforderte Erfolg ist die konkrete Gefahr eines Nachteils für wichtige öffentliche Interessen, insbesondere Nachteile bei behördlichen Verfahren durch die Kenntnis Dritter, Graf, in: Münchener Kommentar zum Strafgesetzbuch 2014, § 353b StGB, Rn. 38.

23 S. z.B. § 30 VwVfG.

24 Lackner, in: Lackner/Kühl 2014, § 353b StGB, Rn. 6; Graf, in: Münchener Kommentar zum Strafgesetzbuch 2014, § 353b StGB, Rn. 19 ff.

25 Graf, in: Münchener Kommentar zum Strafgesetzbuch 2014, § 353b StGB, Rn. 27 f.

arbeiten, da bereits die Möglichkeit der Kenntnis durch den Cloud-Anbieter genügt.²⁶

Nutzt eine Behörde Cloud-Angebote, kann fraglich sein, wer der eigentliche Täter ist. Als Täter kommen der von der Behörde beauftragte IT-Verantwortliche, der sachlich zuständige Amtsträger oder der Behördenleiter in Betracht.

Die Einwilligung des betroffenen Bürgers schließt zwar die Strafbarkeit aus. Sie einzuholen, ist jedoch selten praktikabel.

17.3.4 Verletzung des Steuergeheimnisses

Ein Amtsträger, der Steuerdaten unverschlüsselt in der Cloud speichert oder verarbeitet, kann sich wegen der Verletzung des Steuergeheimnisses gemäß § 355 StGB strafbar machen. Er offenbart diese Daten, indem er dem Cloud-Anbieter die Kenntnisnahme dieser Daten ermöglicht. Taugliche Täter können zum Beispiel Beamte der Bundes- und Landesfinanzbehörden oder hinzugezogene Sachverständige sein.²⁷ Steuerberater werden dagegen von § 203 Abs. 1 Nr. 3 StGB erfasst.²⁸

17.3.5 Verstoß gegen Datenschutzrecht

Der Cloud-Nutzer kann eine gemäß § 43 Abs. 2 in Verbindung mit § 44 BDSG strafbewehrte Tathandlung vornehmen, wenn er sich nicht datenschutzrechtskonform verhält, vor allem indem er ohne eine datenschutzrechtliche Erlaubnis Daten in die Cloud weitergibt. Tatobjekt des § 43 Abs. 2 Nr. 1 bis 4 BDSG sind „personenbezogene Daten, die nicht allgemein zugänglich sind“. Soweit der Cloud-Nutzer personenbezogene Daten in die Cloud überträgt, ohne die Voraussetzungen einer rechtmäßigen Übermittlung zu erfüllen,²⁹ liegt eine gemäß 28 Abs. 1 Satz 1 BDSG unbefugte Verarbeitung in der Form einer Datenübermittlung vor.

26 Kroschwald/Wicker, CR 2012, 758 ff.

27 Fischer 2014, § 355 StGB, Rn. 2-5a.

28 S. hierzu Abschnitt 17.2.2.1 für Berufsgeheimnisträger sowie Wortlaut des § 203 Abs. 1 Nr. 3 StGB.

29 S. Kapitel 15 zu den datenschutzrechtlichen Anforderungen an Cloud-Computing.

Die Tathandlungen stellen, soweit sie vorsätzlich oder fahrlässig begangen werden, zunächst nur eine Ordnungswidrigkeit nach § 43 Abs. 2 BDSG dar, die mit einem Bußgeld geahndet werden kann. Für eine Strafbarkeit nach §§ 43 Abs. 2, 44 BDSG ist zudem auch eine Schädigungsabsicht erforderlich. Die Tathandlung muss vorsätzlich sowie gegen Entgelt oder in der Absicht begangen werden, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

17.3.5.1 Computersabotage

Soweit ein Cloud-Nutzer die Funktionsfähigkeit des Cloud-Dienstes beeinträchtigt, besteht ein Strafbarkeitsrisiko wegen Computersabotage gemäß § 303b StGB. Geschützt ist das Interesse der Betreiber und anderer Nutzer an einem „störungsfreien Ablauf von Datenverarbeitungen“.³⁰ Durch die Strafbarkeit der Computersabotage soll die Verfügungsbefugnis und die Funktionsfähigkeit der Datenverarbeitungsanlagen sichergestellt werden.³¹

Der Begriff der Datenverarbeitungsanlage umfasst nicht nur einen einzelnen Datenverarbeitungsvorgang, sondern vielmehr den gesamten Umgang mit elektronisch gespeicherten Daten von ihrer Erhebung bis zu ihrer Verwendung.³² Somit stellt die Bereitstellung von Daten in der Cloud ebenso wie die Nutzung von Angeboten aus der Cloud eine Datenverarbeitung dar.

Der objektive Straftatbestand ist die Herbeiführung einer erheblichen Störung der Datenverarbeitungsanlage „Cloud“. Diesen kann der Cloud-Nutzer zum Beispiel dadurch erfüllen, dass er schadhafte Daten in die Cloud einbringt und dadurch – etwa durch den Absturz eines Cloud-Servers – den reibungslosen Ablauf nicht unerheblich beeinträchtigt.³³ Verursacht er dadurch einen Vermögensverlust großen Ausmaßes, kann der Richter wegen eines besonders schweren Falls sogar eine Strafverschärfung nach § 303b Abs. 4 StGB anordnen.

30 BT-Drs. 10/5058, 35.

31 Lackner, in: Lackner/Kühl 2014, § 303b StGB, Rn. 1.

32 Fischer 2014, § 303b StGB, Rn. 4 ff.

33 Fischer 2014, § 303b StGB, Rn. 9 ff.

17.3.5.2 Vorsätzliches Handeln

Alle genannten Straftatbestände führen gemäß § 15 StGB nur dann zur Strafbarkeit des Cloud-Nutzers, wenn dieser die Tatbestandsmerkmale vorsätzlich erfüllt. Dabei genügt es, dass er bewusst und gewollt die Daten in der Cloud speichert oder in der Cloud verarbeiten lässt.³⁴ Dass ihm die Funktionsweise des Cloud-Computing nicht bekannt ist und er sich daher keine Gedanken darüber gemacht hat, ob der Cloud-Anbieter auf die ungeschützten Daten zugreifen und diese zur Kenntnis nehmen kann, schließt eine vorsätzliche Tathandlung nicht aus.

17.3.6 Strafbarkeitsrisiko des Cloud-Anbieters

Der Cloud-Anbieter kann grundsätzlich durch zwei Verhaltensweisen Strafbarkeitsrisiken begründen. Erstens kann der Cloud-Anbieter seine faktische Möglichkeit unrechtmäßig ausnutzen, die Daten seiner Cloud-Nutzer zur Kenntnis zu nehmen. Zweitens kann er den Cloud-Nutzern den Zugriff auf ihre in seiner Cloud gespeicherten Daten vereiteln.

17.3.6.1 Ausspähen von Daten

Mitarbeiter des Cloud-Anbieters können sich wegen Ausspähens von Daten gemäß § 202a StGB strafbar machen, wenn sie ihre Zugangsmöglichkeiten zu den Daten missbrauchen. Rechtsgut der Vorschrift ist das Verfügungsrecht über die Daten.³⁵

Voraussetzung für die Tatbestandserfüllung ist jedoch, dass die Daten nicht für den Täter bestimmt³⁶ und gegen den unberechtigten Zugriff besonders gesichert sind.³⁷ Zwar können Mitarbeiter des Cloud-Anbieters – vergleichbar mit Netzwerkadministratoren bei einer lokalen Datenhaltung³⁸ –

34 Fischer 2014, § 15 StGB, Rn. 2 ff.

35 Im Zusammenhang mit dem Cloud-Computing Hilgendorf/Valerius 2012, Rn. 536.

36 Graf, in: Münchener Kommentar zum Strafgesetzbuch 2012, § 202a StGB, Rn. 19.

37 BGH, MMR 2010, 711.

38 Graf, in: Münchener Kommentar zum Strafgesetzbuch 2012, § 202a StGB, Rn. 43.

während des regulären Cloud-Betriebs auf die Daten ihrer Cloud-Kunden zugreifen. Erfolgt ein solcher Zugriff außerhalb der eigentlichen Dienstbereitstellung – also etwa nicht nur, wenn er für die Speicherung, die Verarbeitung oder Wartung tatsächlich erforderlich ist –, so stellt der Zugriff einen Missbrauch der Rechte dar.³⁹ Der Mitarbeiter handelt dann unbefugt. Er überwindet eine formale Schutzvorrichtung,⁴⁰ da der Zugriff auf die Daten durch eine Zugangssicherung geschützt ist. Fehlt diese, etwa bei Informationsportalen in einer Cloud, und können Dritte auf die Daten zugreifen, entfällt dieses Tatbestandsmerkmal und damit auch ein Strafbarkeitsrisiko.

Der Tatbestand des Ausspähens von Daten entfällt jedoch, wenn der Mitarbeiter befugt ist, auf die Daten zuzugreifen. Dies ist immer dann der Fall, wenn dieser Zugriff für das Erbringen oder die Aufrechterhaltung des Cloud-Angebots erforderlich ist. Muss beispielsweise der Cloud-Anbieter prüfen, ob die Cloud-Server nach einem Angriff funktionsfähig sind, missbraucht er seine Zugriffsrechte nicht. In solchen Konstellationen ist der Zugriff befugt und der Straftatbestand nicht erfüllt.⁴¹

17.3.6.2 Verstoß gegen Datenschutzrecht

Verarbeitet ein Mitarbeiter des Cloud-Anbieters unerlaubt personenbezogene Daten,⁴² die der Cloud-Nutzer in die Cloud gegeben hat, kann er dadurch nach § 43 Abs. 2 BDSG eine Ordnungswidrigkeit oder nach § 44 Abs. 1 BDSG sogar eine Straftat begehen.⁴³ Das Datenschutzrecht dient dem Schutz des Rechts auf informationelle Selbstbestimmung der Betroffenen aus

39 „Elektronischer Hausfriedensbruch“ nach Lenckner/Eisele, in: Schönke/Schröder 2014, § 202a StGB, Rn. 18.

40 Weidemann, in: Beck'scher Online-Kommentar StGB 2013, § 202a StGB, Rn. 17.

41 Das Abfangen von Daten nach § 202b StGB tritt als subsidiärer Tatbestand hinter § 202a StGB zurück. Spezielle Anknüpfungspunkte für den Straftatbestand des Vorbereitens, des Ausspähens oder Abfangens von Daten nach § 202c StGB ergeben sich beim Cloud-Computing nicht.

42 Tatobjekt des § 43 Abs. 2 Nr. 1 bis 4 BDSG sind „personenbezogene Daten, die nicht allgemein zugänglich sind“.

43 Dazu Hilgendorf/Valerius 2012, Rn. 734; vorab sind verschiedene Handlungen bereits gemäß § 43 BDSG bußgeldbewehrt.

Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.⁴⁴ Eine Erhebung besteht in jeder Aktivität, durch die er Kenntnis von den Daten erhält.⁴⁵ Eine Verarbeitung kann nach § 3 Abs. 4 BDSG in jeder Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung der Daten bestehen. Unbefugt ist die Erhebung oder Datenverarbeitung, wenn für sie weder ein datenschutzrechtlicher Erlaubnistatbestand noch eine Einwilligung vorliegen. An einem Erlaubnistatbestand fehlt es auch, wenn die Daten dem Cloud-Anbieter im Rahmen eines Vertrages zu einem bestimmten Zweck übertragen werden und er sie zu anderen Zwecken nutzt.⁴⁶ In diesem Fall begeht der Mitarbeiter des Cloud-Anbieters eine Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 5 BDSG.

Stellt ein Cloud-Anbieter fest, dass Mitarbeiter oder Dritte Daten aus der Cloud unrechtmäßig übermittelt oder auf sonstige Weise Kenntnis von diesen erlangt haben, und drohen schwerwiegende Beeinträchtigungen für die Rechte des Betroffenen oder für dessen schutzwürdige Interessen, ist er nach § 42a BDSG verpflichtet, sowohl den Betroffenen als auch die Aufsichtsbehörden darüber zu informieren. Unterlässt er diese Mitteilung, begeht er nach § 43 Abs. 2 Nr. 7 BDSG eine Ordnungswidrigkeit. Eine Interessenkollision wegen der Selbstoffenbarung einer Ordnungswidrigkeit besteht im Regelfall nicht, weil die Pflicht zur Offenbarung den gesetzlichen Vertreter des Cloud-Anbieters und nicht den Mitarbeiter, der die Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG begangen hat, trifft.⁴⁷

Nach § 44 Abs. 1 BDSG begeht eine Straftat, wer eine in § 43 Abs. 2 BDSG bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht. Ob die besonderen Absichten des § 44 BDSG im Zusammenhang mit dem Cloud-Computing vorliegen, bedarf einer Einzelfallprüfung. Die bloße Nutzung oder die Bereitstellung einer Cloud an sich indiziert allerdings keine entsprechenden Absichten der handelnden Akteure.

44 BVerfGE 65, 1, 42 ff.; s. Kapitel 15 zum Datenschutzrecht beim Cloud-Computing.

45 Dammann, in: Simitis 2014, § 3 BDSG, Rn. 102.

46 S. Kapitel 15 zur unzulässigen Zweckänderung.

47 S. ausführlich Dix, in: Simitis 2014, § 42a BDSG, Rn. 21.

17.3.6.3 Datenveränderung

Erschwert oder verhindert der Cloud-Anbieter dem Cloud-Nutzer rechtswidrig die Verbindung zu dessen Daten, kann er dadurch den Tatbestand der Datenunterdrückung gemäß § 303a StGB erfüllen. Das gleiche gilt, wenn er die Daten löscht, verändert oder unbrauchbar macht. Die Tathandlung des Unterdrückens ist erfüllt, wenn der Cloud-Anbieter dem Cloud-Nutzer den Zugang zu den Daten, die dieser in seiner Cloud gespeichert hat, für einen wesentlichen Zeitraum sperrt. Nur vorübergehende Störungen erfüllen nicht den Tatbestand.

Diese Vorschrift schützt die Verfügungsgewalt des Berechtigten über die gespeicherten Daten.⁴⁸ Der Cloud-Nutzer verwendet die Speicherkapazitäten auf den Cloud-Servern, die aus sachenrechtlicher Sicht dem Cloud-Anbieter oder einem Dritten gehören.⁴⁹ Aufgrund der vertraglichen Beziehung ist jedoch nur der Mieter des Speicherplatzes, also der Cloud-Nutzer, Verfügungsberechtigter an den Daten. Das Eigentum am Datenträger selbst spielt hierfür keine Rolle.⁵⁰ Die genannten Handlungen des Cloud-Anbieters sind daher im Regelfall rechtswidrig.

Erstellt der Cloud-Anbieter beispielsweise zum Zweck der Sicherung oder der schnelleren Verfügbarkeit Datenkopien und weichen diese nicht vom Original ab (Redundanzkopien), gilt das Original als mehrfach vorhanden.⁵¹ Soweit mindestens eine solche Kopie erhalten bleibt, ist der Tatbestand trotz der Löschung anderer Kopien nicht erfüllt und es besteht keine Strafbarkeit. Schadprogramme, die ein Cloud-Nutzer – absichtlich oder versehentlich – zum Speichern hochgeladen hat, kann der Cloud-Anbieter straflos löschen, um seine eigene Server-Struktur zu schützen.⁵²

Ob eine Sperrung des Zugangs zur Cloud, etwa weil der Nutzer das vertraglich fällige Entgelt nicht beglichen hat, oder das Löschen von Daten rechtswidrig ist, hängt von den vertraglichen Vereinbarungen ab. Vertrag-

48 Weidemann, in: Beck'scher Online-Kommentar StGB 2013, § 303a StGB, Rn. 2; Hilgendorf/Valerius 2012, Rn. 587

49 Weiler, in: Dölling/Duttge/Rössner 2013, § 303a StGB, Rn. 3.

50 Wieck-Noodt, in: Münchener Kommentar zum StGB 2014, § 303a StGB, Rn. 10.

51 Bär, in: Wabnitz/Janovsky 2007, 25. Kapitel, Rn. 41.

52 Heidrich/Tschoepe, MMR 2004, 75 ff.

liche Vereinbarungen, wonach sich der Cloud-Anbieter das Recht zur Sperrung bei vertragswidrigem Verhalten des Cloud-Nutzers oder zur Löschung von Daten nach Beendigung des Vertragsverhältnisses vorbehält, können daher eine Strafbarkeit verhindern.

17.3.6.4 Computersabotage

Die Strafbarkeit wegen Computersabotage nach § 303b StGB kann auch den Cloud-Anbieter treffen.⁵³ Geschützt ist das Interesse der Cloud-Nutzer an einem „störungsfreien Ablauf von Datenverarbeitungen“.⁵⁴ Die Nutzung von Cloud-Computing ist für den Cloud-Nutzer eine Datenverarbeitung von wesentlicher Bedeutung,⁵⁵ da die Cloud-Nutzung gerade dazu dient, Ressourcen nicht selbst vorzuhalten, sondern aus dem Internet zu beziehen. Der Cloud-Nutzer ist daher im Regelfall auf die Verfügbarkeit der Cloud angewiesen. Das gilt auch, wenn die Cloud nur als Backup genutzt wird.⁵⁶

Wird das Funktionieren des Cloud-Dienstes verhindert und kann der Cloud-Nutzer deshalb nicht auf seine Daten zugreifen, ist von einer erheblichen Störung der Datenverarbeitung gemäß § 303b StGB auszugehen.⁵⁷

Als Tatbestandshandlung sieht § 303b Abs. 1 StGB drei Alternativen vor. Die Funktionsstörung kann dadurch hervorgerufen werden, dass der Täter eine Zugangsverhinderung gemäß § 303a StGB herbeiführt. Sie kann auch dadurch ausgelöst werden, dass der Täter Daten⁵⁸ gemäß § 202a Abs. 2 StGB in der Absicht, einem anderen einen Nachteil zuzufügen,⁵⁹ eingibt oder übermittelt. Schließlich kann die verbotene Handlung auch darin bestehen,

53 S. zur Computersabotage durch den Cloud-Nutzer Abschnitt 17.2.1.6.

54 Hilgendorf/Valerius 2012, Rn. 600.

55 Wieck-Noodt, in: Münchener Kommentar zum StGB 2014, § 303b StGB, Rn. 6 ff.

56 Ernst, NJW 2007, 2661, 2664.

57 Weidemann, in: Beck'scher Online-Kommentar StGB 2013, § 303b StGB, Rn. 14.

58 Daten im Sinne von § 202a Abs. 2 StGB.

59 S. zum Vermögensnachteil Eisele, JURA 2012, 922, 933; Stree/Hecker, in: Schönke/Schröder 2014, § 303b StGB, Rn. 7.

dass der Täter die Datenverarbeitungsanlage⁶⁰ zerstört, beschädigt, unbrauchbar macht,⁶¹ beseitigt oder verändert.⁶²

Handelt es sich bei dem Geschädigten der Tat, also dem Cloud-Nutzer, um einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde,⁶³ erhöht sich gemäß § 303b Abs. 2 StGB das Strafmaß. Wird außerdem ein Vermögensverlust großen Ausmaßes⁶⁴ herbeigeführt, handelt es sich um einen besonders schweren Fall gemäß § 303b Abs. 4 StGB, der noch schärfer bestraft wird. Dies kann beim Cloud-Computing besonders relevant werden, wenn der Cloud-Nutzer sich hinsichtlich seiner Ressourcen überwiegend auf die Cloud verlässt.

17.3.6.5 Vorsätzliches Handeln

Die Straftatbestände erfordern gemäß § 15 StGB jeweils, dass der Täter vorsätzlich handelt. Hierfür genügt bedingter Vorsatz. Es genügt also, wenn der Täter den kriminellen Erfolg seiner Tat in Kauf genommen hat.⁶⁵ Da die verschiedenen Merkmale, wie „von wesentlicher Bedeutung“ und „erhebliche Störung“ aber eine umfassende Kenntnis des Täters über Wirkungen und Zusammenhänge der Bedeutung und der Wirkung seiner Tat erfordern, bedarf es einer genauen Prüfung, ob der Täter sämtliche notwendigen Tatbestandsmerkmale kannte oder überhaupt kennen konnte.

60 Zaczyk, in: Kindhäuser/Neumann/Paeffgen 2013, § 303b, Rn. 11a.

61 Fischer 2014, § 303b StGB, Rn. 12 mit weiteren Erläuterungen zu DDoS (distributed Denial-of-Service) -Attacken.

62 Fischer 2014, § 303b StGB, Rn. 13.

63 Weidemann, in: Beck'scher Online-Kommentar StGB, § 303b StGB, Rn. 20.

64 Allgemein zum Vermögensverlust großen Ausmaßes (einschließlich Gewinnausfall) s. auch Fischer 2014, § 263 StGB, Rn. 215 ff.

65 Fischer 2014, § 15 StGB, Rn. 2 ff.

17.4 Praktische Relevanz der Strafbarkeitsrisiken

Die praktische Relevanz der dargestellten Strafbarkeitsrisiken ist gering. Dennoch hemmt das aktuelle, wenn auch nur theoretische Risiko einer Strafbarkeit die Nutzung von Cloud-Angeboten – insbesondere durch Berufsgeheimnisträger oder die Verwaltung.

Die geringe praktische Relevanz ist zum einen darauf zurückzuführen, dass die meisten der dargestellten Straftaten nur bei einem Strafantrag des Betroffenen verfolgt werden können.⁶⁶ Selbst soweit die Staatsanwaltschaft auch von sich aus tätig werden könnte, wird das hierfür erforderliche öffentliche Interesse an der Strafverfolgung nicht angenommen, wenn kein Strafantrag gestellt wird.⁶⁷ Zum anderen folgt die geringe praktische Relevanz aus der Tatsache, dass das Opfer – also der Cloud-Nutzer oder der betroffene Dritte – meist überhaupt nicht in Erfahrung bringen kann, dass die Straftat verübt worden ist. Teilweise besteht keine Kenntnis über die Cloud-Nutzung. Schließlich ist den Betroffenen nicht bewusst, dass die Handlung strafbewehrt ist. Seitens des Cloud-Nutzers ist beispielsweise häufig unklar, dass eine ungerechtfertigte Zugangsverhinderung oder ein erheblicher Datenverlust eine Straftat darstellen können. Insbesondere bei kostenlosen Angeboten wird der Cloud-Nutzer meist nicht davon ausgehen, dass ein unredliches Verhalten seines Vertragspartners strafrechtlich von Belang sein könnte.

66 Der Verrat von Privatgeheimnissen gemäß § 203 StGB und das Ausspähen von Daten gemäß § 202a StGB werden gemäß § 205 Abs. 1 StGB nur auf Antrag verfolgt; Straftaten gemäß § 355 Abs. 1 StGB werden gemäß Absatz 3 nur auf Antrag des Dienstvorgesetzten oder des Verletzten verfolgt; auch datenschutzrechtliche Straftaten werden nur auf Antrag gemäß § 44 Abs. 2 Satz 1 BDSG verfolgt; ebenso sind die Straftaten gemäß §§ 303a und 303b StGB von einem Strafantrag gemäß § 303c StGB abhängig, bei der öffentlichen Verwaltung bedarf es sogar einer besonderen Ermächtigung gemäß § 353b Abs. 4 StGB.

67 So z.B. im Datenschutzstrafrecht, Ehmann, in: Simitis 2014, § 44 BDSG, Rn. 9.

17.5 Gestaltungsempfehlung für die Cloud-Akteure

Für den Cloud-Nutzer und den Cloud-Anbieter bestehen Risiken einer Strafbarkeit bei der Nutzung beziehungsweise bei der Bereitstellung von Cloud-Computing. Um die Nutzung und das Vertrauen in die Möglichkeiten des Cloud-Computing zu fördern, ist es erforderlich, zum einen die Cloud-Akteure auf die Risiken der Strafbarkeit hinzuweisen und zum anderen das Angebot und seine Nutzung auch strafrechtskonform zu gestalten.

17.5.1 Gestaltungsempfehlungen für Cloud-Nutzer

Unter Berücksichtigung der im Folgenden genannten Gestaltungsempfehlungen kann der Cloud-Nutzer Angebote aus der Cloud in Anspruch nehmen, ohne strafrechtliche Konsequenzen befürchten zu müssen.

17.5.1.1 Zur Geheimhaltung besonders Verpflichtete

Die Strafbarkeitsrisiken für den Cloud-Nutzer liegen insbesondere in der Nutzung von Cloud-Angeboten zur Speicherung von Daten oder zur Verarbeitung von Daten in der Cloud, wenn der Cloud-Nutzer aufgrund besonderer Pflichten zur Geheimhaltung der Inhalte verpflichtet ist.

Durch die Nutzung von Cloud-Computing können die Mitglieder besonderer Berufsgruppen die Tathandlung begehen, die darin besteht, einem Unberechtigten die Kenntnisnahme geheimhaltungsbedürftiger Daten zu ermöglichen. Dies gilt nach § 203 StGB für Berufsgeheimnisträger wie Ärzte, Rechtsanwälte oder Steuerberater und deren Gehilfen, nach § 206 StGB für Telekommunikationsdiensteanbieter,⁶⁸ nach § 353b StGB für Mitarbeiter in der öffentlichen Verwaltung und nach § 355 StGB für Amtsträger in der Steuerverwaltung.

Um diesem Strafbarkeitsrisiko zu begegnen, sollte der Cloud-Nutzer nur verschlüsselte Daten in der Cloud speichern oder bei der Datenverarbeitung in der Cloud besondere Sicherheitskonzepte wählen, die trotz der unverschlüsselten Datenverarbeitung sicherstellen können, dass keine Stelle – auch

68 Dies können auch Arbeitgeber sein, die ihren Mitarbeitern die private Nutzung ihrer Telekommunikationsanlage erlauben.

nicht Mitarbeiter des Cloud-Anbieters – den Inhalt der Daten und damit potenzielle Geheimnisse zur Kenntnis nehmen können.⁶⁹

17.5.1.2 Datenschutzrechtlich verantwortliche Stellen

Wer personenbezogene Daten ohne Einwilligung oder Erlaubnistatbestand in die Cloud überträgt, begeht eine Ordnungswidrigkeit gemäß § 43 Abs. 2 BDSG. Wer dies in der von § 44 Abs. 1 BDSG geforderten Absicht tut, begeht einen Straftatbestand. Daher ist dringend zu empfehlen, die datenschutzrechtlichen Vorgaben zur Cloud-Nutzung einzuhalten.⁷⁰

17.5.1.3 Gewährleistung der gebotenen Sicherheit

Die letzte Möglichkeit einer Strafbarkeit des Cloud-Nutzers bezieht sich – anders als die zuvor genannten strafbewehrten Verhaltensweisen – nicht auf den Umgang mit Daten Dritter, sondern betrifft das Verhältnis zwischen Cloud-Nutzer und Cloud-Anbieter. Soweit der Cloud-Nutzer mit seinem Verhalten den Cloud-Anbieter schädigt, indem er die Datenverarbeitung des Cloud-Anbieters stört, unterliegt er einem Strafbarkeitsrisiko der Computersabotage gemäß § 303b StGB.

Da nur die vorsätzliche Schädigung strafbewehrt ist, muss der Cloud-Nutzer vor allem bewusste und gewollte schädigende Handlungen unterlassen. Um darüber hinaus zu verhindern, dass davon ausgegangen werden kann, der Cloud-Nutzer habe einen Schaden beim Cloud-Anbieter billigend in Kauf genommen und damit bedingt vorsätzlich gehandelt, ist dem Cloud-Nutzer zu empfehlen, Sicherheitsmaßnahmen, wie beispielsweise aktuelle Anti-Virus-Software und Software-Updates, zu nutzen.

17.5.2 Gestaltungsempfehlung für Cloud-Anbieter

Der Cloud-Anbieter kann einen enormen Reputationsverlust erleiden, wenn Informationen über sein mögliches strafrechtlich relevantes Verhalten bekannt werden, deshalb muss er jedes strafrechtliche Risiko vermeiden.

69 S. hierzu das Konzept des Trusted-Cloud-Projekts „Sealed Cloud“, hierzu auch Kroschwald, in: Taeger 2013, 301 ff.

70 S. Kapitel 15 zu den datenschutzrechtlichen Anforderungen.

17.5.2.1 Keine Kenntnisnahme der Daten

Soweit der Cloud-Anbieter Daten, die ein Cloud-Nutzer in seiner Cloud speichert oder verarbeitet, unbefugt zur Kenntnis nimmt,⁷¹ besteht das Risiko einer Strafbarkeit wegen Ausspähens von Daten nach § 202a StGB. Wenn er personenbezogene Daten unbefugt für sich verwendet, begeht er eine Ordnungswidrigkeit nach § 43 Abs. 2 BDSG wegen datenschutzrechtlich unzulässiger Verarbeitung von personenbezogenen Daten. Soweit er dabei eine Bereicherungs- oder Schädigungsabsicht hat, kann er nach §§ 44 StGB eine Straftat begehen. Der Cloud-Anbieter sollte daher, um keinem entsprechenden Risiko zu unterliegen, jede Kenntnisnahme der Dateninhalte des Cloud-Nutzers vermeiden. Zudem sollte er dem Nutzer empfehlen, gespeicherte Daten nutzerseitig zu verschlüsseln, und sich selbst technisch von der Möglichkeit der Kenntnisnahme der gespeicherten Daten ausschließen.⁷²

17.5.2.2 Cloud-Anbieter schadet dem Cloud-Nutzer

Ein weiteres Strafbarkeitsrisiko kann für den Cloud-Anbieter gemäß § 303a StGB oder § 303b StGB dann entstehen, wenn er dem Cloud-Nutzer die Nutzung der Cloud vorsätzlich vereitelt. Der Cloud-Anbieter, der zwar das Risiko einer Strafbarkeit ausschließen, jedoch auch eine gewisse Flexibilität seines Angebotes bewahren will, sollte daher vertragliche Vereinbarungen über die Datenlöschung und Zugangsverhinderung treffen und Veränderungen des Cloud-Angebotes rechtzeitig kommunizieren oder gar mit dem Cloud-Nutzer abstimmen.

17.5.3 Unterstützung zur Vermeidung der Strafbarkeit

Die aufgezeigten Risiken der Strafbarkeit knüpfen stets an eine vorsätzliche Handlung der Cloud-Akteure an. Daher sind die strafrechtlichen Folgen beim Cloud-Computing grundsätzlich vermeidbar. Eine Cloud-Unterstützung sollte den Cloud-Nutzer und den Cloud-Anbieter über ihre möglichen Strafbar-

71 Big-Data-Analysen oder „Verkauf“ von verschiedenen Daten für Marketing-Zwecke.

72 S. hierzu das Konzept des Trusted-Cloud-Projekts „Sealed Cloud“, hierzu auch Kroschwald, in: Taeger 2013, 301 ff.

keitsrisiken aufklären und ihnen die Möglichkeiten zur Vermeidung aufzeigen. Da der Cloud-Anbieter gegenüber einem potenziellen Cloud-Nutzer im Regelfall über mehr technisches und sogar rechtliches Wissen verfügt, kann auch der Cloud-Anbieter seine neuen Kunden über mögliche Risiken einer Strafbarkeit vorab informieren und Vermeidungsstrategien wie die Verschlüsselung anregen und damit zur Rechtsverträglichkeit des Cloud-Computing beitragen.

17.6 Literaturverzeichnis

- Boos, C.; Kroschwald, S.; Wicker, M.:** Datenschutz bei Cloud Computing zwischen TKG, TMG und BDSG – Datenkategorien bei der Nutzung von Cloud Diensten. In: Zeitschrift für Datenschutz (ZD), 2013, S. 205-210.
- Buchner, B.:** Outsourcing in der Arztpraxis – zwischen Datenschutz und Schweigepflicht. In: Medizinrecht (MedR), 2013, S. 337-342.
- Conrad, I.; Fechtner, S.:** IT-Outsourcing durch Anwaltskanzleien nach der Inkasso-Entscheidung des EuGH und dem BGH, Urteil vom 7.2.2013. In: Computerrecht (CR), 2013, S. 137-148.
- Dölling, D.; Duttge, G.; Rössner, D.:** Gesamtes Strafrecht StGB – StPO, Nebengesetze. 3. Auflage, Baden-Baden 2013.
- Eisele, J.:** Der Kernbereich des Computerstrafrechts. In: Juristische Ausbildung (Jura), 2012, S. 922-934.
- Ernst, S.:** Das neue Computerstrafrecht. In: Neue Juristische Wochenschrift (NJW), 2007, S. 2661-2666.
- Fischer, T.:** Strafgesetzbuch mit Nebengesetzen. 61. Auflage, München 2014.
- Geppert, M.; Schütz, R.:** Beck'scher TKG-Kommentar. 4. Auflage, München 2013.
- Giesen, T.:** Zum Begriff des Offenbarens nach § 203 StGB im Falle der Einschaltung privatärztlicher Verrechnungsstellen. In: Neue Zeitschrift für Strafrecht (NStZ), 2012, S. 122-128.
- Graf, J. P.:** Beck'scher Onlinekommentar StGB. Edition 23, München 2013.
- Hartung, J.:** Datenschutz und Verschwiegenheit bei Auslagerung durch Versicherungsunternehmen. In: Versicherungsrecht (VersR), 2012, S. 400-410.
- Härting, N.:** Anwalt in der Wolke: Realität, Berufsethos, Rechtssicherheit, Plädoyer für eine Lösung im Bereich des Strafrechts. In: Anwaltsblatt (AnwBl), 2012, S. 486.
- Heghmanns, M.; Niehaus, H.:** Outsourcing im Versicherungswesen und der Gehilfenbegriff des § 203 III 2 StGB. In: Neue Zeitschrift für Strafrecht (NStZ), 2008, S. 57-62.
- Heidrich, J.; Tschoepe, S.:** Rechtsprobleme der E-Mail-Filterung. In: Multimedia und Recht (MMR), 2004, S. 75-80.
- Hilgendorf, E.; Valerius, B.:** Computer- und Internetstrafrecht – Ein Grundriss. 2. Auflage, Berlin 2012.

- Hoenike, M.; Hülsdunk, L.:** Outsourcing im Versicherungs- und Gesundheitswesen ohne Einwilligung?. In: Multimedia und Recht (MMR), 2004, S. 788-792.
- Jahn, M.; Palm, J.:** Outsourcing in der Kanzlei: Verletzung von Privatgeheimnissen?. In: Anwaltsblatt (AnwBl), 2001, S. 613-621.
- Joecks, W.; Miebach, K.:** Münchener Kommentar zum StGB. Band 4, 2. Auflage, München 2012.
- Joecks, W.; Miebach, K.:** Münchener Kommentar zum StGB. Band 5, 2. Auflage, München 2014.
- Kilian, W.; Heussen, B.:** Computerrechtshandbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis. 23. Ergänzungslieferung, München 2013.
- Kindhäuser, U.; Neumann, U.; Paeffgen, H-U.:** Strafgesetzbuch. 4. Auflage, Baden-Baden 2013.
- Klasen, E.:** Whistleblower, Zeuge und „Beschuldigter“ – Informationsweitergabe im Spannungsfeld grundrechtlicher Positionen. In: Betriebs-Berater (BB), 2012, S. 641-647.
- Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“:** Ein rechtspolitisches Thesepapier der AG Rechtsrahmen des Cloud Computing. 1. Auflage, Berlin 2012.
- Kroschwald, S.:** Verschlüsseltes Cloud Computing – Anwendung des Daten- und Geheimnisschutzrechts auf „betriebssichere“ Clouds am Beispiel der „Sealed Cloud“. Hrsg.: Taeger, J., Edewecht 2013, Band. 1, S. 981-1000.
- Kroschwald, S.:** Verschlüsseltes Cloud Computing – Auswirkungen der Kryptografie auf den Personenbezug in der Cloud. In: Zeitschrift für Datenschutz (ZD), 2014, S. 75-80.
- Kroschwald, S.; Wicker, M.:** Einwilligung des Betroffenen in den Umgang mit seinen Daten als Lösung für das Cloud Computing. In: Datenschutzberater (DSB), Newsletter zum 15. Euroforum Datenschutzkongress 2014, S. 12-13.
- Kroschwald, S.; Wicker, M.:** Kanzleien und Praxen in der Cloud – Strafbarkeit nach § 203 StGB. In: Computerrecht (CR), 2012, S. 758-764.
- Kroschwald, S.; Wicker, M.:** Zulässigkeit von Cloud Computing für Berufsgeheimnisträger: Strafbarkeit von Anwälten und Ärzten durch die Cloud? Hrsg.: Taeger, J., Edewecht 2012, S. 733-758.
- Lackner, K.; Kühl, K.:** Strafgesetzbuch. 28. Auflage, München 2011.
- Lagodny, O.:** Münchener Kommentar zum Strafgesetzbuch. Band 5, 2. Auflage, München 2014.
- Maisch, M. M.; Seidl, A.:** Cloud-Nutzung für Berufsgeheimnisträger – § 203 StGB als „Showstopper“?. In: Datenschutzberater (DSB), 2012, S. 127-129.
- Schönke, A.; Schröder, H.:** Strafgesetzbuch. 29. Auflage, München 2014.
- Schuster, F.:** Der Arbeitgeber und das Telekommunikationsgesetz. In: Computerrecht (CR) 2014, S. 21-27.
- Simitis, S.:** Bundesdatenschutzgesetz. 8. Auflage, Baden- Baden 2014.
- Taeger, J.:** IT und Internet – mit Recht gestalten: Tagungsband Herbstakademie 2012. Edewecht 2012.

- Taeger, J.:** Law as a Service – Recht im Internet- und Cloud-Zeitalter: Tagungsband Herbstakademie 2013. Edeweicht 2013.
- Vietmeyer, K.; Byers, P.:** Der Arbeitgeber als TK-Anbieter im Arbeitsverhältnis Geplante BDSG-Novelle lässt Anwendbarkeit des TKG im Arbeitsverhältnis unangetastet. In: Multimedia und Recht (MMR), 2010, S. 807-811.
- Wabnitz, H.-B.; Janovsky, T.:** Handbuch des Wirtschafts- und Steuerstrafrechts. 3. Auflage 2010, München 2007.
- Wicker, M.:** Die Neuregelung des § 100j StPO auch beim Cloud Computing? Zugriff auf Zugangsdaten zur Cloud nach der neuen Bestandsdatenauskunft?. In: Multimedia und Recht (MMR), 2014, S. 298-302.
- Wicker, M.:** Durchsuchung in der Cloud Nutzung von Cloud-Speichern und der straf- prozessuale Zugriff deutscher Ermittlungsbehörden. In: Multimedia und Recht (MMR), 2013, S. 765-769.

18 Staatliche Zugriffe auf Daten in der Cloud

S. Kroschwald, A. Roßnagel, M. Wicker

18.1 Einleitung

Wenn Daten nicht mehr lokal gespeichert, sondern hierfür Angebote aus der Cloud genutzt werden, ist die Wahrscheinlichkeit eines Zugriffs auf diese Daten durch Dritte im Vergleich zu einer rein lokalen Datenhaltung regelmäßig erhöht. Darüber hinaus sind auch die Datenwege nicht immer transparent, mögliche Zugriffe lassen sich unbemerkt durchführen. Schließlich erhöht die Speicherung umfassender Datenmengen im Vergleich zur nicht-digitalen, lokalen Lagerung von Daten die Möglichkeiten der schnellen Recherche, der (Raster-)Selektion und der Zusammenführung von Daten. Dies gilt insbesondere auch für den staatlichen Zugriff auf in der Cloud gespeicherte Daten durch Ermittlungsbehörden im Strafverfahren.

Solche Zugriffe können erfolgen, um Straftaten, die für die Cloud-Nutzung typisch sind,¹ zu verfolgen, aber auch zur Aufklärung von Straftaten, die an sich keine Verbindung zum Cloud-Computing aufweisen. In beiden Fällen können Nachweise zur ermittlungsrelevanten Tat möglicherweise in der Cloud zu finden sein. Zu denken ist beispielsweise an Zugriffe auf Daten in einem Steuerstrafverfahren gegen einen Cloud-Nutzer, der seine ermittlungsrelevanten Buchhaltungsunterlagen in der Cloud speichert und verarbeitet.

Angesichts der Möglichkeiten eines staatlichen Zugriffs können die beteiligten Cloud-Nutzer vor der Inanspruchnahme von Cloud-Angeboten zurückschrecken, insbesondere wenn hinsichtlich der Pflichten und Befugnisse Unklarheit und Intransparenz herrscht. Eine Anwenderunterstützung kann diesem Informationsdefizit unter Umständen entgegenwirken. Ein Cloud-Nutzer, der IT-Ressourcen aus der Cloud mieten will,² steht insbesondere vor den Fragen, inwiefern er mit einem staatlichen Zugriff auf seine Daten in der

1 S. zu den Strafbarkeitsrisiken der Cloud-Akteure Kapitel 17.

2 Wicker, MMR 2013, 783.

Cloud rechnen muss³ und ob die Risiken eines staatlichen Zugriffs gegenüber der lokalen Speicherung erhöht sind.⁴ Für den Cloud-Anbieter ist es wichtig zu wissen, welchen Verpflichtungen zur Kooperation mit den Ermittlungsbehörden er unterliegt⁵ und durch welches Verhalten er das Vertrauen des Cloud-Nutzers in sein Cloud-Angebot stärken kann.⁶

18.2 Grundlagen der Ermittlungsmaßnahmen

Für Ermittlungsmaßnahmen im Zusammenhang mit Straftaten finden sich die Ermächtigungsgrundlagen in der Strafprozessordnung. Bei Verdacht einer Straftat sind die Staatsanwaltschaft und als ihr Hilfsorgan die Polizei gemäß § 152 Abs. 1 StPO befugt, Ermittlungen durchzuführen. Die Polizei nimmt dabei häufig eine Doppelrolle ein. Zum einen ist es ihre Aufgabe, Gefahren und Straftaten zu verhindern – sie handelt dann präventiv, beispielsweise auf Grundlage der Landespolizeigesetze.⁷ Es ist jedoch gemäß § 161 Abs. 1 Satz 1 StPO zum anderen auch Aufgabe der Polizei, die Staatsanwaltschaft bei der Verfolgung von Straftaten zu unterstützen.

Gemäß § 160 Abs. 2 StPO ist die Staatsanwaltschaft als Leiterin des Ermittlungsverfahrens verpflichtet, „nicht nur die zur Belastung, sondern auch die zur Entlastung dienenden Umstände zu ermitteln“. Ermittlungen, insbesondere wenn sie den Verdacht einer Straftat nicht bestätigen, kollidieren regelmäßig mit den Grundrechten der von den Ermittlungen betroffenen Personen. Um das Interesse an einer effektiven Strafverfolgung auf der einen Seite und den Grundrechtsschutz auf der anderen Seite ausreichend zu wahren, bedürfen daher alle Handlungen von Ermittlungsbehörden einer Ermächtigungsgrundlage.

3 S. zu den Zugriffen gegenüber dem Cloud-Nutzer Abschnitt 18.1.2.

4 S. zu den Zugriffen auf Daten des Cloud-Nutzers beim Cloud-Anbieter Abschnitt 18.2.2.

5 S hierzu Abschnitt 18.2.2.1 und 18.2.2.3.

6 S. zu den Gestaltungsempfehlungen an den Cloud-Anbieter Abschnitt 18.3.2.

7 Germann 2000, 183 ff. bereits mit Bezug zum Internet.

18.2.1 Ermittlungen von Straftaten

Gemäß §§ 161 und 163 StPO sind die Ermittlungsbehörden berechtigt, verschiedene Ermittlungsmaßnahmen durchzuführen. Beispiele sind Auskunftsanfragen bei Behörden, die Verwendung von offenkundigen Informationen oder die Untersuchung eines Tatortes.⁸ Maßnahmen, die darüber hinausgehen und eine Person stärker betreffen, bedürfen dagegen einer speziellen Ermächtigungsgrundlage. Diese sind an weitere Voraussetzungen – insbesondere die Entscheidung eines Richters – geknüpft. Beispiele hierfür sind die Durchsuchung von Wohnungen gemäß §§ 102 ff. StPO oder das Abhören des Telefons gemäß §§ 100a ff. StPO. Wird bei Ermittlungen etwas herausgefunden, wodurch der Verdacht der Straftat belegt oder widerlegt werden kann, sind die entsprechenden Beweismittel gemäß §§ 94 ff. StPO zu beschlagnahmen, damit sie in einem späteren gerichtlichen Prozess verwendet werden können.

Bei allen Maßnahmen muss der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit gewahrt werden, um die effektive Strafverfolgung und die betroffenen Grundrechte angemessen in Einklang zu bringen.⁹ Daher ist stets zu entscheiden, ob eine Maßnahme für die Strafverfolgung von derartiger Wichtigkeit ist, dass der Eingriff in die Rechte der Person hinzunehmen ist. Insbesondere bei Daten, die – anders als etwa ein Tatmesser – vervielfältigt werden können, kann beispielsweise die Kopie der Daten eine mildere Maßnahme sein, als die Mitnahme einer Festplatte.

18.2.2 Daten als Beweismittel

Nach der Strafprozessordnung können Beweismittel grundsätzlich nur Sachen in Form von körperlichen Gegenständen sein.¹⁰ Soweit sich beweis-erhebliche Informationen auf Speichermedien befinden, ist das Beweismittel im Sinne der Strafprozessordnung folglich das Speichermedium selbst. Die Polizei ermittelt bezogen auf Daten in der Regel so, dass sie zunächst im

8 Schmitt, in: Meyer-Goßner/Schmitt 2014, § 161 StPO, Rn. 1a ff.; § 163 StPO, Rn. 28.

9 Schmitt, in: Meyer-Goßner/Schmitt 2014, Einl., Rn. 20.

10 Sachen werden im Strafprozess in Augenschein genommen, weitere Beweismittel sind vor allem Zeugen, Sachverständige und Urkunden sowie Aussagen des Beschuldigten.

Rahmen einer Durchsuchung gemäß §§ 102 ff. StPO die vorhandenen Daten nach so genannten „beweiserheblichen Daten“ durchsieht.¹¹ Bereits zu diesem Zeitpunkt kann sie Speichermedien, auf denen sich digitale Daten befinden, zur Durchsicht von den Ermittlungsbehörden gemäß § 110 StPO mitnehmen.

Ermittelt die Polizei in der Cloud, kann sie jedoch nicht ganze Cloud-Server zur Durchsicht gemäß § 110 StPO im Rahmen der Durchsuchung gemäß §§ 102 ff. StPO mitnehmen. Dadurch würde sie auch die Cloud-Nutzung für andere Nutzer behindern. Da die Erstellung einer Kopie von digitalen Daten eine Vervielfältigung des Originals darstellt, genügt für Ermittlungen die Kopie auf einem weiteren Speichermedium. Ein weitergehender Eingriff in die geschützten Rechte der Betroffenen wäre unverhältnismäßig.¹²

Finden die Ermittlungsbehörden im Rahmen der Durchsicht der kopierten Daten sodann ermittlungsrelevante Daten, erfolgt eine Beschlagnahme dieser beweiserheblichen Daten gemäß §§ 94 ff. StPO. Auch hinsichtlich der Beschlagnahme gilt, dass zur Wahrung der Verhältnismäßigkeit der Ermittlungshandlung nach Möglichkeit auf die Beschlagnahme der Hardware zu verzichten und eine Kopie der Daten zu beschlagnahmen ist. Haben die Ermittlungsbehörden bereits vorher im Rahmen der Durchsuchung gemäß §§ 102 ff. StPO Datenkopien zur Durchsicht mitgenommen, sind im Rahmen der Beschlagnahme die nicht ermittlungsrelevanten Daten zu löschen.¹³ Inwieweit der Beweiswert von Daten verschlechtert wird, weil diese nicht mehr auf dem ursprünglichen Speichermedium als Beweismittel vorliegen, sondern nur noch eine Kopie der Daten auf einem weiteren Medium vorhanden ist, können die Ermittlungsbehörden durch das Verfahren der Erstellung der Kopie entscheidend beeinflussen.¹⁴

11 Wicker, MMR 2013, 765.

12 BVerfGE 124, 43.

13 BVerfGE 113, 29.

14 BSI-Leitfaden 2011, 13 ff.

Für Cloud-Anbieter bedeutet dies, dass sie bei Ermittlungen gegen Cloud-Nutzer nicht befürchten müssen, dass ihr Cloud-Angebot lahmgelegt wird.¹⁵ Da der Verhältnismäßigkeitsgrundsatz zu beachten ist, müssen sich Ermittlungsbehörden im Regelfall mit Kopien der Daten begnügen.¹⁶

18.2.3 Heimliche Maßnahmen in der Strafprozessordnung

Cloud-Computing ermöglicht zumindest faktisch heimliche Maßnahmen der Ermittlungsbehörden. Die Ermittlungsbehörden könnten ohne Kenntnis des Cloud-Nutzers seine Daten mithilfe des Cloud-Anbieters zur Kenntnis nehmen. Auch wenn der Ermittlungserfolg wahrscheinlich höher ausfallen würde, wenn Ermittlungen bei dem Verdacht einer Straftat heimlich durchgeführt würden, muss zum Schutz der Grundrechte die von den Ermittlungen betroffene Person informiert werden, soweit durch die Benachrichtigung der Erfolg der Ermittlungen nicht völlig entfallen würde. Daher hat auf der einen Seite der Wohnungsbesitzer, dessen Wohnung gemäß § 102 StPO durchsucht wird, gemäß § 106 StPO das Recht, dabei anwesend zu sein. Auf der anderen Seite liefe eine Telekommunikationsüberwachung gemäß §§ 100a ff. StPO völlig ins Leere, wenn die betroffene Person bereits vorher wüsste, dass die Ermittlungsbehörden nunmehr ihr Telefon überwachen. Hier darf auf die Benachrichtigung sinnvollerweise verzichtet werden.

Grundsätzlich verlangt also der Grundsatz der Verhältnismäßigkeit, dass Ermittlungen offen erfolgen, solange ihre Heimlichkeit für den Erfolg der Ermittlungen nicht erforderlich ist. Daraus folgt, dass soweit sich Ermittlungen auf Beweismittel beziehen, die bereits existieren, wie beispielsweise Unterlagen oder gespeicherte Daten, die strafprozessuale Maßnahme offen erfolgen muss. Sollen die Ermittlungen dagegen erst noch entstehende Tatsachen als Beweismittel verfügbar machen, wie beispielsweise bei der Überwachung der künftigen Telefongespräche, ist die Heimlichkeit gerechtfertigt.

15 Kolb/Birk/Wegener, BSI-Tagungsband 2013, 189, die einen Fall in den USA aus dem Jahr 2005 schildern, in dem das FBI sämtliche Cloud-Server eines Cloud-Anbieters beschlagnahmt hat, obwohl sich die Ermittlungen nur gegen einen Cloud-Nutzer richteten.

16 BVerfG, NJW 2007, 3343 bezugnehmend auf verschiedene Betroffene einer Maßnahme.

Die Strafprozessordnung ermöglicht demnach keinen heimlichen Zugriff auf bereits bestehende Daten.¹⁷ Nur die künftige Überwachung der Kommunikation zwischen zwei oder mehreren Kommunikationspartnern ist gemäß §§ 100a ff. StPO heimlich zulässig.

Für Cloud-Computing, insbesondere für die Speicherung von Daten in der Cloud, bedeutet dies, dass gegenüber der betroffenen Person, also beispielsweise einem verdächtigen Cloud-Nutzer, in Bezug auf seine Daten keine heimlichen Maßnahmen erfolgen dürfen. Dies gilt unabhängig davon, wo tatsächlich der Zugriff auf die Daten erfolgt – beim Cloud-Nutzer oder beim Cloud-Anbieter.

18.3 Zugriffe gegenüber dem Cloud-Nutzer

Richtet sich eine strafprozessuale Ermittlung gegen den Cloud-Nutzer, weil beispielsweise der Verdacht einer Steuerhinterziehung oder Urheberrechtsverletzung besteht, und ist davon auszugehen, dass der Cloud-Nutzer über Informationen, die seine Tat beweisen könnten, in Form von digital gespeicherten Daten verfügt, müssen die Ermittlungsbehörden primär beim Cloud-Nutzer nach Beweisen suchen.

18.3.1 Ablauf der Ermittlungen

Gehen die Ermittlungsbehörden davon aus, dass der Verdächtige über Daten verfügt, die tatsächlich als Beweismittel für die zu ermittelnde Tat dienen können, ist für eine Suche danach zunächst eine Durchsuchungsanordnung gemäß §§ 102 und 105 StPO beim Ermittlungsrichter zu beantragen. Diese wird meist zusammen mit einer Beschlagnahmeanordnung gemäß §§ 94 und 98 StPO für den Fall erteilt, dass die Durchsuchung erfolgreich ist und Beweismittel gefunden und beschlagnahmt werden können. Handlungen, die sich auf eine Durchsuchungs- oder Beschlagnahmeanordnung stützen, dürfen gegenüber den Betroffenen – also dem Cloud-Nutzer – nicht heimlich erfol-

17 BGHSt 51, 211.

gen.¹⁸ Daher ist spätestens im Zeitpunkt der Suche in Daten oder der Beschlagnahme von Daten der Cloud-Nutzer zu benachrichtigen.¹⁹

Bevor jedoch innerhalb der Daten gesucht werden kann oder gar beweiserhebliche Daten „zu den Akten genommen“ werden, müssen die Ermittlungsbehörden erst einmal an die Daten gelangen. Dies ist bei Cloud-Computing auf mehreren Wegen möglich. Da es sich einerseits um Daten des Cloud-Nutzers handelt²⁰ und diese Daten andererseits aber auf dem beim Cloud-Anbieter gemieteten Speicherplatz gespeichert sind, ist faktisch sowohl ein Zugriff beim Cloud-Nutzer als auch beim Cloud-Anbieter möglich. Denkbar ist auch ein Zugriff auf die Daten während der Datenübertragung zwischen dem Cloud-Nutzer und der Cloud.

18.3.2 Zugriff am Ort des Cloud-Anbieters

Da die Daten beim Cloud-Anbieter gespeichert sind, ist ein Zugriff dort faktisch möglich. Der Cloud-Speicher stellt einen geschützten Raum des Cloud-Nutzers dar – vergleichbar mit einem Hotelzimmer, das sich eine Person mietet und an dem diese Person möglicherweise beweiserhebliche Informationen lagert.²¹ Soweit die Ermittlungsbehörden nach den Vorschriften der Strafprozessordnung in einem Hotelzimmer des Verdächtigen ermitteln dürfen, gilt dies auch für Ermittlung in den vom Cloud-Nutzer gemieteten „Cloud-Räumen“. Die Ermittlungsbehörden können verschiedene Maßnahmen beim Cloud-Anbieter durchführen.

18.3.2.1 Auskunft nach Bestandsdaten beim Cloud-Anbieter

Zunächst können Ermittlungsbehörden beim Cloud-Anbieter Auskunft über die Bestandsdaten des Cloud-Nutzers verlangen. Gemäß §§ 161 Abs. 1 Satz 1 und 163 Abs. 1 StPO in Verbindung mit § 14 Abs. 2 TMG ist die Auskunft über Bestandsdaten beim Cloud-Anbieter als Anbieter von Tele-

18 Aus dem in § 106 StPO normierten Anwesenheitsrecht ergibt sich zwingend, dass die Durchsuchung dem Betroffenen mitgeteilt werden muss.

19 Schmitt, in: Meyer-Goßner/Schmitt 2014, § 106 StPO, Rn. 2 f.

20 Wicker, MMR 2013, 765.

21 Schmitt, in: Meyer-Goßner/Schmitt 2014, § 102 StPO, Rn. 7.

medien²² möglich. Bestandsdaten nach dem Telemediengesetz sind unter anderem der Benutzername und das Passwort. Gemäß § 14 Abs. 2 TMG „darf der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung [...] erforderlich ist“. Im Rahmen der Ermittlungen könnten die Behörden daher versuchen, durch die Bestandsdatenauskunft den Benutzernamen und das Passwort des Cloud-Nutzers zu erforschen, und sich so Zugang zum Cloud-Bereich des von den Ermittlungen betroffenen Cloud-Nutzers verschaffen.

Häufig verfügt jedoch der Cloud-Anbieter nicht über das Passwort seiner Cloud-Nutzer im Klartext. Vielmehr ist das Passwort, das vom Cloud-Nutzer beim Anlegen des Accounts ausgewählt wurde, meist nur als Hashwert gespeichert.²³ In der Praxis ist daher diese Ermittlungsmöglichkeit nicht mit viel Erfolg verbunden. Auch ist diese Ermittlungsmaßnahme nicht zwingend dem verdächtigen Cloud-Nutzer mitzuteilen, da sonst der Ermittlungserfolg meist ins Leere liefe, wenn der Cloud-Nutzer seine Daten umgehend löschen oder das Passwort ändern würde, nachdem ihm Ermittlungen gegen ihn selbst bekannt geworden sind. Es kann daher auch angebracht sein, den betroffenen Cloud-Nutzer noch nicht gemäß § 163a Abs. 1 Satz 1 StPO zu vernehmen, um ihn zu diesem Zeitpunkt noch nicht über gegen ihn laufende Ermittlungen zu informieren.²⁴ Der spätere Zugriff auf die Inhalte der Daten mit Hilfe der gewonnenen Zugangsdaten stellt jedoch eine weitere Maßnahme dar, deren Heimlichkeit nicht gerechtfertigt ist.

Wenn die Ermittlungsbehörden durch die Bestandsdatenauskunft mangels Passwort im Klartext keinen Zugriff auf die Cloud erhalten können, verbleibt die Möglichkeit weiterer Maßnahmen – beispielsweise über den Cloud-Anbieter eine Kopie der Daten des einen Cloud-Nutzers anzufordern.

18.3.2.2 Gast-Account

Wenden sich die Ermittlungsbehörden an den Cloud-Anbieter unter Vorlage entsprechender gerichtlicher Anordnungen gemäß §§ 102 ff. StPO und

22 Boos/Kroschwald/Wicker, ZD 2013, 205.

23 BR-Drs. 664/1/12, 14.

24 Schmitt, in: Meyer-Goßner/Schmitt 2014, § 161 StPO, Rn. 8.

§§ 94 ff. StPO bezüglich der Daten, kann der Cloud-Anbieter auf verschiedene Weise reagieren. Der Cloud-Anbieter hat meist technisch die Möglichkeit, auf die Daten des Cloud-Nutzers zuzugreifen. Selbst wenn er nicht über das (zuvor angefragte) Passwort im Klartext verfügt, besteht für ihn die tatsächliche Möglichkeit, die Daten zu kopieren oder für die Strafverfolgungsbehörden einen so genannten „Gast-Account“ einzurichten, der den Ermittlern den gleichen Zugriff zu den gleichen Daten ermöglicht, wie dem betroffenen Cloud-Nutzer selbst.²⁵

Dabei ist der Cloud-Anbieter keinesfalls zur Erstellung eines Gast-Accounts verpflichtet. Der Grund für solche überobligatorische Zusammenarbeit der (Cloud-)Anbieter ist meist die Befürchtung, dass die Ermittlungsbehörden ansonsten den Betrieb behindern, im schlimmsten Fall einen ganzen Cloud-Server „lahmlegen“.²⁶ Dadurch gibt er im Regelfall den Ermittlungsbehörden jedoch mehr Daten preis, als von den Ermittlungsvorschriften oder den gerichtlichen Entscheidungen umfasst sind. Soweit es keine gesetzliche Erlaubnis oder eine Einwilligung gibt, ist die Eröffnung eines Zugangs datenschutzrechtlich eine unbefugte Übermittlung und folglich unzulässig und nach § 43 Abs. 2 BDSG als Ordnungswidrigkeit zu verfolgen.²⁷

Haben die Ermittlungsbehörden einen solchen Gast-Account erhalten, müssen sie zwar den Cloud-Nutzer nicht sofort über die Möglichkeit ihres entstandenen Zugangs informieren. Dies entspricht auch dem Ergebnis einer erfolgreichen Bestandsdatenauskunft.²⁸ Die Ermittlungsbehörden müssen in einem solchen Fall jedoch die Offenheit einer anschließenden Durchsuchung innerhalb der Daten sicherstellen, indem sie den Cloud-Nutzer über ihre Nutzung des Gast-Accounts informieren.²⁹ Außerdem dürfen sie nicht über die gerichtliche Anordnung hinaus ermitteln, auch wenn dies im Rahmen der dann bestehenden Möglichkeiten des eigenen Gast-Accounts äußerst verführerisch erscheint. Werden bei solchen ausgeweiteten Ermittlungen weitere Beweismittel für zusätzliche Straftaten gefunden, dürfen sich die Strafverfol-

25 Kelnhofer/Nadeborn, StV 2011, 352.

26 Kolb/Birk/Wegener, BSI-Tagungsband 2013, 189.

27 S. zu den datenschutzrechtlichen Problemen des Cloud-Computing Kapitel 15.

28 S. zur Bestandsdatenauskunft Abschnitt 18.2.2.1.

29 S. zu den Grundlagen des Ermittlungsverfahrens Abschnitt 18.1.

gungsbehörden nicht auf einen Zufallsfund gemäß § 108 StPO stützen, denn es fand eine zielgerichtete Suche innerhalb von weiteren Informationen und kein zufälliger Fund innerhalb der zu durchsuchenden Daten statt.³⁰

Nicht alle Cloud-Anbieter handeln jedoch derart überobligatorisch, viel häufiger ist eine andere Vorgehensweise zwischen dem Cloud-Anbieter und den Ermittlungsbehörden.

18.3.2.3 Kopie der Daten durch den Cloud-Anbieter

Die Ermittlungsbehörden können den Cloud-Anbieter im Rahmen der Ermittlungen auch aufsuchen. Diese Situation ist vergleichbar mit der Durchsuchung eines angemieteten Hotelzimmers: Der Hotelier ist in diesem Fall verpflichtet, den Zugang zu dem Zimmer zu ermöglichen, damit die Ermittlungsbehörden es durchsuchen können.

Müssen die Ermittlungsbehörden auf den Servern des Cloud-Anbieters selbst die Daten des Cloud-Nutzers suchen, liegt eine Durchsuchung bei Dritten gemäß § 103 StPO vor.³¹ Soweit jedoch der Cloud-Anbieter die Daten selbst vom Server lädt und an die Ermittlungsbehörden weitergibt, wird beim Cloud-Anbieter selbst nicht gesucht.³² Der Cloud-Anbieter handelt dann vielmehr unter Befolgung der Herausgabepflicht aus § 95 Abs. 1 StPO. Die Norm verpflichtet jeden, der einen beweiserheblichen Gegenstand im Gewahrsam hat, zur Herausgabe, damit anschließend eine Durchsuchung beim Cloud-Nutzer gemäß § 102 StPO erfolgen kann.

Daher muss der Cloud-Anbieter eine Kopie der Daten erstellen oder einem IT-Forensiker der Ermittlungsbehörden die Möglichkeit verschaffen, selbst Kopien der Daten des jeweiligen Cloud-Nutzers zu erstellen. Die Pflicht zur Zusammenstellung von Daten aus einer größeren Menge gespeicherter Daten beruht „auf einer vertretbaren Auslegung des §§ 95 StPO“. ³³ Das Verlangen, nach § 95 Abs. 1 StPO nach konkreten Kriterien zusammengestellte Einzeldaten in Kopie herauszugeben, ist ein milderer Mittel gegen-

30 So auch Kelnhofer/Nadeborn, StV 2011, 352, 353; a.A. LG Mannheim, StV 2011, 532.

31 Wicker, MMR 2013, 765.

32 Wicker, in: Taeger 2013, 981, 993 f.

33 BVerfG, NStZ-RR 2003, 176, 177.

über der Beschlagnahme der Originaldatenträger mit umfangreichem Datenbestand und daher nach dem Grundsatz der Verhältnismäßigkeit gegenüber dem Cloud-Anbieter geboten.³⁴

Im Anschluss an die Kopieerstellung kann dann die Suche „innerhalb“ der Daten des Cloud-Nutzers gemäß § 102 StPO erfolgen. Da während der Erstellung der Datenkopie die Ermittlungsbehörden noch keine Kenntnis von den Dateninhalten nehmen, müssen weder unabhängige Zeugen gemäß § 105 Abs. 2 StPO hinzugezogen werden, noch muss der von der Maßnahme Betroffene nach § 106 StPO beiwohnen können.

18.3.3 Zugriffe am Ort des Cloud-Nutzers

Befinden sich die Daten ausschließlich in der Cloud und ist keine lokale Datensicherung beim Cloud-Nutzer vorhanden, müssen die Ermittlungen in der Cloud vorgenommen werden. Diese Daten befinden sich im Internet, sie sind auf einem Cloud-Server gespeichert und können über das Internet abgerufen werden. Obwohl es selbst für den Cloud-Anbieter ohne eine genaue Prüfung schwer ist zu bestimmen, wo die Daten zu einem bestimmten Zeitpunkt „liegen“, ist allerdings ein Zugriff auf die Daten sowohl für den Cloud-Nutzer als auch für den Cloud-Anbieter über den entsprechenden Zugang möglich. Der Zugriff am Ort des Cloud-Nutzers auf die Daten ist dann die einzige Möglichkeit der Ermittlung, wenn der Cloud-Anbieter keine Niederlassung in Deutschland hat.³⁵

Sind den Ermittlungsbehörden Zugangsdaten zur Cloud bekannt – beispielsweise weil der Cloud-Nutzer diese freiwillig mitteilt³⁶ oder weil die Auskunft nach Bestandsdaten beim Cloud-Anbieter erfolgreich war –, können sie gemäß § 102 StPO am Endgerät des Cloud-Nutzers über den Nutzer-Account seine Cloud durchsuchen.³⁷ Es handelt sich insofern um eine Durchsuchung beim Beschuldigten, da die Daten dem beschuldigten Cloud-Nutzer

34 BVerfG, NStZ-RR 2003, 176, 177.

35 Ein ausländischer Cloud-Anbieter kann nicht gemäß § 95 Abs. 1 StPO zur Erstellung einer Kopie verpflichtet werden.

36 Eine Motivation zur Mitteilung der Zugangsdaten kann für den Cloud-Nutzer die Erwartung einer geringeren Strafe im Fall der Geständigkeit sein.

37 Wicker, MMR 2013, 765.

„gehören“.³⁸ Die für eine Durchsuchung beim Cloud-Nutzer erforderliche Durchsuchungsanordnung gemäß § 106 StPO ist dem Cloud-Nutzer gleichzeitig mitzuteilen.³⁹ Werden beweiserhebliche Daten gefunden, kann eine Kopie aus der Cloud auf einem Speichermedium erstellt und die Datenauswahl gemäß § 94 StPO beschlagnahmt werden.⁴⁰

Im Rahmen der Durchsuchung gemäß § 102 StPO ist die Vorschrift des § 110 Abs. 3 StPO zu beachten, die Verfahrenshinweise für eine Durchsuchung enthält. Durchsuchen die Ermittlungsbehörden am Ort des Cloud-Nutzers und nehmen sie davon Kenntnis, dass der Verdächtige auch oder ausschließlich Daten in der Cloud speichert, wird eine Durchsuchung des Cloud-Inhalts als „entferntes Speichermedium“ davon abhängen, ob der „Verlust der gesuchten Daten“ zu befürchten ist. Dies ist regelmäßig der Fall: Soweit der Cloud-Nutzer nämlich aufgrund der Durchsuchung weiß, dass ein Zugriff auf seine Daten in der Cloud nunmehr erfolgen wird, wird er die Daten in der Cloud umgehend löschen, sobald er hierzu die Gelegenheit erhält. Verlassen also die Ermittlungsbeamten seine Wohnung, um beispielsweise beim Cloud-Anbieter, wo die Daten tatsächlich gespeichert sind, die Daten zu beschlagnahmen, wird er seinen Account „aufräumen“. Daher darf im Rahmen einer Durchsuchung beim Verdächtigen stets auch auf die räumlich entfernten Speichermedien wie Cloud-Speicher zugegriffen werden.

Eine Ermittlung vom Endgerät des Cloud-Nutzers aus ist auch möglich, wenn sich der Cloud-Server und damit die Daten im Ausland befinden.⁴¹ Zwar müssen die Ermittlungsbehörden die Souveränität anderer Staaten achten und dürfen dort nicht ermitteln.⁴² Greifen sie auf den Cloud-Speicher zu, können sie jedoch nicht bestimmen, wo sich die Daten befinden.⁴³ Ein willkürlicher Zugriff ins Ausland, der die Souveränität des anderen Staates an-

38 A. A. Brodowski/Eisenmenger, ZD 2014, 119.

39 S. zum Grundsatz der Offenheit von strafprozessualen Ermittlungen Abschnitt 18.1.1.

40 S. zu Daten als Beweismittel Abschnitt 18.1.2.

41 Wicker, in: Taeger 2013, 981.

42 S. dazu ausführlich Gercke, StraFo 2009, 271.

43 Schmitt, in: Meyer-Goßner 2014, § 110 StPO, Rn. 7b.

greifen würde, findet nicht statt. Die Tatsache, dass ein Zugriff für den verdächtigen Cloud-Nutzer und für die Ermittlungsbehörden jederzeit vom Gerät des Verdächtigen möglich ist, steht der Tatsache gegenüber, dass beim Cloud-Computing Daten häufig in hoher Frequenz ihren Speicherort entsprechend der aktuellen Lastverteilung verändern. Ein möglicherweise erfolgreiches Rechtshilfeersuchen bei einem anderen Staat im Sinne der Cybercrime-Konvention würde bei einem sich unvermittelt ändernden Speicherort wieder obsolet.⁴⁴ Daher ist davon auszugehen, dass ein Zugriff auf räumlich getrennte Speichermedien in der Cloud im Sinne von § 110 Abs. 3 StPO fremde Staatssouveränität nicht umgeht. Daher ist ein Zugriff unabhängig vom jeweiligen Speicherort beim Cloud-Computing zulässig.⁴⁵

Befinden sich folglich die Ermittlungsbehörden beim Cloud-Nutzer vor Ort, können sie als offene Maßnahme eine Durchsuchung am Endgerät des Cloud-Nutzers nach §§ 102, 110 StPO mit der anschließenden Beschlagnahme der potenziell beweiserheblichen Daten nach § 94 StPO in der Cloud durchführen. Anschließend ist hierüber auch der Cloud-Anbieter zu informieren.⁴⁶

18.3.4 Heimliche Zugriffe von entfernten Orten

Grundsätzlich versprechen Ermittlungen den größten Erfolg, wenn sie heimlich erfolgen. Insofern wäre es für die Ermittlungen hilfreich, wenn sich Ermittlungsbehörden von einem anderem Ort – also nicht am Endgerät des Cloud-Nutzers und auch nicht beim Cloud-Anbieter – heimlich in die Cloud des Nutzers „hacken“ und so Zugriff auf die in der Cloud gespeicherten und verarbeiteten Daten erhalten könnten. Im Urteil zum so genannten „Staats-trojaner“ hat der Bundesgerichtshof aber festgestellt, dass solche heimlichen Maßnahmen nicht auf die Strafprozessordnung gestützt werden können.⁴⁷ Ein Zugriff auf die Cloud muss offen erfolgen.⁴⁸ Nur die Abfrage der Zugangs-

44 Birk/Heinson/Wegener, DuD 2011, 329 ff.

45 Wicker, MMR 2013, 765, 768 f.; Schmitt: in: Meyer-Goßner/Schmitt 2014, § 110 StPO, Rn. 7b.

46 So schon Warntjen 2007, 196 ff. ohne Bezug zum Cloud-Computing.

47 BGH, MMR 2007, 237.

48 Für E-Mails Meinicke 2013, 68 f.

daten beim Cloud-Anbieter kann aufgrund kriminalistischer Erwägungen ohne Information des verdächtigen Cloud-Nutzers erfolgen. Hierbei dürfen aber noch keine Inhaltsdaten heimlich zur Kenntnis genommen werden.⁴⁹

18.3.5 Zugriffe auf die Datenübertragung

Vergleichbar mit dem Abhören von Telefongesprächen wäre beim Cloud-Computing auch ein Zugriff während des Up- oder Downloads der Daten technisch denkbar. Gemäß §§ 100a ff. StPO könnte ein solcher Zugriff als Telekommunikationsüberwachung zulässig sein. Allerdings lassen sich diese Vorschriften nicht auf den Fall des Cloud-Computing anwenden. Anders als etwa bei einem Telefongespräch fehlt dem Cloud-Nutzer bei der Datenübertragung der erforderliche Kommunikationswille.⁵⁰ Zwar erfolgt technisch bei der Datenübertragung in die Cloud nichts anderes als bei der Versendung einer E-Mail. Während jedoch der E-Mail-Absender die Nachricht eindeutig mit dem Ziel auf den Weg bringt, dass deren Inhalte vom Empfänger zur Kenntnis genommen werden, will der Cloud-Nutzer seine Dateninhalte lediglich an einem externen Ort speichern. Es kann daher beim Cloud-Computing nicht von gezielter Kommunikation die Rede sein. Die Regelungen des § 100a StPO finden daher auf die Datenübertragung in und aus der Cloud keine Anwendung und rechtfertigen daher auch keinen Zugriff auf den Up- und Download der Daten.⁵¹ Ebenso wie die Überwachung von Selbstgesprächen im Rahmen der Wohnraumüberwachung nach §§ 100c ff. StPO⁵² ist auch die Überwachung des Datenverkehrs in und aus der Cloud strafprozessual unzulässig.

18.3.6 Untersuchung der Daten aus der Cloud

Soweit den Ermittlungsbehörden Daten aus der Cloud vorliegen oder sie Zugang zu Daten in der Cloud haben, können die Ermittlungen in den Daten

49 Dalby, CR 2013, 361, 368.

50 Braun, jurisPR-ITR 22/2013 Anm. 2.

51 Bär, in: KMR-Kommentar StPO 2013, § 100j StPO, Rn. 16.

52 Schmitt, in: Meyer-Goßner/Schmitt 2014, § 100c StPO, Rn. 16.

mit dem Ziel, Beweise hinsichtlich des zu Grunde liegenden Straftatenverdachts zu finden, stattfinden.

18.3.6.1 Ermittlungen innerhalb der Daten des Cloud-Nutzers

Wenn die Ermittlungsbehörden eine Kopie des Cloud-Speichers vom Cloud-Anbieter erhalten oder sich Zugriff über den Anschluss des Cloud-Nutzers verschafft haben, kann eine Suche nach Beweismitteln beginnen. Gemäß § 102 StPO kann dann innerhalb des Datenbestandes gesucht werden.⁵³ Dabei ist auch die Verfahrensvorschrift des § 110 Abs. 1 StPO⁵⁴ zu berücksichtigen. Nach § 110 Abs. 1 StPO steht die Durchsicht der Papiere des von der Durchsuchung Betroffenen nur der Staatsanwaltschaft zu.⁵⁵ Unter Papieren sind außer Schriftstücken auch digitale Daten zu verstehen.⁵⁶

Erst wenn die Inhalte „durchforstet“ werden, beginnt die Maßnahme nach § 102 StPO und der Cloud-Nutzer darf dieser Durchsuchung nach § 106 Abs. 1 Satz 1 StPO beiwohnen. Die Vorschrift des § 110 StPO enthält kein ausdrückliches Recht des Inhabers von Papieren zur Anwesenheit während der Durchsicht mehr.⁵⁷ „Gleichwohl kann es zur Sicherung der Verhältnismäßigkeit des Eingriffs im Einzelfall geboten sein, den Inhaber des jeweiligen Datenbestands in die Prüfung der Verfahrenserheblichkeit sichergestellter Daten einzubeziehen.“⁵⁸ Die praktische Umsetzung der Teilhabe des Cloud-Nutzers während der gesamten Durchsicht, die durchaus mehr als sechs Monate in Anspruch nehmen kann,⁵⁹ muss in jedem Einzelfall „unter

53 Wicker, MMR 2013, 765.

54 § 110 Abs. 3 StPO findet hier keine Anwendung, da gerade nicht an einem räumlich entfernten Speicherplatz gesucht wird, s. Abschnitt 18.2.3 zu Ermittlungen am Ort des Cloud-Nutzers.

55 Die Befugnis kann nur auf Anordnung der Staatsanwalt auch den sonstigen Ermittlungsbehörden übertragen werden.

56 Statt vieler Bruns, in: Karlsruher Kommentar StPO 2013, § 110 StPO, Rn. 2; dies gilt insbesondere auch für E-Mails auf dem E-Mailserver des Providers, BVerfG, NJW 2009, 2431.

57 § 110 Abs. 3 StPO a.F. enthielt die Regelung, dass der Inhaber der Papiere oder sein Vertreter ein Anwesenheitsrecht bei der Durchsicht hatten.

58 Hegmann, in: Beck'scher Online-Kommentar StPO 2013, § 110 StPO, Rn. 11.

59 Hartmann, in: Dölling/Dutge/Rössner 2013, § 110 StPO, Rn. 10.

Berücksichtigung einer wirksamen Strafverfolgung einerseits und der Intensität des Datenzugriffs andererseits“ beurteilt werden.⁶⁰

18.3.6.2 Auffinden von Beweismitteln

Finden sich innerhalb der Daten des Cloud-Nutzers dann Daten, die als Beweismittel dienen können, müssen diese Beweismittel gesichert werden. Gemäß § 94 Abs. 1 und 2 StPO findet eine formlose Sicherstellung oder, im Falle der Verweigerung der Herausgabe, die förmliche Beschlagnahme statt.⁶¹ Diese erfolgt bei Daten in der Regel durch eine Kopie der Daten auf einem Speichermedium der Ermittlungsbehörden.⁶²

Haben die Ermittlungsbehörden im Rahmen der Durchsuchung bereits Daten zum Zwecke der Durchsicht kopiert, so erfolgt die Beschlagnahme, indem die kopierten Daten, die nicht als Beweismittel gebraucht werden, gelöscht werden.⁶³ Insbesondere werden dabei beispielsweise Dokumente und Daten, die den Kernbereich privater Lebensgestaltung betreffen, gelöscht.⁶⁴ Die übrigen Daten gelten dann als beschlagnahmt oder sichergestellt.⁶⁵

Da die Beschlagnahme nach § 94 StPO stets einer richterlichen Anordnung bedarf, ist dem betroffenen Cloud-Nutzer der Beschluss über die Daten, die nunmehr beschlagnahmt und damit nicht wieder gelöscht werden, zukommen zu lassen, um auch hier die Offenheit der Maßnahme sicherzustellen.

60 BVerfG, NJW 2009, 2431, 2437.

61 S. zum Ablauf der Ermittlungen Abschnitt 18.2.1.

62 Statt vieler Schmitt, in: Mayer-Goßner 2014, § 94 StPO, Rn. 16a.

63 Hartmann, in: Dölling/Duttge/Rössner 2013, § 110 StPO, Rn. 10; zum Anspruch auf Löschung im Ermittlungsverfahren BVerfG, NJOZ 2006, 2025.

64 Hartmann, in: Dölling/Duttge/Rössner 2013, § 94 StPO, Rn. 6.

65 Inwieweit eine formlose Sicherstellung oder eine förmliche Beschlagnahme stattfindet, ist in der Konstellation bereits zuvor kopierter Daten unklar. Allerdings ist die förmliche Beschlagnahme auch zulässig, wenn eine formlose Sicherstellung möglich wäre, Greven, in: Karlsruher Kommentar StPO 2013, § 94 StPO, Rn. 16; der Gewahrsamsinhaber muss nicht gefragt werden, ob er mit der Herausgabe einverstanden ist, Pfeiffer 2005, § 94 StPO, Rn. 3.

18.3.7 Zugriffe gegenüber dem Cloud-Anbieter

Richten sich die Ermittlungen nicht gegen den Cloud-Nutzer, sondern gegen den Cloud-Anbieter, ergeben sich keine cloud-spezifischen Besonderheiten. Sie folgen den regulären strafprozessualen Grundsätzen der Durchsuchung und anschließenden Beschlagnahme oder auch der Telekommunikationsüberwachung.⁶⁶

In diesem Zusammenhang ist ausschließlich relevant, dass im Zusammenhang mit der Verhältnismäßigkeit jeder Ermittlungsmaßnahme berücksichtigt werden muss, dass der Cloud-Anbieter IT-Ressourcen für zahlreiche Cloud-Nutzer bereitstellt. Beim Zugriff auf die Hardware ist daher im Einzelfall zu entscheiden, ob Behinderungen des Betriebes des Cloud-Servers unter Berücksichtigung der Interessen der Cloud-Nutzer angemessen sind. Außerdem ist beim Zugriff auf Dateninhalte zu beachten, dass die Kenntnisnahme des überwiegenden Teils der Daten des Cloud-Nutzers für den Cloud-Anbieter vertraglich oder gesetzlich (etwa daten- oder berufsrechtlich) untersagt ist.⁶⁷ Eine Kenntnisnahme der (geheimen) Daten von Cloud-Nutzern im Ermittlungsverfahren gegen den Cloud-Anbieter ist somit im Rahmen der Verhältnismäßigkeit zu vermeiden.

18.4 Gestaltungsempfehlungen

Um das Vertrauen in Cloud-Computing zu stärken und dadurch die Nutzung von Cloud-Angeboten zu fördern, ist es notwendig, dass die Cloud-Akteure über die tatsächliche Möglichkeit und die rechtliche Zulässigkeit des Zugriffs auf die Cloud informiert sind. Geht man davon aus, dass ehemals lokale IT-Ressourcen durch Cloud-Computing nicht grundlegend verändert werden, sondern lediglich internetbasiert und skalierbar werden, dürfen strafprozessuale Ermittlungen in der Cloud zu keinen anderen Ergebnissen gelangen als bei Ermittlungen in lokalen Systemen.

66 §§ 102 ff., 94 ff., §§ 100a ff. StPO und grundsätzlich auch die Ermittlungsgeneralklauseln in §§ 161 und 163 StPO.

67 S. Abschnitte 15.2.2.1 und 15.2.2.2 zu den Strafbarkeitsrisiken des Cloud-Anbieters bei unbefugter Kenntnisnahme von Daten des Cloud-Nutzers sowie Abschnitt 15.4.2.1 zu den Vermeidungsstrategien einer Strafbarkeit.

Für den Cloud-Nutzer bedeutet dies, dass er durch Inanspruchnahme von Cloud-Angeboten keinen geringeren Grundrechtsschutz erhalten darf. Andererseits dürfen sich für Ermittlungsbehörden auch die Zugriffsmöglichkeiten auf Beweismittel im Vergleich zur lokalen Datenhaltung nicht verschlechtern. Der Cloud-Anbieter muss folglich seinen Vertragspartner schützen und gleichzeitig seinen Pflichten gegenüber den Ermittlungsbehörden nachkommen. Nur wenn die Cloud-Akteure über die vorgenannten Besonderheiten der Ermittlung in der Cloud ausreichend informiert sind, können sie ihre Risiken minimieren, ohne dass das rechtmäßige Strafverfolgungsinteresse beeinträchtigt ist.

18.4.1 Gestaltungsempfehlungen für Cloud-Nutzer

Der Cloud-Nutzer muss grundsätzlich davon ausgehen, dass eine Abfrage seiner Bestandsdaten beim Cloud-Anbieter durch die Strafverfolgungsbehörden gemäß §§ 161 Abs. 1 Satz 1 und 163 Abs. 1 StPO in Verbindung mit § 14 Abs. 2 TMG vorgenommen werden kann – und zwar auch heimlich. Will der Cloud-Nutzer dies vermeiden, sollte er einen Cloud-Anbieter wählen, der Auskunft darüber erteilt, ob er das Passwort im Klartext speichert oder selbst nur über einen Hashwert des Passwortes verfügt.

Dem Cloud-Nutzer kann ein Nachteil entstehen, wenn der Cloud-Anbieter – statt nur im Rahmen eines vorhandenen Durchsuchungs- und Beschlagnahmebeschlusses gemäß §§ 102 ff. StPO und §§ 94 ff. StPO mit den Strafverfolgungsbehörden zu kooperieren, indem er beispielsweise bestimmte Daten kopiert – rechtswidrig einen Gastzugang zu allen Daten des Cloud-Nutzers eröffnet. Dies sollte der Cloud-Anbieter unterlassen, um keine Ordnungswidrigkeit nach § 43 Abs. 2 BDSG zu begehen. Der Cloud-Nutzer sollte sich informieren, wie der Cloud-Anbieter die Pflicht zur Zusammenarbeit mit den Ermittlungsbehörden handhabt. Vertragliche Vereinbarungen hierüber können Abhilfe schaffen.

Cloud-Computing als IT-Bereitstellungsmodell kann den Bezug von IT-Ressourcen verändern. Dies soll jedoch weder dazu führen, dass strafrechtliche Ermittlungen scheitern, weil die Daten nunmehr beim Cloud-Anbieter sind, noch den Grundrechtsschutz des Cloud-Nutzers absenken. Der Cloud-Nutzer muss daher die Kenntnis haben, dass – soweit ein Durchsuchungs-

und Beschlagnahmebeschluss gemäß §§ 102 ff. StPO und §§ 94 ff. StPO vorliegt – die Ermittlungsbehörden auch beim Cloud-Anbieter eine Kopie der Daten verlangen können. Dabei ist denkbar, dass Ermittlungsbehörden zeitgleich beim Cloud-Nutzer und beim Cloud-Anbieter vor Ort sind. Während der Cloud-Nutzer über die Erstellung der Kopie informiert wird, kann beim Cloud-Anbieter durch eben diese zeitgleiche Datenkopie sichergestellt werden, dass der Cloud-Nutzer keine Veränderungen mehr vornehmen kann.

Zwar ist die tatsächliche Möglichkeit heimlicher Maßnahmen beim Cloud-Computing größer, jedoch ergeben sich hierfür keine strafprozessualen Rechtsgrundlagen. Der Cloud-Nutzer ist nicht zur Herausgabe seiner Zugangsdaten zur Cloud verpflichtet. Ungeachtet des Cloud-Computing besteht für den Cloud-Nutzer stets die Möglichkeit, seine Daten verschlüsselt in der Cloud zu speichern, um sie so der Strafverfolgung auf zulässige Weise zu entziehen. Wird beim Cloud-Nutzer vor Ort ermittelt, ändert sich durch das Cloud-Computing nichts. Hier sind auch Maßnahmen im Ausland über den Nutzer-Account möglich.

18.4.2 Gestaltungsempfehlungen für Cloud-Anbieter

Der Cloud-Anbieter unterliegt gemäß §§ 161 Abs. 1 Satz 1 und 163 Abs. 1 StPO der Verpflichtung, Auskunft über vorhandene Bestandsdaten zu erteilen. § 14 Abs. 2 TMG gibt ihm die datenschutzrechtliche Erlaubnis, dieser Pflicht nachzukommen.⁶⁸ Eine Pflicht zur Erhebung bestimmter Daten, insbesondere des Passwortes im Klartext, trifft ihn dagegen nicht.⁶⁹ Der Cloud-Anbieter kann, um den Cloud-Nutzer vor heimlichen Ermittlungsmaßnahmen zu schützen, insbesondere darauf verzichten, das Passwort im Klartext zu speichern. Um das Vertrauen in sein Cloud-Angebot zu stärken, sollte der Cloud-Anbieter den Cloud-Nutzer darauf hinweisen, dass er zwar grundsätzlich zur Auskunft von Bestandsdaten an Strafverfolgungsbehörden verpflichtet ist, dass er jedoch selbst das Passwort nur als Hashwert vorhält und daher im Ergebnis keine Auskunft darüber erteilen kann.

68 S. Dix, in: Roßnagel 2013, § 14 TMG, Rn. 47 ff.

69 Wicker, MMR 2014, 298 ff.

Der Cloud-Anbieter kann aus Sorge um die Betriebsfähigkeit seines gesamten Cloud-Angebots dazu geneigt sein, überobligatorisch mit den Strafverfolgungsbehörden hinsichtlich eines einzelnen Cloud-Nutzers zu kooperieren. Sofern dies eine datenschutzrechtlich unzulässige Übermittlung personenbezogener Daten darstellt, würde er dadurch aber zugleich eine Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG begehen. Um dies zu vermeiden und zugleich seinen Cloud-Nutzer in seinen Grundrechten bestmöglich zu schützen, sollte der Cloud-Anbieter ausschließlich innerhalb der Grenzen der ihm vorgelegten gerichtlichen Anordnungen handeln. Sein Cloud-Angebot wird ein höheres Vertrauen genießen, wenn der Cloud-Anbieter darüber informiert, dass er keine Gastzugänge für die faktische Möglichkeit der heimlichen Ermittlung eröffnet, sondern nur im Rahmen seiner gesetzlichen Pflichten nach Prüfung von formellen Anordnungen handelt.

Der Cloud-Anbieter ist gemäß § 95 StPO verpflichtet, bei Vorlage einer Durchsuchungs- oder Beschlagnahmeanordnung zumindest eine Kopie der Daten an die Ermittlungsbehörden auszuhändigen. Eine Mitnahme der Cloud-Server durch die Strafverfolgungsbehörden wird meist mangels Verhältnismäßigkeit der Maßnahme ausscheiden. Der Cloud-Anbieter sollte den Cloud-Nutzer über diese Pflicht informieren. Um jedoch gegenüber dem Cloud-Nutzer nicht den Eindruck zu erwecken, die in der Cloud gespeicherten Daten seien beim Cloud-Anbieter nicht so gut aufgehoben, wie bei einer lokalen Speicherung am Ort des Cloud-Nutzers, weil der Cloud-Anbieter zur Herausgabe der Daten verpflichtet ist, bietet es sich an, dass der Cloud-Anbieter den Cloud-Nutzer in diesem Zusammenhang darüber in Kenntnis setzt, dass der gleiche Durchsuchungs- und Beschlagnahmebeschluss eine Mitnahme der lokalen Rechner des Cloud-Nutzers oder ein Erstellen von Datenkopien hiervon auch rechtfertigen würde.

Darüber hinaus kann der Cloud-Anbieter technische Maßnahmen ergreifen, die seinen eigenen Zugriff zu den Daten seiner Cloud-Nutzer auf seinen Servern ausschließen.⁷⁰ Soweit er selbst und seine Mitarbeiter keine Zugriffsmöglichkeiten haben, kann er selbstverständlich auch keine Datenkopien im Rahmen seiner Pflicht von § 95 Abs. 1 StPO erstellen. Auf diese

70 S. hierzu das Konzept des Trusted-Cloud-Projekts „Sealed Cloud“.

Weise kann der Cloud-Anbieter dem Cloud-Nutzer ein besonders vertrauenswürdiges Cloud-Angebot präsentieren.

Schließlich ist der Cloud-Nutzer am besten geschützt, wenn er seine Daten – ob lokal oder in der Cloud – verschlüsselt speichert. Der Cloud-Anbieter sollte daher den Cloud-Nutzer darauf aufmerksam machen, dass seine Daten im verschlüsselten Zustand den besten Schutz vor strafprozessualen Ermittlungen genießen. Der Cloud-Anbieter sollte in diesem Zusammenhang den Cloud-Nutzer darauf hinweisen, dass die Ermittlungsbehörden auch beim Cloud-Nutzer vor Ort in der Cloud ermitteln können, soweit entweder der Cloud-Nutzer ihnen die Zugangsdaten zur Cloud mitteilt oder die Bestandsdatenauskunft – wider Erwarten – mit Erfolg verlaufen ist.

18.4.3 Ausländische Angebote und ausländische Strafverfolgungsbehörden

Problematisch wird der Schutz der Daten im Hinblick auf ausländische Cloud-Anbieter und den Zugriff ausländischer Behörden. Ausländische Anbieter unterliegen ausländischen Gesetzen, die unter einfacheren Voraussetzungen den Zugriff auf Daten ermöglichen könnten. Auch können dort Praktiken herrschen, die rechtsstaatlichen Zweifeln unterliegen.

Anders als nach deutschem Recht kann das Abfangen von Daten auf dem Weg in die Cloud oder aus der Cloud beispielsweise für US-amerikanische Ermittlungsbehörden und Geheimdienste zulässig sein.⁷¹ Zugriffe auf Inhaltsdaten sind teilweise sogar ohne gerichtliche Anordnung möglich, soweit die Daten ermittlungsrelevant sind.⁷² Die Rechte von US-Ermittlungsbehörden bestehen nach US-Recht auch, wenn die Daten außerhalb der USA, also beispielsweise in Deutschland, gespeichert sind.⁷³ Den weiterreichenden Ermittlungsbefugnissen ausländischer Staaten, insbesondere der USA, nach ihrer Rechtsordnung kann faktisch dadurch begegnet werden, dass der Nutzer

71 Voigt, MMR 2014, 158, 159; s. zur Unzulässigkeit des Zugriffs auf die Datenübertragung in Deutschland Abschnitt 18.2.5.

72 Voigt, MMR 2014, 158, 159.

73 Hierin liegt allerdings nicht zwingend ein Unterschied zu deutschem Recht vor – eine Durchsuchung nach § 102 StPO über den Account des Cloud-Nutzers ist auch außerhalb Deutschlands möglich.

nur auf Cloud-Anbieter mit Sitz und Servern innerhalb von Deutschland oder der Europäischen Union zurückgreift⁷⁴ oder seine Daten verschlüsselt.

18.4.4 *Cloud-Computing ohne zusätzliche strafprozessuale Risiken*

Sind Daten nicht mehr lokal gespeichert, sondern befinden sich in der Cloud, steigt das Risiko von unerwünschten Zugriffen anderer – auch von Strafverfolgungsbehörden. Der Cloud-Nutzer kann nur dann auf das Angebot seines Cloud-Anbieters vertrauen, wenn er weiß, wie der Cloud-Anbieter im Fall von Ermittlungen handeln wird. Ein offener Umgang mit der Möglichkeit eines strafprozessualen Zugriffs stärkt daher das Vertrauen des Cloud-Nutzers in seinen Cloud-Anbieter.

18.5 Literaturverzeichnis

- Birk, D.; Heinson, D.; Wegener, C.:** Virtuelle Spurensuche. In: Datenschutz und Datensicherheit (DuD), 2011, S. 329-332.
- Boos, C.; Kroschwald, S.; Wicker, M.:** Datenschutz bei Cloud Computing zwischen TKG, TMG und BDSG, Datenkategorien bei der Nutzung von Cloud Diensten. In: Zeitschrift für Datenschutz (ZD), 2013, S. 205-210.
- Braun, F.:** Zum Telekommunikationsbegriff in § 3 Abs. 1 Nr. 22 TKG, Anmerkung zu OLG Jena, 1. Strafsenat, Beschluss vom 14.08.2013, Aktenzeichen: 1 Ws 217/13. In: juris PraxisReport IT-Recht (jurisPR-ITR), 22/2013, Anmerkung 2.
- Brodowski, D.; Eisenmenger, F.:** Zugriff auf Cloud Speicher und Internetdienste durch Ermittlungsbehörden. In: Zeitschrift für Datenschutz (ZD), 2014, S. 119-126.
- Bundesamt für Sicherheit in der Informationstechnik:** Informationssicherheit stärken – Vertrauen in die Zukunft schaffen, Tagungsband zum 13. Deutschen IT-Sicherheitskongress, Bonn 2013.
- Bundesamt für Sicherheit in der Informationstechnik:** Leitfaden „IT-Forensik“. Berlin 2011.
- Dalby, J.:** Das neue Auskunftsverfahren nach § 113 TKG – Zeitdruck macht Gesetze. In: Computerrecht (CR), 2013, S. 361-369.
- Dölling, D.; Duttge, G.; Rössner, D.:** Gesamtes Strafrecht StGB – StPO, Nebengesetze. 3. Auflage, Baden-Baden 2013.
- Gercke, B.:** Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten. In: Strafverteidiger Forum (StraFo), 2009, S. 271-274.
- Germann, M.:** Gefahrenabwehr und Strafverfolgung im Internet. Berlin 2000.

⁷⁴ Voigt, MMR 2014, 158, 159.

- Graf, J. P.:** Beck'scher Onlinekommentar Strafprozessordnung. Edition 17, München 2013.
- Hannich, R.:** Karlsruher Kommentar zur Strafprozessordnung. 7. Auflage, München 2013.
- Jäger, H.; Rieken, R.:** IDGARD Sealed Cloud – das erste vollfunktionale Kommunikationsnetz, das sowohl Inhalte als auch Metadaten schützt. München 2014.
- Kelnhofer, E.; Nadeborn, D.:** Anmerkung zu LG Mannheim, Beschluss vom 12.10.2012, Aktenzeichen 24 Qs 2/10. In: Strafverteidiger (StV), 2011, S. 352-354.
- Kleinknecht, T.; Müller, H.; Reitberger, L.:** KMR-Kommentar zur Strafprozessordnung. 70. Ergänzungslieferung, Köln 2013.
- Kolb, A.; Birk, D.; Wegener, C.:** Digitale Forensik in IaaS-Cloud-Umgebungen. Hrsg.: Bundesamt für Sicherheit in der Informationstechnik, Bonn 2013.
- Meinicke, D.:** Der Zugriff der Ermittlungsbehörden auf beim Provider zwischengelegte E-Mails. Edeweicht 2013.
- Meyer-Goßner, L.; Schmitt, B.:** Strafprozessordnung: Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen. 57. Auflage, München 2014.
- Pfeiffer, G.:** StPO: Strafprozessordnung. 5. Auflage. München 2005.
- Roßnagel, A.:** Beck'scher Kommentar zum Recht der Telemediendienste, Kommentar zum TMG, SigG, SigV, JMStV, BGB (Auszüge), VwVfG (Auszüge), ZPO (Auszüge). München 2013.
- Taeger, J.:** Law as a Service – Recht im Internet- und Cloud-Zeitalter, Tagungsband der Herbstakademie 2013. Edeweicht 2013.
- Voigt, P.:** Weltweiter Datenzugriff durch US-Behörden – Auswirkungen für deutsche Unternehmen bei der Nutzung von Cloud-Diensten. In: Multimedia und Recht (MMR), 2014, S. 158-161.
- Warntjen, M.:** Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung. Baden-Baden 2007.
- Wicker, M.:** Die Neuregelung des § 100j StPO auch beim Cloud Computing? Zugriff auf Zugangsdaten zur Cloud nach der neuen Bestandsdatenauskunft?. In: Multimedia und Recht (MMR), 2014, S. 298-302.
- Wicker, M.:** Durchsuchung in der Cloud Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden. In: Multimedia und Recht (MMR), 2013, S. 765-769.
- Wicker, M.:** Ermittlungsmöglichkeiten in der Cloud – Vereitelt das Speichern in der Cloud die Zuständigkeit deutscher Ermittlungsbehörden?. Hrsg.: Taeger, J., Edeweicht 2013, Band. 2, S. 981-1000.

Teil F:
Marktunterstützung durch
Einsatz der Value4Cloud-
Mehrwertdienste

19 Marktunterstützung in den Bereichen Bedarfsanalyse, Service-Auswahl und Service-Management

J. Wollersheim, H. Krcmar

19.1 Einleitung

Das Projekt Value4Cloud adressiert mit den erarbeiteten Ergebnissen insbesondere den Unterstützungsbedarf kleinerer und mittelgroßer Unternehmen in Deutschland, die eine Nutzung von Cloud-Services in Erwägung ziehen. Gerade Unternehmen dieser Größe sind oft noch unsicher, ob und wenn ja welche Besonderheiten bei der Beschaffung von IT in Form von Cloud-Services zu beachten sind. Die Unternehmen konnten zumeist noch keine eigenen Erfahrungen mit Cloud-Services sammeln und es fehlen Erfahrungen im engeren Kollegen und Bekanntenkreis, die helfen könnten, die initiale Unsicherheit zu überwinden. Hier setzen die im Projekt Value4Cloud entwickelten Werkzeuge an. Sie unterstützen Unternehmen im Beschaffungsprozess, weisen auf Besonderheiten hin, unterstützen die Akteure und strukturieren die Abläufe. Vorhandene Unsicherheit wird somit durch Information verringert; klare Strukturen werden etabliert und Unternehmen werden für Sicherheitsaspekte sensibilisiert, nicht verschreckt. Value4Cloud wirbt somit für eine Kriterien-basierte, wohlüberlegte Auswahl- und Beschaffungsentcheidung. Die im Projekt entwickelten Werkzeuge, die im Rahmen einer Cloud-Service-Beschaffung unterstützen, sind:

- Werkzeuge zur Unterstützung der Bedarfsanalyse
- Werkzeuge zur Unterstützung der Service-Auswahl
- Werkzeuge zur Unterstützung des Service-Management

Die Werkzeuge werden in den nachfolgenden Abschnitten im Überblick vorgestellt. Wie sie im Rahmen des Beschaffungsprozesses unterstützen können, verdeutlicht darüber hinaus auch die in Kapitel 25 folgende Fallstudie.

19.2 Werkzeuge zur Unterstützung der Bedarfsanalyse

Der Beschaffungsprozess in Unternehmen wird von unterschiedlichsten Faktoren beeinflusst. Diese sind bei jedweder Prozessgestaltung zu berücksichtigen, so auch bei der Gestaltung eines unternehmensindividuellen Beschaffungsprozesses für Cloud-Services. Der in Kapitel 10 dieses Buchs vorgestellte Analyserahmen umfasst sechs wesentliche Aspekte, die die Ausgestaltung des Beschaffungsprozesses für Cloud-Services beeinflussen und somit bei der Prozessgestaltung berücksichtigt werden sollten. [Abbildung 1](#) visualisiert die im Projekt Value4Cloud adressierten Faktoren und ihre Ausprägungen.

Service-Typ	Software as a Service (SaaS) Beschaffungen		Plattform or Infrastructure Services (PaaS/IaaS)-Beschaffungen	
Werte und Normen am Markt	Beschaffungsgut ist etabliert		Beschaffungsgut ist innovativ und neu	
Gesetzliche Rahmenbedingungen	Beschaffung tangiert Daten mit Personenbezug	Beschaffung tangiert Daten mit gesetzlich festgelegter Aufbewahrungsfrist		Beschaffung tangiert keine Daten mit Personenbezug oder Aufbewahrungsfristen
Unternehmenssituation des Beschaffers	Start-Up / Gründungsphase		Stabilität	Down-Sizing, Turnaround
Kaufanlass und Innovationsgrad	Innovative, neue Lösung für experimentellen Einsatz	Innovative, neue Lösung für tagtäglichen Einsatz	Lösung zur Unterstützung des Unternehmenswachstums, Ergänzungsbeschaffung	Lösung zur Effizienzsteigerung, Ersatz einer bestehenden Lösung
Typ des (initialen) Beschaffungsobjekts	Unternehmensweite IT-Infrastruktur		Anwendung, die von einer Abteilung genutzt werden soll	Anwendung, die von mehreren Abteilungen genutzt werden soll

Abbildung 1: Einflussfaktoren und ihre Ausprägungen (Eigene Darstellung).

Abbildung 2: Template zur Analyse und Klassifizierung des Schutzbedarfs (Eigene Darstellung).

Da Informations- und Kommunikationstechnik für eine Vielzahl von Unternehmen eine bedeutende Rolle spielt und die Abhängigkeit von IT tendenziell zunimmt, nimmt für die Unternehmen auch das Gefährdungspotenzial durch IT stetig zu. Bei der Suche nach Antworten auf entstehende Fragen der Informationssicherheit ist zu bedenken, dass Sicherheitsaspekte in unterschiedlichem Ausmaß zu adressieren sind, etwa in Abhängigkeit vom Schutzbedarf der betroffenen Daten. IT-Systeme, die Daten mit eher typischem Schutzbedarf verarbeiten, werden mittels Standard-Sicherheitsmaßnahmen abgesichert. Solche, die Daten mit hohem Schutzbedarf verarbeiten, benötigen ein entsprechend höheres Schutzniveau und verlangen somit nach besseren Sicherungsmaßnahmen. Im Projekt wurde die Schutzbedarfsanalyse als ein wichtiges Element im Beschaffungsprozess identifiziert, zu dem in den meisten Unternehmen nicht ausreichend Informationen vorhanden sind. Um den Bedarf zu adressieren und für den Themenbereich Datenschutz zu sensibilisieren, wurde unter anderem [Abbildung 2](#) entwickelt.

Die Abbildung und die vermittelten Zusammenhänge sensibilisieren Unternehmen für den Schutzbedarf der Daten, die von der jeweiligen Beschaf-

fungsentscheidung betroffen sein können. Die Abbildung regt die Diskussion an und ermuntert, ggf. eine eigene Klassifizierung vorzunehmen und eine Liste notwendiger Sicherheitsmaßnahmen auf Basis des IT-Grundschutzkatalogs (BSI 2011) oder vergleichbarer Kataloge im Unternehmen zu diskutieren.

Ebenfalls im Rahmen der Spezifikation des eigenen Bedarfs und des Beschaffungsprozess-Aufbaus ist aus Sicht des beschaffenden Unternehmens festzulegen, welche Abteilung mit welcher Verantwortung in den Beschaffungsprozess eingebunden werden soll. Die nachfolgende [Abbildung 3](#) visualisiert ein im Rahmen des Projektes entwickeltes und im wissenschaftlichen Kontext veröffentlichtes und diskutiertes (Wollersheim/Krcmar 2013) Template, das eine feingranulare Darstellung des Beschaffungsprozesses (in Anlehnung an Heckman 2003; Van der Valk/Rozemeijer 2009) sowie bereits vorformulierte Abteilungen oder Anspruchsgruppen umfasst, die typischerweise im Prozess zu berücksichtigen sind. Unternehmen können weitere Anspruchsgruppen hinzufügen und im Anschluss Verantwortlichkeiten festlegen. In Anlehnung an das verbreitete RACI-Schema (ohne Autor 2014) wird vorgeschlagen, Zuständigkeiten wie folgt festzulegen:

- R) Responsible: Person ist verantwortlich für das Ergebnis einer Aktivität
- A) Accountable: Person ist mit der Durchführung einer Aktivität beauftragt. Diese Kennzeichnung ist nur zu verwenden, wenn die beauftragte Person ungleich der ergebnisverantwortlichen Person ist.
- C) Consulted: Person wird beratend hinzugezogen
- I) Informed: Person ist bezgl. des Ergebnisses einer Aktivität zu informieren

	Grobe Spezifikation (funkt. & techn.)	Schutzklasse identifizieren	Bedarfsspezifikation			Abgleich von Bedarf und Angebot	Priorisierung der Angebote	Verhandlung und Vertrag
			Funktional	Technisch	Rechtlich			
Fachabteilung	R		R	C	C	R		C
IT-Abteilung		R		R		I		
Legal					R	I		
Geschäftsführung		I	I	I	I	I	R	R
...								

Legende: A = Accountable C = Consulted I = Informed R = Responsible

Abbildung 3: Template zur Zuordnung von Verantwortlichkeiten (In Anlehnung an Heckman 2003; Van der Valk/Rozemeijer 2009).

19.3 Werkzeuge zur Unterstützung der Service-Auswahl

Sind die Anspruchsgruppen festgelegt, der Schutzbedarf und weitere Anforderungen bekannt und grob skizziert, muss dem eruierten Bedarf das Angebot am Markt gegenübergestellt werden. Um beim Abgleich Missverständnisse zwischen Service-Anbieter und Kunde zu vermeiden, ist ein möglichst eindeutiges Vokabular nötig, das sowohl in der Lage ist, den angebotenen Service wie auch den spezifizierten Bedarf zu beschreiben. Ein Kriterienkatalog kann bei der systematischen Zusammenstellung der für die Beschaffungsentscheidung relevanten Kriterien und deren Ausformulierung helfen. Auf diese Weise können Lücken in der Anforderungsbeschreibung aufgedeckt und nachhaltig verhindert werden. Zu diesem Zweck wurde im Projekt der Kriterienkatalog CloudServiceCheck entwickelt. Er bietet Mitarbeitern von Unternehmen, die an einer Nutzung von Cloud-Services interessiert sind, die nötige Orientierung bei der Frage, welche Informationen bei der Entscheidung für oder gegen ein Service-Angebot relevant sein können. Der hier beschriebene Kriterienkatalog für Cloud-Services kann wie eine Checkliste eingesetzt werden und hilft bei der Identifikation relevanter Auswahlkrite-

rien. Darüber hinaus bietet der CloudServiceCheck Unterstützung bei der Analyse und Bewertung von Serviceangeboten, damit keine als entscheidungsrelevant identifizierten Kriterien außer Acht gelassen werden.

Zur detaillierten Vorstellung der Kriterien sei an dieser Stelle auf Kapitel 9 dieses Buches verwiesen.

19.4 Werkzeuge zur Unterstützung des Service-Managements

Anders als bei IT-Hardware können Cloud-Services nicht einer umfassenden Wareneingangsprüfung unterzogen werden, um alle Qualitätsaspekte abschließend zu beurteilen. Es ist eine kontinuierliche Überwachung der Dienstleistung notwendig. Anhand welcher Kriterien diese Überwachung etabliert werden sollte, wurde im Projekt untersucht. [Tabelle 1](#) zeigt die im Laufe des Projektes auf Basis der Norm ISO/IEC 25010 (2011) entwickelten Qualitätseigenschaften, die für Unternehmen zum Zeitpunkt der Service-Nutzung relevant werden.

Tabelle 1: Qualitätskriterien / kontinuierliche Service-Nutzung

Qualitätskriterien	Bewertung	Ergänzende Kommentare
Effektivität Exaktheit und Vollständigkeit, mit denen die an den Service gesteckten Ziele erreicht werden konnten	> Sterne-Bewertung <	>>Freitext<<
Effizienz Aufgewendete Ressourcen in Relation zu der Exaktheit und Vollständigkeit der erreichten Ziele	> Sterne-Bewertung <	>>Freitext<<
Nützlichkeit Grad, zu dem ein Nutzer mit der wahrgenommenen Zielerreichung zufrieden ist; inkl. dem Ergebnis und der sonstigen Konsequenzen der Service-Nutzung	> Sterne-Bewertung <	>>Freitext<<
Vertrauen Grad, zu dem ein Nutzer oder Interessenvertreter Vertrauen in die bezogene Dienstleistung hat, dass sich diese wie beabsichtigt verhält	> Sterne-Bewertung <	>>Freitext<<

Qualitätskriterien	Bewertung	Ergänzende Kommentare
Vergnügen Grad, zu dem ein Nutzer bei der Nutzung und Zielerreichung mittels des Services Vergnügen erzielt	> Sterne-Bewertung <	>>Freitext<<
Komfort Grad, zu dem ein Nutzer mit dem Komfort zufrieden ist	> Sterne-Bewertung <	>>Freitext<<
Risikominderung – Ökonomisch Grad, zu dem die Dienstleistung das ökonomische Risiko mindert (bspw. bzgl. effizientem Betrieb, Reputation, etc.)	> Sterne-Bewertung <	>>Freitext<<
Risikominderung – Arbeitsschutz Grad, zu dem die Dienstleistung das Risiko für die damit arbeitenden Nutzer mindert, bei angedachter Nutzung	> Sterne-Bewertung <	>>Freitext<<
Risikominderung – Umwelt Grad, zu dem die Dienstleistung das Risiko für Eigentum und Umwelt mindert, bei angedachter Nutzung	> Sterne-Bewertung <	>>Freitext<<
Inhaltlicher Abdeckungsgrad – Vollständigkeit Grad, zu dem die Dienstleistung effizient und effektiv, frei von Risiken und mit Vergnügen in allen beabsichtigten Nutzungsszenarien genutzt werden kann	> Sterne-Bewertung <	>>Freitext<<
Inhaltlicher Abdeckungsgrad – Flexibilität Grad, zu dem die Dienstleistung effizient und effektiv, frei von Risiken und mit Vergnügen in Nutzungsszenarien genutzt werden kann, die nicht zu Beginn spezifiziert wurden	> Sterne-Bewertung <	>>Freitext<<

19.5 Zusammenfassung der Marktunterstützung

Gerade für mittelständische Unternehmen ist es eine große Herausforderung, die im Beschaffungsprozess relevanten Qualitätsanforderungen festzulegen und die zugehörigen Qualitätsinformationen bezüglich der am Markt verfügbaren und prinzipiell in Frage kommenden IT-Serviceangebote zu eruieren. Die im Projekt erzielten Ergebnisse adressieren diese Herausforderungen mittelständischer Unternehmen bei der Beschaffung von Cloud-Services ganzheitlich, von der Anforderungsspezifikation bis zur Auswahlentscheidung.

Mit Hilfe von Informationsdiensten und einem Kriterienkatalog wird die notwendige Transparenz und Vergleichbarkeit verschiedener Cloud-Computing-Angebote für kleine und mittelständische Anwenderunternehmen geschaffen. Der Kriterienkatalog bietet ein Werkzeug für potenzielle Anwender, anhand dessen sie den relevanten Informationsbedarf für ihre Auswahlentscheidung festlegen können. Somit können Anwender sicherstellen, dass alle entscheidungsrelevanten Informationen berücksichtigt werden. Basis des entwickelten Kriterienkatalogs CloudServiceCheck und der Vokabular-Erweiterung eUSDL ist unter anderem die Unified Service Description Language (USDL), die im Rahmen des Leuchtturmprojektes THESEUS TEXO entwickelt wurde und auf der in diesem Projekt aufgebaut wurde.

Um die Qualität von Cloud-Services nicht nur zum Zeitpunkt des Kaufs, sondern kontinuierlich während der Nutzung zu messen und für die Steuerung relevante Informationen zeitnah zu erhalten, benötigen Unternehmen weitere Werkzeugunterstützung. Die Bewertung von Dienstleistungsqualität ist wissenschaftlich keine gänzlich neue Herausforderung. Modelle zur Bewertung der wahrgenommenen Servicequalität wurden beispielsweise bereits von Parasurama et al. (1991), Grönroos (1984), Rust and Oliver (1994) sowie von Fassnacht und Koesel (2006) beforscht und in der Praxis validiert. Jedoch zeigte sich in den jüngeren der genannten Untersuchungen, dass Modelle zur Bewertung der Qualität von IT-Services individuell an bestimmte Service-Kategorien anzupassen sind. Dies konnte auch in Forschungen von Repschläger et al. (2013) oder in diesem Projekt durch Hoberg et al. (2012a) bestätigt werden. Entsprechend ist es notwendig, die Bewertungskriterien und Skalen an den im Projekt entwickelten Kriterienkatalog CloudServiceCheck und weitere Erkenntnisse anzupassen. Auf Basis der Norm ISO/IEC 25010 (2011)

wurden im Projekt Value4Cloud Qualitätsdimensionen und Skalen entwickelt, anhand derer Anwender und unabhängige Prüfinstitutionen Cloud-Services bewerten können. Die entstehenden Kennzahlenwerte können in Summe einen aggregierten Überblick über die wahrgenommene Servicequalität bezüglich des Cloud-Services geben. Ausschlaggebende und folglich in der Bewertung zu berücksichtigende Eigenschaften von Cloud-Services wurden im Projekt zunächst empirisch entwickelt. Es folgte eine prototypische Umsetzung in Software, die in Workshops spielerisch mit Praxispartnern validiert wurde. Mit Hilfe der entwickelten Werkzeuge haben Unternehmen nun die Möglichkeit, die für sie individuell relevanten Qualitätskriterien zu identifizieren, anhand derer sie die Qualität von Cloud-Services kontinuierlich überwachen möchten. Somit können sie etwa Minderleistung und damit verbundene Verletzungen von Service Level Agreements feststellen oder auch eine Datenbasis zu dem dahinter stehenden Service-Anbieter schaffen, etwa als Input für zukünftige Investitionsentscheidungen.

19.6 Literaturverzeichnis

- BSI (2011):** IT-Grundschutz-Kataloge, Bundesamt für Sicherheit in der Informationstechnik – BSI, Bonn, Deutschland 2011.
- Fassnacht, M.; Koese, I. (2006):** Quality of Electronic Services. In: Journal of Service Research, Vol. 9 (2006) No. 1, S. 19-37.
- Grönroos, C. (1984):** A service quality model and its marketing implications. In: European journal of marketing, Vol. 18 (1984) No. 4, S. 36-44.
- Heckman, R.L. (2003):** Managing the IT Procurement Process. In: IS Management Handbook. Brown, C.V.; Topi, H. (Hrsg.). 8. Aufl., Auerbach Publications, Washington D.C., USA 2003, S. 73-88.
- Hoberg, P.; Reidt, A.; Wollersheim, J.; Krcmar, H. (2014):** CloudServiceCheck, Ausgabe 1, 2014.
- Hoberg, P.; Wollersheim, J.; Krcmar, H. (2012a):** The Business Perspective on Cloud Computing – A Literature Review of Research on Cloud Computing. Präsentiert auf der 18th Americas Conference on Information Systems, Seattle, USA.
- Hoberg, P.; Wollersheim, J.; Krcmar, H. (2012b):** Service Descriptions for Cloud Services – The Customer's Perspective. Präsentiert auf der ConLife Academic Conference 2012, Köln, Deutschland.
- ISO/IEC 25010 (2011):** Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE), 2011.

- ohne Autor (2014):** RACI. <http://de.wikipedia.org/wiki/RACI>, zugegriffen am 28.07.2014.
- Parasuraman, A.; Berry, L.L.; Zeithaml, V.A. (1991):** Refinement and Reassessment of the SERVQUAL Scale. In: Journal of Retailing, Vol. 67 (1991) No. 4, S. 420-450.
- Repschlaeger, J.; Wind, S.; Zarnekow, R.; Turowski, K. (2013):** Decision Model for Selecting a Cloud Provider: A Study of Service Model Decision Priorities. Präsentiert auf der 19th Americas Conference on Information Systems, Chicago, USA.
- Rust, R.T.; Oliver, R.L. (1994):** Service quality: insights and managerial implications from the frontier. In: Service quality: New directions in theory and practice. Rust, R.T.; Oliver, R.L. (Hrsg.). Sage Publications, Thousand Oaks, USA 1994, S. 1-19.
- Van der Valk, W.; Rozemeijer, F. (2009):** Buying business services: Towards a structured service purchasing process. In: Journal of Services Marketing, Vol. 23 (2009) No. 1, S. 3-10.
- Wollersheim, J.; Krcmar, H. (2013):** Purchasing processes for cloud services – An exploratory study of process influencing factors. Präsentiert auf der 22nd Annual IPSERA Conference, Nantes, Frankreich.

20 Entwicklung eines Kriterienkatalogs zur Zertifizierung von Cloud-Services

S. Schneider, J. Lansing, F. Gao, A. Sunyaev

20.1 Einleitung¹

Wie in Kapitel 12 aufgezeigt, entstehen zahlreiche Cloud-Service-Zertifizierungen (CSZ) in der Praxis. Doch in ihrem Bestreben, den Marktstandard zu schaffen, entwickeln sich diese CSZ-Initiativen unabhängig voneinander, was zu einer heterogenen Sammlung von CSZ führt, die überwiegend proprietär sind, auf unterschiedlichen Standards beruhen und sich in Bezug auf Umfang, Audit-Prozess und den zugrunde liegenden Zertifizierungsschemata unterscheiden. In der Forschung wurde gezeigt, dass der Inhalt einer Zertifizierung (also das zugrunde liegende Zertifizierungsschema) dessen Wirksamkeit beeinflusst (Kim/Benbasat 2009). Jedoch mangelt es trotz des Bedarfs nach Forschung zu CSZ (Khan/Malluhi 2010; Bundesministerium für Bildung und Forschung 2012; Sunyaev/Schneider 2013; European Commission 2012) an Richtlinien zur Gestaltung und Entwicklung von CSZ (Schneider et al. 2013; Lansing et al. 2013). Derzeit gibt es keine allgemein anerkannten Strukturmerkmale einer CSZ. Wie in Kapitel 12 bereits identifiziert, rücken je nach Anwendungszweck und Zielgruppe unterschiedliche Aspekte von CSZ in den Vordergrund. In diesem Kapitel wird aufgezeigt, wie diese Herausforderungen in der Praxis adressiert werden können, indem eine Taxonomie zur Strukturierung von CSZ entwickelt wird. Bestehende Cloud-Standards und CSZ bieten fundiertes Wissen über die Anforderungen an Cloud-Services und darüber, welche Kriterien Cloud-Service-Provider erfüllen müssen. Allerdings wurden dieses Wissen und die generischen Strukturmerkmale von Zertifizierungsschemata bisher nicht formalisiert. Taxonomien bieten ein Mittel, um Wissen einer spezifischen Domäne zu struk-

1 Aufbauend auf der bereits im wissenschaftlichen Kontext von Schneider et al. (2014) erfolgten Veröffentlichung zum Thema dieses Abschnitts werden nachfolgend die wesentlichen Aspekte kurz zusammengefasst.

turieren (Glass/Vessey 1995), und sind daher ein geeignetes Mittel, um eine generische Struktur für CSZ herzuleiten. Dieses Kapitel zeigt die wesentlichen Aspekte der entwickelten Taxonomie von CSZ auf, abgerundet durch Hinweise auf mögliche Anwendungsfälle und Einsatzmöglichkeiten in der Unternehmenspraxis. Eine vollständige Übersicht der Zertifizierungskriterien ist in Schneider et al. (2014) zu finden.

20.2 Vorgehensweise zur Taxonomieentwicklung

Zur Entwicklung der Taxonomie der Zertifizierungskriterien wurde ein dreistufiger Prozess verfolgt. Im ersten Schritt wurden 13 Experteninterviews durchgeführt, um die in der wissenschaftlichen Literatur dargelegte Wissensbasis zu erweitern (siehe auch Kapitel 12 dieses Buches) und eine Basis zur Ableitung der Taxonomie aufzubauen. Im darauffolgenden Schritt wurde eine iterative Methode zur Entwicklung von Taxonomien angewendet (Nickerson et al. 2013). Dazu wurden zunächst die Interviewtranskripte analysiert, um Dimensionen und Charakteristiken für die Taxonomie abzuleiten, anschließend wurden Zertifizierungskriterien aus sieben Cloud-Standards abgeleitet. Im letzten Schritt wurde jedes Zertifizierungskriterium im Rahmen von Workshops mit vier Forschern in diese Taxonomie klassifiziert.

Eine Taxonomie strukturiert und organisiert Wissen einer spezifischen Domäne (Glass/Vessey 1995). Taxonomien nehmen eine zentrale Rolle in der Forschung und Praxis ein, denn eine Klassifizierung von Objekten hilft Forschern und Praktikern dabei, komplexe Domänen zu verstehen und zu analysieren (Nickerson et al. 2013), und stellt somit einen fundamentalen Mechanismus zur Wissensorganisation dar (Wand et al. 1995). Nach Nickerson et al. (2013) ist eine Taxonomie ein Artefakt, das existierende oder zukünftige Objekte in einer spezifischen Domäne beschreibt und klassifiziert. Sie besteht aus einer Menge von n Dimensionen D_i ($i = 1, \dots, n$), die jeweils aus einer Menge von k_i ($k_i \geq 2$) gegenseitig unabhängigen und zusammen vollständigen Charakteristiken C_{ij} ($j = 1, \dots, k_i$) bestehen, sodass jedes Betrachtungsobjekt genau ein C_{ij} für jedes D_i besitzt. Formal beschrieben als

$$T = [D_i, i = 1, \dots, n \mid D_i = [C_{ij}, j = 1, \dots, k_i, k_i \geq 2]].$$

Nickerson et al. (2013) haben eine iterative Methode zur Entwicklung von Taxonomien entwickelt. Im Folgenden wird die Anwendung dieser Methode beschrieben. Für eine detaillierte Beschreibung und eine Schritt-für-Schritt Anwendung sei auf Nickerson et al. (2013) und zu weiteren Details zur Anwendung der Taxonomieentwicklung in diesem Forschungskontext auf Schneider et al. (2014) verwiesen.

Nickerson et al. (2013) definieren den Ablauf der Iterationen, indem sie induktive (empirisch → konzeptuell) und deduktive (konzeptuell → empirisch) Iterationen unterscheiden. Als empirische Daten sind hier die Objekte zu verstehen, die klassifiziert werden sollen. In der vorliegenden Forschungsarbeit sind dies also existierende Zertifizierungskriterien, die z. B. aus existierenden Cloud-Standards abgeleitet werden können. Induktive Iterationen eignen sich, wenn Forscher begrenztes Verständnis über die Domäne besitzen, aber signifikante empirische Daten verfügbar sind (hier: Kriterien zur Zertifizierung von Cloud-Services). Deduktive Iterationen eignen sich, wenn Forscher ein umfassendes Verständnis über die Domäne haben, aber nur wenig empirische Daten verfügbar sind. Da sowohl empirische Daten (Cloud-Standards und die dort definierten Kriterien (siehe Bernnat et al. 2012; Gao/Schneider 2012; Grochol et al. 2014) als auch ausführliches konzeptuelles Wissen der Domäne – in Form von Experteninterviews und Erfahrung der Forscher – vorhanden sind, können beide Vorgehensweisen durchgeführt werden. Im Rahmen dieser Forschung wurden zu Beginn deduktive Iterationen durchgeführt, um Charakteristiken und Dimensionen anhand der Interviews ableiten zu können. Es wurde also Domänenwissen angewendet, um die Dimensionen und Charakteristiken der Taxonomie abzuleiten. Im Anschluss daran wurden induktive Iterationen durchgeführt. Es wurden also die zu klassifizierenden Objekte betrachtet, um die Taxonomie zu erweitern sowie Zertifizierungskriterien zu identifizieren. [Tabelle 1](#) fasst die Vorgehensweise und die Datenquellen für jede Iteration zusammen. Bei den Experteninterviews ist jeweils die Position der Interviewpartner und in Klammern die Branche angegeben. In eckigen Klammern ist die Nummer des Interviewpartners angegeben, auf die im Folgenden bei Zitaten referenziert wird.

Tabelle 1: Übersicht über Ablauf und Art der Iterationen

Iteration	Vorgehensweise	Datenquelle
1	Deduktiv	3 Experteninterviews <ul style="list-style-type: none"> • [01] Senior Research Manager (Beratung) • [02] CEO (Software-Lösungen) • [03] Head of Research (Beratung)
2	Deduktiv	3 Experteninterviews <ul style="list-style-type: none"> • [04] Leiter Softwareentwicklung (Software-Lösungen) • [05] Global Server Virtualization Offering Lead (Beratung) • [06] Senior Consultant (Beratung)
3	Deduktiv	4 Experteninterviews <ul style="list-style-type: none"> • [08] CEO (IT-Services) • [09] CEO (Software-Lösungen) • [10] CMO (Software-Lösungen) • [11] CEO (Software-Lösungen)
4	Induktiv	(Bundesministerium für Sicherheit in der Informationstechnik 2011)
5	Deduktiv	3 Experteninterviews <ul style="list-style-type: none"> • [07] Cloud Territory Business Manager (Software- und Hardware-Lösungen) • [12] Innovation Manager (IT-Services) • [13] Sales Manager (Software-Lösungen)
6	Induktiv	(International Organization for Standardization 2005)
7	Induktiv	(Cloud Security Alliance 2011)
8	Induktiv	(Badger et al. 2012; Cloud-Computing Use Cases Discussion Group 2010)
9	Induktiv	(EuroCloud 2011b)
10	Induktiv	(Stein et al. 2012)

In den deduktiven Iterationen haben zwei Forscher die Interviews unabhängig voneinander iterativ kodiert, um Aussagen zur Ableitung von Dimensionen, Charakteristiken und Objekten der Taxonomie zu identifizieren. Dabei konnten durch die Interviews Charakteristiken und Dimensionen weiter geschärft werden, da nur wenige Aussagen konkrete Zertifizierungskriterien enthielten. Interviewpartner haben eher generische und abstrakte Kriterien genannt, wie bspw. *„Lokalität und Sicherheit der Rechenzentren, der Infrastruktur, die leistungstechnische Anbindung dieser Rechenzentren an den Kunden“* [Interviewpartner 07] oder *„[...] der rechtliche und besonders auch der vertragliche Bereich eines Cloud-Services, der explizit unabdingbar ist für diese Zertifizierung.“* [Interviewpartner 10]. Weitere Aussagen klassifizierten Kriterien, wie bspw. *„Wenn das Thema Sicherheit Zertifizierungskriterium ist, [...], dann würde ich sagen, muss man auch vor Ort gucken, wie der seine Sicherheit managt.“* [Interviewpartner 08] oder *„Wenn auf dem Stack ganz oben der Service liegt, darunter liegt irgendwo mal Hardware. Alles was dazwischen ist, würde ich in Scheiben schneiden [...], weil das sind auch üblicherweise die Schnittstellen, wo eine Möglichkeit besteht, dass ein Cloud-Service-Provider sich für die Implementierung seines Cloud-Services wieder auf andere Provider stützt [...]“* [Interviewpartner 01]. Diese Aussagen wurden genutzt, um Charakteristiken für die Taxonomie ableiten zu können. So beinhalten bspw. die Aussagen von [Interviewpartner 07] und [Interviewpartner 10] drei Charakteristiken, welche in der Dimension „Kategorie“ gruppiert sind: IT-Sicherheit, Vertragsbedingungen, Rechtliche Compliance. Die Aussage von [Interviewpartner 08] spiegelt die Dimension „Vor-Ort-Auditierung“ (Charakteristiken: „ja“, „nein“) wieder und die Aussage von [Interviewpartner 01] demonstriert die Dimension „Servicemodell-Abhängigkeit“ (mit den Charakteristiken: „Utility-Schicht“, „Applikationsschicht“ und „alle Schichten“). Ferner dienen präzise Aussagen als Objekte in der Taxonomie, wurden jedoch für zukünftige induktive Iterationen markiert, damit diese durch detaillierte und messbare Zertifizierungskriterien aus den ausgewählten Standards ersetzt werden konnten. So wurde bspw. die Aussage als Objekt definiert: *„Was zusätzlich auch auf jeden Fall im Vertrag drin stehen sollte, ist die Anforderung, dass man über Incidents informiert wird, die beim Anbieter passieren und die mögliche Auswirkungen auf meine*

eigenen Daten als Kunde hätten.“ [Interviewpartner 06]. In den folgenden Iterationen wurde dieses Kriterium überarbeitet und durch Informationen ergänzt, die das Incident-Management betreffen (z. B. aus ISO 27001).

In den folgenden induktiven Iterationen wurden Zertifizierungskriterien anhand von bekannten und etablierten Standards für Cloud-Computing, IT-Sicherheit und IT-Services mit einem hohen Reifegrad und hohen Einflusspotenzial abgeleitet (siehe auch Gao/Schneider (2012) sowie Bernnat et al. (2012)). Das Ziel war es, eine Auswahl von Standards zu definieren, die einerseits einen großen Umfang von Anforderungen an CSZ aus den Interviews abdecken und andererseits einen tiefen Einblick in hochrelevante Fragestellungen wie Sicherheit und Privatsphäre ermöglichen. Daher wurden zum einen umfassende Standards ausgewählt, welche eine große Anzahl an Themen in einem Standard aggregieren (Badger et al. 2012; Cloud-Computing Use Cases Discussion Group 2010), sowie zum anderen Standards, welche sich auf spezielle Themen wie bspw. Sicherheit (International Organization for Standardization 2005; Bundesministerium für Sicherheit in der Informationstechnik 2011; Cloud Security Alliance 2011), Servicemanagement (Stein et al. 2012) oder rechtliche Bestimmungen (EuroCloud 2011b) beziehen. Dabei wurden Kriterien von jedem Standard wie folgt abgeleitet:

Ein Forscher hat die ausgewählten Standards sequenziell zur Identifizierung von geeigneten Zertifizierungskriterien analysiert, Vorschläge für oder Anforderungen an Cloud-Services als Kriterien extrahiert und diese in Fragen umformuliert, sodass diese mit „ja“ oder „nein“ beantwortet werden konnten. Dabei wurde jedes extrahierte Kriterium mit den bereits identifizierten Kriterien in der Taxonomie verglichen, sodass ähnliche Kriterien von verschiedenen Standards vereint und angepasst wurden. Zudem wurden allumfassende oder unpräzise Kriterien, welche zu mehreren Charakteristiken einer Dimension zugeordnet werden konnten, in kleinere und spezifischere Kriterien aufgeteilt. Da dieses Vorgehen nur von einem Forscher durchgeführt wurde, wurde die Vereinigung unter großer Vorsicht durchgeführt, sodass nur zwei Kriterien vereint wurden, welche zweifelsfrei identisch sind. Im Zweifelsfall wurde ein neues Kriterium eingefügt und in der nächsten Phase genauer untersucht. Durch diese Vorgehensweise konnten insgesamt 417 Zertifizierungskriterien identifiziert werden.

Um die Subjektivität der vorherigen Klassifizierung bei den induktiven Iterationen zu reduzieren und die Gültigkeit und Verlässlichkeit der Taxonomie zu erhöhen, wurden Workshops mit vier Forschern durchgeführt. Dabei wurden die abgeleiteten Kriterien klassifiziert, vereint und obsoletere Kriterien oder Duplikate gelöscht. Dies wurde in Iterationen durchgeführt, welche jeweils aus der Vorarbeit der Forscher und Team-Diskussionen bestanden. Die Workshops führten zu einer Reduzierung der Kriterien von 417 auf 328. Dabei wurden jedoch keine Änderungen an der Taxonomie vorgenommen.

20.3 Ergebnisse

Die entwickelte Taxonomie der Zertifizierungskriterien umfasst sechs Dimensionen und 28 Charakteristika. Dabei wird zwischen den Dimensionen „Kategorie“, „Vor-Ort-Auditierung“, „Auditierungsmethode“, „Kontinuierliches Monitoring“, „Servicemodell“ und „Zertifiziertes Objekt“ unterschieden. [Tabelle 2](#) fasst die Taxonomie, die Zuordnung der Charakteristika zu den Dimensionen und die Verteilung der Kriterien innerhalb der Dimensionen zusammen.

Die Dimension „Kategorie“ beschreibt die Zielsetzung, welche durch die Zertifizierung eines Kriteriums erreicht werden soll. Sie erlaubt es Cloud-Service-Nutzern, einen zertifizierten Cloud-Services hinsichtlich nicht-funktionaler Anforderungen zu evaluieren. Existierende CSZ sind meist hinsichtlich der Charakteristiken dieser Dimension strukturiert (siehe hierzu bspw. EuroCloud (2011a)). Die Dimension „Vor-Ort-Auditierung“ beschreibt, ob ein Auditor vor Ort sein muss, um ein Kriterium überprüfen zu können. Daneben legt die Dimension „Auditierungsmethode“ fest, wie ein Kriterium beurteilt wird. Bei beiden Dimensionen wurde bei der Klassifizierung eine Kosten-Nutzen-Abwägung durchgeführt, um das Ziel einer möglichst kosteneffizienten Zertifizierung zu erreichen. Ferner legt die Dimension „Kontinuierliches Monitoring“ fest, ob ein Kriterium während des Betriebs von einer dritten Partei überwacht werden sollte. Hierbei wird dem Cloud-Service-Provider insbesondere unterstellt, dass er jede legale Möglichkeit zur Senkung der eigenen Kosten oder zur Verbesserung der eigenen Wettbewerbsposition ergreifen wird, auch wenn diese im Widerspruch zu einzel-

Tabelle 2: Taxonomie der CSZ-Kriterien

Dimension	Charakteristikum	Anzahl Kriterien
Kategorie	IT-Sicherheit	179
	Datenschutz	24
	Rechtliche Compliance	12
	Flexibilität	3
	Interoperabilität	7
	Verfügbarkeit	45
	Finanzielle Stabilität	1
	Kundensupport	15
	Vertragsbedingungen	42
Vor-Ort-Auditierung	Ja	203
	Nein	125
Auditierungsmethode	Interview	90
	Servicenutzung	12
	Assetprüfung	115
	Dokumentationsprüfung	108
	Automatisches Audit	3
Kontinuierliches Monitoring	Ja	37
	Nein	291
Servicemodell-Abhängigkeit	Utility-Schicht (Utility Layer)	82
	Applikationsschicht (Application Layer)	65
	Alle Schichten (All Layers)	181
Zertifiziertes Objekt	Prozess	137
	Anbiitereigenschaften	4
	Serviceeigenschaften	22
	Infrastruktur	28
	Softwarearchitektur	77
	Vertrag	52
	Personal	8

nen bereits zertifizierten Kriterien steht. Diese Widersprüche sind aufgrund der langen Gültigkeit der Zertifizierungen ohne eine kontinuierliche Überprüfung über den Inhalt der Kriterien nicht festzustellen. So wäre es bspw. denkbar, dass die Erreichbarkeit eines Teams für Security-Incident-Handling 24 Stunden an sieben Tagen der Woche gewährleistet werden muss, dies während des Zertifizierungszeitraums auch den Anforderungen entspricht, das Team jedoch aus Kostengründen nach der Zertifizierung nur noch einige Stunden in der Woche erreichbar ist. Ferner wird bei der Klassifizierung abgewogen, ob der Cloud-Service-Provider Vorteile generieren kann, wenn er gegen Zertifizierungskriterien verstößt, und ob diese Vorteile nur durch bestimmte Aufwände, bspw. einmalige Kosten, realisiert werden können. Sollten die entstehenden Aufwände gegenüber den Vorteilen überwiegen, so scheint es unwahrscheinlich, dass der Cloud-Service-Provider eine Änderung und somit einen Verstoß gegen ein Kriterium vornehmen wird. Hingegen scheint eine kontinuierliche Auditierung bei kontinuierlich oder regelmäßig durchzuführenden Aufgaben des Cloud-Service-Provider sinnvoll. Des Weiteren beschreibt die Dimension „Servicemodell“, welches Cloud-Computing-Servicemodell bzw. welche Schicht zertifiziert werden muss, damit das Kriterium bestätigt werden kann. Da Cloud-Services aus einer stufenförmigen Struktur von Infrastruktur, Plattform und Software-Services aufgebaut sein können, kann es vorkommen, dass einige Kriterien von dem Infrastruktur-Provider (bspw. die Rechenzentrumssicherheit) gewährleistet werden müssen. Wenn ein SaaS-Provider Services eines IaaS-Providers nutzt, muss daher das Kriterium der Utility-Schicht beim IaaS-Provider zertifiziert sein. Im Folgenden subsumieren wir PaaS und IaaS als Utility-Schicht, da die Unterscheidung zwischen PaaS und IaaS nicht eindeutig ist und sich beide Modelle ähneln, insbesondere hinsichtlich Zertifizierungskriterien (siehe hierzu auch Armbrust et al. (2010)). Die letzte Dimension „Zertifiziertes Objekt“ beschreibt, welche Art von Entität zertifiziert wird, bspw. ein Prozess, Vertrag oder Software.

Jedes Kriterium wurde einer Dimension und einem Charakteristikum zugeordnet. Betrachtet man zum Beispiel das Kriterium: *„Ist eine redundante Auslegung aller wichtigen Versorgungskomponenten für das Rechenzentrum, beispielsweise Strom, Klimatisierung, Internetanbindung, Verkabelung, etc.,*

vorhanden?“, so ist es das Ziel, die Verfügbarkeit sicherzustellen, indem vor Ort eine Assetprüfung der Infrastruktur und somit der Utility-Schicht eines Cloud-Services durchgeführt wird. Ein kontinuierliches Monitoring scheint in diesem Fall nicht vonnöten. Der gesamte Kriterienkatalog ist in Schneider/Sunyaev (2015) zu finden.

20.4 Zusammenfassung der Marktunterstützung durch Zertifizierungen

Unternehmen haben immer noch Hemmungen bei der Adoption von Cloud-Services (Schneider/Sunyaev 2014). Viele Cloud-Computing-Angebote sind für Anwender intransparent und es liegen große Informationsasymmetrien zwischen Anbieter und Anwender vor. Anwendern aus dem deutschen Mittelstand mangelt es an geeigneten, qualifizierten, vertrauenswürdigen Vorgehensweisen und Informationen, um Cloud-Services hinsichtlich ihrer individuellen Vorteilhaftigkeit und den damit verbundenen Risiken zu bewerten. Es mangelt insbesondere mittelständischen Anwendern an Möglichkeiten und Metriken, die Qualität von Cloud-Services hinreichend gut bewerten und verschiedene Services miteinander vergleichen zu können.

Unternehmen, die ihre Prozesse und Daten in die Cloud auslagern möchten oder planen, Cloud-Services zu integrieren, müssen ein umfassendes Verständnis über mögliche Risiken von Cloud-Services entwickeln, um so Gefahren besser beurteilen und ggf. auf ihren Eintritt angemessen reagieren zu können (Heiser/Nicolett 2008). So zeigte sich auch, dass die Mehrheit der Unternehmen Cloud-Computing erst dann nutzen wird, wenn ein umfassendes Wissen über eine Vielzahl von Risiken aufgebaut wurde (Viega 2009). Auf der anderen Seite müssen auch Cloud-Service-Provider ein umfassendes Verständnis von Risiken besitzen, um Vorkehrungen zur Vermeidung oder Kompensation dieser Risiken zu treffen. Wenn sie bspw. nachweisen können, dass sie es durch spezielle Sicherheitsmaßnahmen schaffen, eine Auswahl von Risiken zu minimieren, kann dies als Alleinstellungsmerkmal oder Wettbewerbsvorteil angesehen werden (Subashini/Kavitha 2011; Sturm et al. 2014). An diesem Punkt können Cloud-Service-Zertifizierungen den Markt unterstützen. Damit können neben einer Risikominimierung auch Transpa-

renz und ein erhöhtes Vertrauen für Cloud-Service-Nutzer durch Zertifizierungen geschaffen werden.

Die im Projekt Value4Cloud erzielten Ergebnisse adressieren diese Herausforderungen mittelständischer Unternehmen bei der Beschaffung von Cloud-Services ganzheitlich, indem ein Rahmenwerk zur Zertifizierung von Cloud-Services deren Nutzer bei der Auswahlentscheidung unterstützt und die Bewertung von existierenden CSZ erleichtert. Cloud-Service-Provider haben die Möglichkeit, ihre Services anhand der Vorgaben im Zertifizierungsrahmenwerk auf den Prüfstand zu stellen und entsprechend anzupassen. Cloud-Service-Zertifizierungsinstitutionen können ihre zugrunde liegenden Rahmenwerke mit dem Value4Cloud-Rahmenwerk abgleichen und Gestaltungsempfehlungen (siehe Kapitel 12) umsetzen. Zukünftige Forschung im Bereich der CSZ beschäftigt sich unter anderem mit der Umsetzung einer kontinuierlichen Auditierung von Cloud-Services und baut auf dem im Forschungsprojekt Value4Cloud erarbeiteten Kriterienkatalog auf (siehe u.a. Lins et al. (2015)).

20.5 Literaturverzeichnis

- Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; Zaharia, M. (2010):** A view of cloud computing. In: Communications of the ACM, Vol. 53 (2010) No. 4, S. 50–58.
- Badger, L.; Grance, T.; Patt-Corner, R.; Voas, J. (2012):** Cloud Computing Synopsis and Recommendations. Recommendations of the National Institute of Standards and Technology, <http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf>, zugegriffen am 28.07.2014.
- Bernnat, R.; Zink, W.; Bieber, N.; Strach, J.; Tsai, S. (2012):** Das Normungs- und Standardisierungsumfeld von Cloud Computing. [http://trusted-cloud.de/media/content/20111222_BMWi_Cloud_Standards_Studie_Abschlussbericht_\(FINAL\).pdf](http://trusted-cloud.de/media/content/20111222_BMWi_Cloud_Standards_Studie_Abschlussbericht_(FINAL).pdf), zugegriffen am 28.07.2014.
- Bundesministerium für Bildung und Forschung (2012):** Bekanntmachung des Bundesministeriums für Bildung und Forschung von Richtlinien zur Förderung von Forschungsinitiativen zum Sicheren Cloud Computing. <http://www.bmbf.de/foerderungen/18899.php>, zugegriffen am 28.07.2014.
- Bundesministerium für Sicherheit in der Informationstechnik (2011):** Sicherheitsempfehlungen für Cloud Computing Anbieter. http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile, zugegriffen am 28.07.2014.

- Cloud-Computing Use Cases Discussion Group (2010):** Cloud Computing Use Cases. http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf, zugegriffen am 28.07.2014.
- Cloud Security Alliance (2011):** Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>, zugegriffen am 28.07.2014.
- EuroCloud (2011a):** EuroCloud Star Audit. <http://www.eurocloud-staraudit.eu/>, zugegriffen am 28.07.2014.
- EuroCloud (2011b):** Leitfaden Cloud Computing Recht, Datenschutz und Compliance. <http://www.eurocloud.de/2010/news/datensicherheit/eurocloud-leitfaden-recht-datenschutz-compliance.html>, zugegriffen am 28.07.2014.
- European Commission (2012):** Unleashing the Potential of Cloud Computing in Europe. http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf, zugegriffen am 02.10.2012.
- Gao, F.; Schneider, S. (2012):** Cloud-Frameworks: Eine Übersicht aus der Wirtschaftsinformatik-Perspektive. Präsentiert auf der ConLife Academic Conference 2012, Köln, Deutschland, S. 1–16.
- Glass, R.L.; Vessey, I. (1995):** Contemporary Application-Domain Taxonomies. In: IEEE Software, Vol. 12 (1995) No. 4, S. 63–76.
- Grochol, P.; Schneider, S.; Sunyaev, A. (2014):** Cutting through the Jungle of Cloud Computing Whitepapers: Development of an Evaluation Model. In: Trusted Cloud Computing, H. Krcmar, R. Reussner and B. Rumpe (eds.), Berlin: Springer, pp. 315–331.
- Heiser, J.; Nicolett, M. (2008):** Assessing the Security Risks of Cloud Computing. Gartner, I. In: <http://www.globalcloudbusiness.com/SharedFiles/Download.aspx?pageid=138&mid=220&fileid=12>, zugegriffen am 28.07.2014.
- International Organization for Standardization (2005):** ISO/IEC 27001:2005: Information technology – Security techniques – Information security management systems – Requirements, 2005.
- Khan, K.M.; Malluhi, Q. (2010):** Establishing Trust in Cloud Computing. In: IT Professional, Vol. 12 (2010) No. 5, S. 20–27.
- Kim, D.; Benbasat, I. (2009):** Trust-Assuring Arguments in B2C E-commerce: Impact of Content, Source, and Price on Trust. In: Journal of Management Information Systems, Vol. 26 (2009) No. 3, S. 175–206.
- Lansing, J.; Schneider, S.; and Sunyaev, A. (2013):** Cloud Service Certifications: Measuring Consumer's Preferences for Assurance. In: Präsentiert auf der 21th European Conference on Information Systems, Utrecht, Niederlande.
- Lins, S.; Thiebes, S.; Schneider, S.; and Sunyaev, A. (2015):** What Is Really Going on at Your Cloud Service Provider? Creating Trustworthy Certifications by Continuous Auditing. In: Präsentiert auf der 48th Hawaii International Conference on System Sciences, Kauai, Hawaii, USA.
- Nickerson, R.C.; Varshney, U.; Muntermann, J. (2013):** A method for taxonomy development and its application in information systems. In: European Journal of Information Systems, Vol. 22 (2013) No. 3, S. 1–24.

- Schneider, S.; Lansing, J.; Gao, F.; Sunyaev, A. (2014):** A Taxonomic Perspective on Certification Schemes: Development of a Taxonomy for Cloud Service Certification Criteria. Präsentiert auf der 47th Hawaii International Conference on System Sciences, Big Island, Hawaii, USA.
- Schneider, S.; Lansing, J.; Sunyaev, A. (2013):** Empfehlungen zur Gestaltung von Cloud-Service-Zertifizierungen. In: *Industrie Management*, Vol. 11 (2013) No. 4, S. 13–17.
- Schneider, S.; Sunyaev, A. (2014):** Determinant Factors of Cloud-Sourcing Decisions: Reflecting on the IT Outsourcing Literature in the Era of Cloud Computing. In: *Journal of Information Technology* (advance online publication), DOI: 10.1057/jit.2014.25, S. 1–31.
- Schneider, S.; Sunyaev, A. (2015):** Cloud-Service-Zertifizierung: Ein Rahmenwerk und Kriterienkatalog zur Zertifizierung von Cloud-Services, Springer, Berlin, Deutschland.
- Stein, F.; Schneider, S.; Sunyaev, A. (2012):** ITIL als Grundlage zur Zertifizierung von Cloud-Services und -Anbietern. In: *HMD – Praxis der Wirtschaftsinformatik*, Vol. 288 (2012), S. 33–41.
- Sturm, B.; Lansing, J.; Sunyaev, A. (2014):** Moving in the Right Direction?: Mapping Literature on Cloud Service Certifications' Outcomes with Practitioners' Perceptions. Präsentiert auf der 22th European Conference on Information Systems, Tel Aviv, Israel.
- Subashini, S.; Kavitha, V. (2011):** A survey on security issues in service delivery models of cloud computing. In: *Journal of Network and Computer Applications*, Vol. 34 (2011) No. 1, S. 1–11.
- Sunyaev, A.; Schneider, S. (2013):** Cloud Services Certification. In: *Communications of the ACM*, Vol. 56 (2013) No. 2, S. 33–36.
- Viega, J. (2009):** Cloud Computing and the Common Man. In: *Computer*, Vol. 42 (2009) No. 8, S. 106–108.
- Wand, Y.; Monarchi, D.E.; Parsons, J.; Woo, C.C. (1995):** Theoretical foundations for conceptual modelling in information systems development. In: *Decision Support Systems*, Vol. 15 (1995) No. 4, S. 285–304.

21 Markunterstützung durch vertrauensunterstützende Dienste

L. Gebauer, M. Söllner, J.M. Leimeister

21.1 Einleitung

Die Inhalte, die in diesem Kapitel berichtet werden, basieren auf den Publikationen von Buch/Gebauer (2013). und Buch et al. (2014). Dieses Kapitel präsentiert die Inhalte dieser beiden Publikationen in verkürzter und zusammenfassender Form. Detaillierte Ergebnisse finden Sie in den Publikationen.

21.2 Durchführung von Experteninterviews

Das Kapitel liefert Anregungen, welche Maßnahmen Cloud-Computing-Anbieter durchführen können, um das Vertrauen der (potenziellen) Nutzer in sie und ihre Dienste zu fördern. Dazu wurden Interviews mit Cloud-Computing-Experten durchgeführt, da diese über besonders viel Erfahrungen und Wissen in dem Themenfeld verfügen. Auch sind Experten täglich mit den Unsicherheiten und den Nutzungshemmnissen der (potenziellen) Kunden konfrontiert und somit ständig auf der Suche nach geeigneten Lösungsmöglichkeiten.

Insgesamt wurden Interviews mit elf Cloud-Computing-Experten durchgeführt (siehe auch Buch/Gebauer 2013; Buch et al. 2014). Die Experten waren alle im Themenfeld des Cloud-Computing beschäftigt, entweder als Analysten bei Beratungsfirmen, bei Forschungseinrichtungen oder als Mitarbeiter bei Cloud-Computing-Anbietern. Mit Hilfe der Interviews wurden Maßnahmen identifiziert, die von den Experten als vertrauensförderlich angesehen werden.

21.3 Ableitung und Priorisierung vertrauensförderlicher Faktoren

Die befragten Experten verfügten über ausreichend Wissen im Bereich des Cloud-Computing, hatten jedoch keinen theoretischen Wissenshintergrund zur Entstehung von Vertrauen. Daher wurden mit Hilfe einer Literaturrecherche neun Faktoren identifiziert, die das Vertrauen in Dienstleistungen beeinflussen (Buch/Gebauer 2013). Diese neun Faktoren wurden den Experten vorgelegt, um zu beurteilen, welche der Faktoren für die Bildung von Vertrauen in Cloud-Computing von Bedeutung sind. Gleichzeitig sollten die Experten auf einer fünfstufigen Skala (von „unwichtig“ bis „sehr wichtig“) einschätzen, wie bedeutsam ihrer Meinung nach jeder einzelne Faktor für das Vertrauen in Cloud-Computing ist, und klassifizieren, ob der Faktor relevant ist für das interpersonelle Vertrauen, das Systemvertrauen oder beides.

Die Auswertung der Experteninterviews ergab, dass sieben der neun Faktoren von den Experten als wichtig für den Aufbau von Vertrauen in Cloud-Computing-Dienste erachtet wurden (Buch/Gebauer 2013; Buch et al. im Druck). Die Faktoren sind absteigend nach dem Mittelwert (MW) der Relevanz-Bewertung sortiert. Die Experten klassifizierten keinen der sieben Faktoren als ausschließlich dem interpersonellen Vertrauen zugehörig. Die Auswertung ergab, dass folgende Faktoren nach Meinung der Experten sowohl das interpersonelle Vertrauen als auch das Systemvertrauen beeinflussen:

- *Qualität der Dienstleistung* (MW = 3,82): umfasst Aspekte, die herangezogen werden, um Rückschlüsse auf die Qualität der Dienstleistung und dessen Anbieter zu ziehen, bspw. Pünktlichkeit, die Verfügbarkeit, die Zuverlässigkeit.
- *Frühere Erfahrungen mit dem Dienstleister* (MW = 3,36): umfasst alle früheren Erfahrungen, die der potenzielle Kunde zuvor schon selbst mit dem Dienstleister gemacht hat.
- *Empfehlungen Dritter* (MW = 2,82): umfasst alle persönlichen Empfehlungen, die der potenzielle Kunde von Dritten erhalten hat, wie zum Beispiel von Kollegen, Freunden oder von eingestellten Beratern.

- *Kundenorientierung des Dienstleisters* (MW = 2,55): umfasst, inwieweit der Dienstleister sich auf seine Kunden einstellt und auf dessen Wünsche eingeht.

Weiterhin ergab die Auswertung, dass nach Meinung der Experten folgende Faktoren ausschließlich das Systemvertrauen beeinflussen:

- *Datensicherheit* (MW = 3,73): beinhaltet, dass alle die Dienstleistung betreffenden Daten sowie die verarbeiteten Daten vor Zugriffen von Dritten sowie vor Verlust geschützt sind.
- *Reputation* (MW = 2,55): gibt die öffentliche Meinung über den Dienst wieder und wird als der Ruf des Unternehmens verstanden, welcher in Form von generellen Einstellungen und Gefühlen gegenüber dem Dienst zum Ausdruck kommt.
- *Customizing* (MW = 2,27): umfasst, inwieweit die Dienstleistung auf die Kundenwünsche angepasst werden kann.

Aufbauend auf diesen Faktoren wurden die Experten gebeten, in einem zweiten Schritt Maßnahmen abzuleiten, von denen sie annehmen, dass diese die Faktoren adressieren und somit vertrauensförderlich wirken.

21.4 Ableitung und Priorisierung vertrauensförderlicher Maßnahmen

Um die sieben vertrauensbeeinflussenden Faktoren zu adressieren, haben die Experten insgesamt 35 verschiedene Maßnahmen ([Tabelle 1](#)) zur Förderung des Vertrauens in Cloud-Computing-Dienste und deren Anbieter identifiziert (Buch et al. im Druck). Anhand der Zuordnung der Einflussfaktoren zu den Vertrauenskomponenten *interpersonelles Vertrauen* und *Systemvertrauen* ist erkennbar, mit Hilfe welcher Maßnahmen die Vertrauenskomponenten adressiert werden können. Dabei ist zu beachten, dass nach der Meinung der Experten einige Maßnahmen mehrere vertrauensbeeinflussende Faktoren und damit auch unterschiedliche Vertrauenskomponenten adressieren. Im Detail wird nur auf die vier Maßnahmen eingegangen, die mehrere vertrauensbeein-

Tabelle 1: Vertrauensunterstützende Maßnahmen für Cloud-Computing
(Quelle: Buch et al. 2014)

Einflussfaktoren für die Vertrauenskomponenten: Cloud-spezifische vertrauens- beeinflussende Faktoren Vertrauens- unterstützende Maßnahmen	Interpersonelles Vertrauen & Systemvertrauen				System-vertrauen			Summe Mittelwerte
	Qualität der Dienstleistung	Frühere Erfahrungen	Empfehlungen Dritter	Kunden-orientierung	Datensicherheit	Reputation	Customizing	
Zertifizierungen	x				x	x		10,1
SLAs	x			x				6,37
Referenzen			x				x	5,09
Checkliste des Angebots				x			x	4,82
Problemhotlines	x							3,82
Qualitätskriterien	x							3,82
Besichtigung der RZ					x			3,73
Deutscher Rechtsraum					x			3,73
Deutsches Rechenzentrum					x			3,73
Honeypots					x			3,73
Initiativen beitreten					x			3,73
Physische Sicherheit der RZ					x			3,73
Redundante Datenhaltung					x			3,73
Sicherheitsarchitektur					x			3,73
Fehlerszenarien durchspielen		x						3,36
Prüfung der Servicehotlines		x						3,36
Trialversionen anbieten		x						3,36
Vorabbesichtigung der RZ		x						3,36
Einsatz von Social Media			x					2,82

Einflussfaktoren für die Vertrauenskomponenten:		Interpersonelles Vertrauen & Systemvertrauen				Systemvertrauen			
Vertrauensunterstützende Maßnahmen	Cloud-spezifische vertrauensbeeinflussende Faktoren	Qualität der Dienstleistung	Frühere Erfahrungen	Empfehlungen Dritter	Kundenorientierung	Datensicherheit	Reputation	Customizing	Summe Mittelwerte
Empfehlungsbasiertes Marketing			x						2,82
Fachartikel			x						2,82
Kundenveranstaltungen			x						2,82
Sicherheitsüberprüfungen			x						2,82
Social Media Monitoring			x						2,82
24x7 Servicedesk				x					2,55
Arbeit mit Marktanalysten						x			2,55
Ehrliche Angebote				x					2,55
ITIL				x					2,55
persönliche Ansprechpartner				x					2,55
Signalling						x			2,55
Transparenz schaffen						x			2,55
User-Helpdesk				x					2,55
Anpassung durch den Kunden							x		2,27
Einfache Migration							x		2,27
Individualisierungsgrad anpassen							x		2,27
Anzahl Maßnahmen pro Faktor	4	4	7	7	9	4	5		

flussende Faktoren adressieren. Detaillierte Beschreibungen aller 35 Maßnahmen finden sich in dem Beitrag von Buch et al. (2014).

Die bedeutsamste vertrauensförderliche Maßnahme nach der Einschätzung der Experten ist „Zertifizierung“. Das bedeutet, dass es vertrauensför-

derlich für den (potenziellen) Cloud-Computing-Nutzer wirkt, wenn sich das Unternehmen von einer externen Institution zertifizieren lässt (siehe Kapitel 12 und 20). Die Experten sehen „Zertifizierung“ dabei als eine Maßnahme zur Adressierung der vertrauensbeeinflussenden Faktoren „Qualität der Dienstleistung“, „Datensicherheit“ und „Reputation“. Die Reputation wird gestärkt, da die Zertifizierung meist durch eine anerkannte unabhängige Institution erfolgt. Eine Zertifizierung der Geschäftsprozesse, Rechenzentren und Mitarbeiter signalisiert dem Kunden, dass in dem Unternehmen qualitativ hochwertig gearbeitet wird. Damit kann aus der Sicht des Kunden Zertifizierung ebenfalls als ein Kennzeichen für die „Qualität der Dienstleistung“ und der „Datensicherheit“ gewertet werden.

Als eine weitere Möglichkeit, das Vertrauen der (potenziellen) Nutzer zu fördern, sahen die Experten die Verwendung von Service-Level-Agreements (SLAs). Diese sollten nach Meinung der Experten einfach und gut strukturiert sein, sowie alle wichtigen Details in ausformulierter Form enthalten. Diese dienen damit als Merkmal für die „Qualität der Dienstleistung“ und der „Kundenorientierung“ des Anbieters.

Durch die Maßnahme „Referenzen“ adressieren die Experten zwei vertrauensbeeinflussende Faktoren: „Empfehlungen Dritter“ und „Customizing“. Dementsprechend können Referenzen dazu dienen, den Empfehlungen Dritter Ausdruck zu verleihen und um dem (potenziellen) Kunden zu zeigen, dass bereits andere Kunden mit dem Angebot zufrieden waren. Die Darstellung von Referenzen ist auch eine Möglichkeit, dem vertrauensbeeinflussenden Faktor „Customizing“ Ausdruck zu verleihen. Nach Meinung der Experten kann durch das Aufzeigen verschiedenster Referenzen dem Kunden die gesamte Bandbreite des möglichen Angebots aufgezeigt werden.

Die von den Experten abgeleitete vertrauensförderliche Maßnahme „Checkliste des Angebots“ umschreibt die Aufstellung einer übersichtlichen Liste, die alle möglichen Angebote des Cloud-Computing-Anbieters enthält, um den (potenziellen) Kunden die gesamte Bandbreite des Angebots übersichtlich darlegen zu können. Mit dieser Maßnahme adressieren die Experten die vertrauensbeeinflussenden Faktoren „Kundenorientierung“ und „Customizing“, da dem Kunden schnell und übersichtlich dargelegt wird, welche

Angebote möglich sind und ob der Anbieter seinen Bedürfnissen gerecht werden kann.

21.5 Zusammenfassung

Um die Anbieter von Cloud-Computing-Diensten zu unterstützen, wurden mit Hilfe der Befragung von Cloud-Computing-Experten insgesamt 35 Maßnahmen zur Förderung des Vertrauens von (potenziellen) Kunden abgeleitet (vgl. Buch et al. im Druck; Buch/Gebauer 2013).

Die Auswertung der Experteninterviews zeigt, dass vor allem Maßnahmen zur Steigerung der Transparenz (wie Angebots-Checklisten und SLAs), zur Sicherstellung der Qualität des Dienstes und Reputationen durch Dritte (wie Referenzen und Zertifizierung) von enormer Bedeutung sind, um das Vertrauen in den Cloud-Computing-Dienst und dessen Anbieter zu fördern.

21.6 Literaturverzeichnis

- Buch, M.; Gebauer, L. (2013):** Maßnahmenkatalog zur Vertrauenserrhöhung im Cloud Computing. In: Leimeister, J.M. (Hrsg.), (4. Aufl.). Kassel, Deutschland: Working Paper Series, Chair for Information Systems, Kassel University.
- Buch, M.; Gebauer, L.; Hoffmann, H. (2014):** Vertrauen in Cloud Computing schaffen – Aber wie? In: WIRTSCHAFTSINFORMATIK & MANAGEMENT, Vol. 03/2014 (2014), S. 67–77.

22 Markunterstützung durch Open-Service-Innovation

Die Bedeutung von Ideenwettbewerben in Online-Communities für Open Service Innovation in Bezug auf die Stakeholder des Cloud-Computing-Ökosystems

M. Kunz, P. Ebel, J.M. Leimeister

22.1 Einleitung

Dieses Kapitel beschreibt eine Methode für die Integration von Kunden und anderen Stakeholdern des Cloud-Computing in den so genannten „online-basierten Ideenentwicklungsprozess“. In einem ersten Abschnitt werden dazu die Funktionsweise und die Einsatzgebiete von Ideenwettbewerben dargestellt. Die Einordnung des Ideenwettbewerbs in den Innovationsprozess erfolgt in einem zweiten Abschnitt und zeigt die bedeutende Rolle, die Ideenwettbewerbe, insbesondere bei Innovationen im Bereich des Cloud-Computing, spielen können. Ein dritter Abschnitt gibt einen Überblick über die Charakteristika der Cloud-Computing-Stakeholder. In einem letzten Abschnitt werden auf Basis des modellhaften Ablaufs eines Ideenwettbewerbs spezifische Anforderungen an die Durchführung von Ideenwettbewerben im Cloud-Computing-Umfeld erarbeitet.

22.2 Funktionsweise und Einsatzgebiete von Ideenwettbewerben

Der Ideenwettbewerb ist eine Methode zur Kundenintegration, die insbesondere in frühen Phasen des Innovationsprozesses Anwendung findet. Die Kunden des innovationstreibenden Unternehmens werden dabei durch eine konkrete Aufgabenstellung aufgefordert, innerhalb eines bestimmten Zeitraums innovative Ideen einzureichen, die einen engen Bezug zum Produkt

des Unternehmens oder zu dem direkten Unternehmensumfeld haben (Ebner 2008). Der Ideenwettbewerb erhält seinen Wettbewerbscharakter durch die von einer (Experten-)Jury vorgenommene Evaluation der Ideen und die anschließende leistungsorientierte Prämierung. Auf diese Weise werden Anreize zur Teilnahme am Ideenwettbewerb – insbesondere durch die leistungsorientierte Prämierung – und zur Einreichung kreativer Ideen mit hoher Qualität gesetzt (Reichwald et al. 2009).

Ideenwettbewerbe werden in der Regel internetbasiert über eine IT-gestützte Plattform durchgeführt (Leimeister/Bretschneider 2012). So können sie einem breiten Nutzerkreis kostengünstig zugänglich gemacht werden. Ebenfalls können komplexe Zusammenhänge durch multimediale Inhalte nutzerfreundlich dargestellt werden (Walcher 2006). IT-gestützte Internetplattformen ermöglichen die Einrichtung von Vernetzungsaktivitäten, mithilfe derer die Ideen gemeinschaftlich weiterentwickelt werden können (Leimeister 2014). Durch Vernetzung und Kollaboration steigt die Qualität der eingereichten Ideen (Bretschneider et al. 2007). Ideenwettbewerbe bieten (für das Produktmanagement) Potenziale in doppelter Hinsicht. So können Innovationsideen einerseits zur Verbesserung oder Modifizierung (Top-Down-Ansatz von Ideenwettbewerben) von bestehenden Produkten beitragen; andererseits kann auch die Einführung gänzlich neuer Produkte im Sinne „radikaler Innovationen“ (Bottom-Up-Ansatz von Ideenwettbewerben) initiiert werden (Bretschneider et al. 2007). Ideenwettbewerbe können entlang der Dimensionen Aufgabenspezifität und Ausarbeitungsgrad systematisiert werden (Walcher 2006). Die Dimension der Aufgabenspezifität beschreibt den Detaillierungsgrad der Ausschreibung. Die Aufgabenspezifität muss in Abhängigkeit von dem Ziel des Ideenwettbewerbs gewählt werden. So eignen sich detailliert beschriebene Aufgaben vor allem für die Modifizierung und Verbesserung, während breit beschriebene Aufgaben auch die Einbringung radikaler Innovationen ermöglichen. Die Dimension des Ausarbeitungsgrads bezieht sich auf die Anforderungen an Qualität, Umfang und Beschaffenheit der Aufgaben. Je höher die Anforderungen sind, die an die Ausarbeitung gestellt werden, desto qualitativ hochwertiger sind die Ideen, die das Unternehmen erwarten kann. Allerdings können höhere Anforderungen auch eine hemmende (abschreckende) Wirkung haben und damit den Ideenpool verkleinern.

22.3 Einordnung in den Innovationsprozess

Obwohl empirische Untersuchungen vielfach gezeigt haben, dass Innovationsprozesse nicht linear verlaufen, werden Innovationsprozesse aufgrund des Abstrahierungsbedürfnisses von Modellen meist in linearen Phasenmodellen dargestellt (Walcher 2006). In der Literatur finden sich zahlreiche dieser Phasenmodelle (Walcher 2006).

Herstatt und Verworn (2007) unterscheiden in einem fünfstufigen Innovationsmodell beispielsweise die Phasen der Ideengenerierung und -bewertung, der Konzepterarbeitung, der Entwicklung, des Prototypenbaus und der Markteinführung. Die ersten beiden Phasen können unter dem Oberbegriff „frühe Phasen“ zusammengefasst werden (Herstatt/Verworn 2007). Die frühen Phasen beinhalten diejenigen Aktivitäten, die vor dem eigentlichen Projektstart durchgeführt werden (Khurana/Rosenthal 1998). Die Unterschiede zwischen den einzelnen Phasenmodellen können bei der Betrachtung der Ideenwettbewerbe vernachlässigt werden. Es genügt die Feststellung, dass die meisten dieser Phasenmodelle den Innovationsprozess in eine frühe und eine späte Phase einteilen (Dorbrandt et al. 1990), die allerdings in der Literatur mit einer Reihe unterschiedlicher Begriffe bezeichnet werden (Khurana/Rosenthal 1998).

Ideenwettbewerbe werden vor allem in der frühen Phase des Innovationsprozesses eingesetzt. In dem oben genannten Phasenmodell nach Herstatt/Verworn (2007) sind sie in erster Linie im Bereich der Ideengenerierung anzusiedeln (Herstatt/Verworn 2007; Walcher 2006). Kunden können prinzipiell in jede Phase des Innovationsprozesses integriert werden. Da der Aufwand, den Kunden investieren müssen, entlang des Innovationsprozesses zunimmt, müssen aber in späteren Phasen höhere Anreize für die Einbindung gesetzt werden. Die Kosten für die Kundenintegration steigen folglich im Laufe des Innovationsprozesses (Bretschneider et al. 2007). Den frühen Innovationsphasen kommt weiterhin im Hinblick auf den Innovationserfolg eine entscheidende Bedeutung zu. So haben Bürgel und Zeller (1997) festgestellt, dass 75 bis 85 % der Produktlebenskosten und 70 % der Qualität durch die frühen Innovationsphasen determiniert werden, gleichzeitig aber nur 5 bis 7 % der Gesamtkosten anfallen (Bürgel/Zeller 1997). Dies bestärkt nochmals die Aussage der frühzeitigen Einbindung des potenziellen Kunden

in den Innovationsprozess von Produkten und Services, da so von Beginn an die Qualität eines Produktes oder Services zu möglichst niedrigen Kosten für das Unternehmen vom Kunden selbst definiert und ausgestaltet werden kann. Ideenwettbewerbe stellen somit eine wertvolle Methode dar, um der enormen Bedeutung dieser frühen Innovationsphasen Rechnung zu tragen.

Mit Blick auf das Cloud-Computing kommt dem Ideenwettbewerb so eine besondere Relevanz zu. Durch die frühe systematische Bedürfnisermittlung des potenziellen Kundenkreises kann das Risiko gesenkt werden, dass an den Bedürfnissen der Kunden „vorbei innoviert“ wird (Bretschneider et al. 2007). Die Unsicherheitsfaktoren der Zahlungsbereitschaft potenzieller Cloud-Nutzer sowie deren Erwartungshaltung, beispielsweise bezüglich des Datenschutzes, der Skalierbarkeit und der einzelnen Funktionen, können durch die Durchführung eines Ideenwettbewerbs verringert werden. Ideenwettbewerbe können dazu beitragen, die Bedürfnisermittlung zu systematisieren. Auf Basis der Bedürfnisermittlung können Potenziale für neue, vielversprechende und auch radikale Innovationen ausgemacht werden.

Wie aus den obigen Ausführungen hervorgeht, stellt der Ideenwettbewerb ein vielversprechendes Mittel dar, um den eigenen Innovationsprozess für externe Stakeholder zu öffnen. Grundvoraussetzung für den Erfolg eines Ideenwettbewerbes bildet jedoch erst die genaue Kenntnis der zu integrierenden Stakeholder. Aus diesem Grund sollen deren Charakteristika im Rahmen des nächsten Abschnitts genauer beleuchtet werden.

22.4 Die Cloud-Computing-Stakeholder

Aus der Gruppe der Stakeholder im Cloud-Computing-Umfeld sind für die Betrachtung von Ideenwettbewerben vor allem die Kunden des Cloud-Anbieters von Bedeutung. Die potenziellen Kunden eines Cloud-Anbieters lassen sich in die Kategorien Business-to-Business (B2B), Business-to-Consumer (B2C) und Business-to-Government (B2G) unterteilen. B2B-Kunden können weiter in kleine und mittelständische Unternehmen (KMU) und Großunternehmen differenziert werden. Unterschiede zwischen diesen beiden Arten von B2B-Kunden bestehen beispielsweise im Hinblick auf folgende vier Merkmale:

- *Unternehmensführung und Organisation*: KMU werden häufig vom Unternehmer selbst oder von einem durch den Unternehmer ausgewählten Geschäftsführer geleitet, während in Großunternehmen Manager für die Unternehmensleitung eingesetzt werden (Pichler et al. 1997). Hieraus resultiert, dass in Großunternehmen tendenziell eher betriebswirtschaftlich fundierte Entscheidungen getroffen werden als in KMU. Mittelständische Unternehmen gelten zudem als wenig professionell; sie werden „aus dem Bauch heraus“ geführt (Wolf et al. 2009). Ob die Entscheidungsqualität in KMU, verglichen mit der Entscheidungsqualität in Großunternehmen, deswegen schlechter oder gleichwertig ist, ist in der Literatur umstritten (Martin/Bartscher-Finzer 2006). Aus Sicht des Cloud-Anbieters resultiert aus dieser Feststellung vor allem, dass bei KMU neben rationalen Erwägungen auch emotionale Faktoren, beispielsweise ein Misstrauen gegenüber Cloud-Anbietern, verstärkt in die Entscheidungsfindung einfließen.
- *Standortwahl*: KMU wählen wegen der geringeren Gewerbesteuer und den geringeren Grundstücks- sowie Mietpreisen häufig einen Sitz in ländlichen Regionen (Wolf et al. 2009). In diesen Regionen kann die Abdeckung mit – für die komplexen Dienstleistungen des Cloud-Computing benötigtem – Breitband-Internet problematisch sein.
- *Flexibilität*: Die Möglichkeit für KMU, auf Marktveränderungen und Konkurrenzsituationen flexibel zu reagieren, kann einen entscheidenden Wettbewerbsvorteil gegenüber Großunternehmen darstellen (Blaeser-Benfer 2009). Dieses Flexibilitätsbedürfnis kann von Cloud-Betreibern als wesentliches Argument für die Nutzung von Cloud-Services angebracht werden.
- *Einsparpotenziale*: Cloud-Computing bietet aufgrund der dynamischen Nutzung von IT-Ressourcen Einsparpotenziale (Armbrust et al. 2010; Mell/Grance 2011). Der Wegfall des mit hohen Anfangsinvestitionen verbundenen Aufbaus einer eigenen IT-Infrastruktur kann aufgrund des schwierigeren Zugangs zu Kapitalmärkten insbesondere für KMU ein zentrales Argument für das Cloud-Computing darstellen. Dass sich einige nicht cloud-basierte IT-Dienstleistungen erst ab einer gewissen Unter-

nehmensgröße lohnen, kann ein weiteres Argument für den Einsatz von Cloud-Computing in KMU darstellen.

Die Zielgruppe der B2C-Kunden unterscheidet sich deutlich von den B2B-Kunden. IT kommt in Privathaushalten in einem deutlich geringeren Umfang zum Einsatz. Cloud-Computing wird hier vor allem für die Datensicherung, für die Verwendung von Daten auf verschiedenen Geräten und für den Austausch der Daten mit anderen Nutzern eingesetzt. Sowohl B2B- als auch B2C-Kunden stellen eine interessante Zielgruppe für die Durchführung von Ideenwettbewerben dar.

22.5 Ablauf des Ideenwettbewerbs

Der Ablauf eines Ideenwettbewerbs wird nach Bretschneider et al. (2007) in fünf Schritten systematisch dargestellt.

In einem ersten Schritt („Zieldefinition“) werden die Ziele des Ideenwettbewerbs diskutiert und festgelegt. Hierbei ist vor allem zu entscheiden, ob mit dem Ideenwettbewerb eine radikale Innovation oder lediglich eine Modifizierung erreicht werden soll. Auch muss die Dauer des Ideenwettbewerbs bestimmt werden. Die Wahl der Zielgruppe stellt eine weitere wichtige Entscheidung dar. Hier sollte der Cloud-Anbieter zunächst überlegen, ob er eine B2C- oder eine B2B-Leistung anbieten möchte. Im Falle einer B2B-Leistung muss er weiterhin festlegen, ob eher KMU oder Großunternehmen angesprochen werden sollen.

In einem zweiten Schritt („Analyse“) müssen relevante soziale, ökonomische, technische und juristische Einflussfaktoren auf die zuvor definierten Ziele geprüft werden. Ein besonderer Stellenwert kommt hier der juristischen Perspektive zu. So müssen beispielsweise Regelungen zum Umgang mit den Rechten des Ideengebers an der eingereichten Idee getroffen werden. In dieser Phase wird auch der Informations- und Interaktionsbedarf der Teilnehmer analysiert. Im Bereich des Cloud-Computing hängen die Einflussfaktoren entscheidend von der zuvor definierten Zielgruppe ab. Aus technischer Sicht muss hier insbesondere auch das technische Vorwissen der potenziellen Teilnehmer berücksichtigt werden. Je nach Innovationsziel müssen die Teilneh-

mer vor Beginn des Ideenwettbewerbs mit umfassenden technischen Informationen versorgt werden.

In einem dritten Schritt („Entwicklung der Online-Plattform“) wird dann aufbauend auf den gesammelten Informationen eine Online-Community entwickelt. Diese sollte im Hinblick auf das verwendete System, die Oberflächengestaltung, die Funktionalitäten, die Inhalte sowie deren Strukturierung und die Vernetzungsmöglichkeiten individuell auf die Zielgruppe abgestimmt werden. Für das Cloud-Computing sind hier insbesondere die Darstellungsmöglichkeiten und deren Nutzerfreundlichkeit relevant, damit die Teilnehmer potenziell komplexe Ideen übersichtlich darstellen können. Einer Kommentierungs- und Bearbeitungsfunktion kommt im Hinblick auf die Steigerung der Ideenqualität besondere Bedeutung zu.

In einem vierten Schritt („Aktivierung potenzieller Teilnehmer“) müssen Kunden und andere potenzielle Teilnehmer, beispielsweise durch Anreize, aktiviert werden. Bei der Auswahl externer Anreize muss dabei der erwartete Aufwand der Kunden berücksichtigt werden. Wird eine Prämierung als externer Anreiz gewählt, sollte der Wert (und bei Sachpreisen die Art des Preises) den Aufwand und die Vorlieben der Teilnehmer berücksichtigen.

In einem letzten Schritt („Ideenbewertung“) werden die eingereichten Ideen im Hinblick auf die im ersten Schritt definierten Ziele evaluiert. Gleichzeitig werden die für den Innovationsprozess relevanten Informationen herausgefiltert. Die Bewertung der Ideenqualität stellt eine besondere Herausforderung dar, da sie zum einen komplex und zum anderen aber stets subjektiv ist. Eine Idee kann dann als qualitativ hochwertig bezeichnet werden, wenn sie neuartig, angemessen und ausgereift ist (Blohm et al. 2011). Die Neuartigkeit einer Idee beschreibt das Ausmaß, zu dem der Inhalt der Idee dem Veranstalter vor Ideenabgabe unbekannt war und zu dem die Idee etablierte Strukturen überwindet. Die Angemessenheit einer Idee beschreibt, inwiefern eine Idee für den Empfänger relevant und umsetzbar ist. Zuletzt muss die Idee ausgereift, das heißt ausreichend konkretisiert und verständlich beschrieben sein. Ideen für Cloud-Lösungen sollten anhand dieser drei Dimensionen beurteilt werden, da nur so der Wert der Idee umfassend beurteilt werden kann.

22.6 Schlussbetrachtung

In diesem Kapitel wurde die Methode der online-basierten Ideenwettbewerbe diskutiert und auf den Anwendungsbereich des Cloud-Computing übertragen. Ideenwettbewerbe können im Innovationsprozess von Unternehmen eine bedeutende Rolle einnehmen. So können sie insbesondere bei Innovationen im Bereich des Cloud-Computing, etwa bei der Entwicklung neuer radikaler Innovationen oder der Weiterentwicklung bestehender Produkte oder Services, eingesetzt werden (Leimeister 2012). Sie helfen dabei, neue, kundenspezifische Ideen in den Innovationsprozess von Produkten und Services direkt einzubeziehen. Cloud-Computing-Kunden, insbesondere im B2B-Bereich, können so direkt am Entwicklungsprozess beteiligt werden. Dies hilft dabei, Cloud-Services hinsichtlich wichtiger Merkmale wie der Sicherheit und dem Funktionsumfang gemäß der Kundenanforderungen von vornherein auszugestalten. Ein solches Vorgehen kann letztlich zu einer Steigerung der Akzeptanz neuer oder bestehender Cloud-Services führen.

Wie bereits aufgeführt spielen Ideenwettbewerbe besonders in den frühen Phasen der Innovationstätigkeit von Unternehmen eine zentrale Rolle. So können aus Kundenideen neue Lösungen entstehen oder bestehende weiter ausgearbeitet werden. Oftmals erfolgt dieser Weiterentwicklungsprozess jedoch nur innerhalb des Unternehmens selbst, ohne den weiteren Einbezug des Kunden in nachfolgende Innovationstätigkeiten. Ideenwettbewerbe stellen somit nur einen ersten Schritt in der Entwicklung vollständiger Cloud-Service-Geschäftsmodelle dar. Ideenwettbewerbe sollen daher im Aufbau einer Open Service Innovation-Online-Community für das Cloud-Ökosystem (Kap. 14) einen wichtigen integralen Bestandteil bilden. Sie fließen in die Ermittlung von Anforderungen an eine Online-Community (Kap. 7) ein. Eine solche Online-Community soll für Cloud-Nutzer und Cloud-Anbieter als Kommunikationsplattform fungieren, auf der eingereichte Ideen der Cloud-Nutzer kollaborativ zu Cloud-Service-Geschäftsmodellen ausgearbeitet werden.

22.7 Literaturverzeichnis

- Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; Zaharia, M. (2010):** A view of cloud computing. In: Communications of the ACM, Vol. 53 (2010) No. 4, S. 50-58.
- Blaeser-Benfer, A. (2009):** Innovationsstrategien von kleinen und mittleren Unternehmen im Zeichen der globalen Rezession. *White Paper*.
- Blohm, I.; Ebner, W.; Leimeister, J.M.; Krcmar, H. (2011):** Was bringen die aktivsten Teilnehmer in IT-gestützten Ideenwettbewerben? Der Einfluss von Teilnehmer-Aktivität auf Ideengenerierung und Ideenbewertung. Präsentiert auf der 73. Wissenschaftliche Jahrestagung des Verbandes der Hochschullehrer für Betriebswirtschaft e.V., Kaiserslautern, Deutschland.
- Bretschneider, U.; Ebner, W.; Leimeister, J.M.; Krcmar, H. (2007):** Internet-basierte Ideenwettbewerbe als Instrument der Integration von Kunden in das Innovationsmanagement von Software-Unternehmen. Präsentiert auf der Virtuelle Organisationen und Neue Medien 2007 /Workshop GeNeMe 2007: Gemeinschaften in Medien, Dresden, Deutschland.
- Bürgel, H.D.; Zeller, A. (1997):** Controlling kritischer Erfolgsfaktoren in der Forschung und Entwicklung. In: Controlling, Vol. 9 (1997) No. 4, S. 218-225.
- Dorbrandt, J.; Fröhlich, J.; Schmelzer, H.J.; Schopp, R. (1990):** Ausgewählte Projektbeispiele zur Reduzierung der Entwicklungszeit. In: Durchlaufzeiten in der Entwicklung: Praxis des industriellen F&E-Managements. Reichwald, R.; Schmelzer, H.J. (Hrsg.). Oldenbourg, München Wien 1990.
- Ebner, W. (2008):** Community Building for Innovations – Der Ideenwettbewerb als Methode für die Entwicklung und Einführung einer virtuellen Innovations-Gemeinschaft, Technische Universität München 2008.
- Herstatt, C.; Verworn, B. (2007):** Management der frühen Innovationsphasen: Grundlagen – Methoden – Neue Ansätze (2. Auflage), Springer Gabler, Wiesbaden, Deutschland 2007.
- Khurana, A.; Rosenthal, S.R. (1998):** Towards Holistic Front Ends in New Product Development. In: Journal of Product Innovation Management, Vol. 15 (1998) No. 1, S. 57-74.
- Leimeister, J.M. (2012):** Dienstleistungsengineering und -management, Springer, Heidelberg, Deutschland 2012.
- Leimeister, J.M. (2014):** Collaboration Engineering – IT-gestützte Zusammenarbeitsprozesse systematisch entwickeln und durchführen, Springer Gabler, Wiesbaden, Deutschland 2014.
- Leimeister, J.M.; Bretschneider, U. (2012):** IT-gestützter Ideenwettbewerb, Fachlexikon Technologie- und Innovationsmanagement. In: Fachlexikon Technologie- und Innovationsmanagement. Achatz, R.; Braun, M.; Sommerlatte, T. (Hrsg.). Symposium, Düsseldorf, Deutschland 2012.
- Martin, A.; Bartscher-Finzer, S. (2006):** Die Führung mittelständischer Unternehmen — Zwischen Defizit und Äquivalenz. In: Praxishandbuch des Mittelstands. Gabler 2006, S. 203-217.

- Mell, P.M.; Grance, T. (2011):** The NIST Definition of Cloud Computing. National Institute of Standards & Technology, 2011.
- Pichler, J.H.; Pleitner, H.J.; Schmidt, K.-H. (1997):** Management in KMU: Die Führung von Klein- und Mittelunternehmen (Vol. 2), Haupt, Bern, Schweiz 1997.
- Reichwald, R.; Piller, F.; Ihl, C.; Seifert, S. (2009):** Interaktive Wertschöpfung: Open Innovation, Individualisierung und neue Formen der Arbeitsteilung, Gabler, Wiesbaden, Deutschland 2009.
- Walcher, D. (2006):** Der Ideenwettbewerb als Methode der aktiven Kundenintegration – Theorie, empirische Analyse und Implikationen für den Innovationsprozess, Technische Universität München, München, Deutschland 2006.
- Wolf, J.; Paul, H.; Zipse, T. (2009):** Erfolg im Mittelstand: Tipps für die Praxis, Gabler, Wiesbaden, Deutschland 2009.

23 Markunterstützung durch rechtskonforme Gestaltung von Cloud-Services

S. Kroschwald, M. Wicker, A. Roßnagel

23.1 Einleitung

Das Projekt Value4Cloud zielt mit den erarbeiteten Ergebnissen insbesondere auf den Unterstützungsbedarf kleinerer und mittelgroßer Unternehmen in Deutschland ab, die eine Nutzung von Cloud-Services in Erwägung ziehen.

Aus der Darstellung der rechtlichen Voraussetzungen der Bereitstellung und Nutzung von Cloud-Angeboten¹ können Maßnahmen zur rechtsvertraglichen Gestaltung von Cloud-Computing abgeleitet werden. Hierzu sind die zuvor untersuchten Nutzerpflichten dahingehend zu überprüfen, ob der Cloud-Anbieter bei der Gestaltung seines Cloud-Angebotes diese Pflichten frühzeitig berücksichtigen könnte. Die Gestaltung des Cloud-Services obliegt regelmäßig dem Cloud-Anbieter. Häufig ist dieser jedoch gar nicht Adressat der gesetzlichen Anforderungen – insbesondere im Straf- und Datenschutzrecht ist der Cloud-Nutzer als Adressat verantwortlich für die Einhaltung der Vorgaben. Durch ein rechtsverträgliches Cloud-Angebot kann der gesetzlich verpflichtete Cloud-Nutzer in der Erfüllung seiner Pflichten unterstützt und von (rechtlichen) Risiken entlastet werden. Das Angebot einer rechtsvertraglichen Cloud kann dem Cloud-Anbieter in der Folge wiederum eine bessere Positionierung im Cloud-Markt ermöglichen.

Die Maßnahmen zur Bereitstellung einer rechtsverträglichen Cloud beziehen sich – entsprechend den hier untersuchten rechtlichen Vorgaben – auf

¹ S. zu Rechtsfragen des Cloud-Computing Kapitel 15 bis 18.

den Datenschutz,² die Vertragsgestaltung,³ die Vermeidung einer Strafbarkeit⁴ und strafprozessuale Ermittlungen⁵.

23.2 Datenschutz-Rechtsverträglichkeit

23.2.1 Verschlüsselung

Der Cloud-Nutzer muss nach Möglichkeit Daten ohne Personenbezug übermitteln, indem er die Daten vor der Übertragung sicher verschlüsselt. Der Nutzer trägt dabei das Risiko, dass die Verschlüsselung mittelfristig gebrochen und die Cloud-Nutzung rückwirkend unzulässig werden könnte. Aufgrund der Intransparenz der Datenwege und Speicherorte sowie der beim Cloud-Computing häufig erstellten Sicherungskopien könnten die Daten dann aber nicht mehr „rückholbar“ sein.

Sollen die Daten in der Cloud aber nicht nur gespeichert, sondern auch verarbeitet werden, müssen sie in der Cloud unverschlüsselt vorliegen – zumindest der Cloud-Anbieter kann dann vom Dateninhalt Kenntnis nehmen. Eine datenschutz-rechtsverträgliche Cloud müsste folglich gewährleisten, dass auch mittelfristig weder der Cloud-Anbieter noch ein sonstiger Dritter eine Möglichkeit haben, Dateninhalte zur Kenntnis zu nehmen, indem

- Daten unabhängig von der Verschlüsselung des Cloud-Nutzers durch den Cloud-Anbieter immer nur verschlüsselt gespeichert und übermittelt werden,
- Daten und Backup-Prozesse für den Nutzer verfolgbar und transparent sind – Daten müssen vollständig „rückholbar“ sein, indem auf Anfordern des Cloud-Nutzers nachweislich alle Sicherungskopien gelöscht oder ebenso neu verschlüsselt werden,
- die Server durch technische und organisatorische Maßnahmen vor dem Zugriff durch unbefugte Dritte geschützt werden,

² S. Abschnitt 23.1.

³ S. Abschnitt 23.2.

⁴ S. Abschnitt 23.3.

⁵ S. Abschnitt 23.4.

- Datenverarbeitungsprozesse an unverschlüsselten Daten nur „versiegelt“ stattfinden. Der Cloud-Anbieter muss dabei technisch und organisatorisch sicherstellen, dass nachweislich niemand, auch nicht die Mitarbeiter des Cloud-Anbieters, vom Inhalt der Daten Kenntnis nehmen können.⁶ Die Einhaltung sollte durch eine neutrale Stelle, möglichst in einem staatlichen Verfahren, kontrolliert und zertifiziert werden,
- der Cloud-Anbieter den Cloud-Nutzer ausdrücklich zur Übertragung von ausschließlich verschlüsselten Daten ermutigt und ihn gegebenenfalls auf Verschlüsselungsschwächen oder mögliche Angriffe hinweist.

23.2.2 *Auftragsdatenverarbeitung*

Der Cloud-Nutzer wird eine Datenübertragung regelmäßig nur im Rahmen einer Auftragsdatenverarbeitung vornehmen dürfen. Im Rahmen der Auftragsdatenverarbeitung obliegen dem Cloud-Nutzer als verantwortlichem Auftraggeber die Pflichten nach § 11 BDSG zur Auswahl, Weisung und Kontrolle des Cloud-Anbieters als Auftragnehmer.

Ein Cloud-Anbieter könnte seine Cloud Datenschutz-rechtsvertraglich gestalten und den Cloud-Nutzer bei der Einhaltung dieser Pflichten unterstützen, indem er

- dem Cloud-Nutzer umfangreiche Informationen als Grundlage für eine sorgfältige Auswahl sowie zu den regelmäßigen Kontrollen liefert. Informationen sollten insbesondere hinsichtlich des Datensicherheitskonzepts und technischer und organisatorischer Maßnahmen, des logischen Aufbaus der Cloud, möglicher Datenwege, Ansprechpartner, Empfänger und Serverstandorte sowie möglicher rechtlicher oder wirtschaftlicher Abhängigkeitsverhältnisse zu anderen Unternehmen vorhanden sein. Die Informationen sollten ständig aktualisiert über eine Online-Plattform abrufbar sein.
- den Cloud-Nutzer über mögliche Zertifizierungen in Kenntnis setzt und Unterlagen zur Prüfung bereitstellt.

⁶ S. hierzu das Konzept des Trusted-Cloud-Projekts „Sealed Cloud“.

- dem Cloud-Nutzer gegebenenfalls sogar eine Vor-Ort-Kontrolle ermöglicht.
- dem Cloud-Nutzer die Möglichkeit einräumt, auf Basis eines Vertragsmusters möglichst durch automatisierte Optionsmöglichkeiten einen Auftragsdatenverarbeitungsvertrag zu erstellen, der den Vorgaben des § 11 BDSG entspricht und die Interessen des Cloud-Nutzers abbildet und so den Cloud-Nutzer als Auftraggeber in seiner Weisungspflicht unterstützt.
- Datenverarbeitungsprozesse und Datenwege ununterbrochen protokolliert und für den Cloud-Nutzer leicht zugänglich dokumentiert.

23.2.3 *Auslandsbezug*

Das Cloud-Computing mit Auslandsbezug ist für den Cloud-Nutzer mit noch größeren rechtlichen Hürden verbunden. Für ein rechtsverträgliches Cloud-Angebot sollte der Cloud-Anbieter deshalb

- seinen Sitz und sämtliche Server, kurz die gesamte Cloud-Datenverarbeitung, innerhalb Deutschlands oder innerhalb der Schengen-Staaten, maximal innerhalb der Grenzen der EU und des EWR oder eines von der Kommission anerkannten „sicheren Drittlands“ errichten.
- Unterauftragnehmer ebenso nur in diesen Staaten beauftragen.
- im Rahmen seiner Möglichkeiten auch die Datenwege innerhalb der EU und des EWR sicherstellen.
- den staatlichen Zugriff fremder Staaten auf die Daten durch technische Maßnahmen sowie die Wahl seines Sitzes und der Serverstandorte verhindern.
- keine rechtliche oder wirtschaftliche Abhängigkeit zu Unternehmen in unsicheren Drittstaaten aufweisen.
- für den Fall, dass ein Datenexport in einen „unsicheren Drittstaat“ dennoch erforderlich sein sollte, dem Cloud-Nutzer EU-Standardvertragsklauseln anbieten und durch Datenschutzmaßnahmen auf eine zulässige Datenübermittlung an ihn hinwirken.

23.2.4 *Betroffenenrechte*

Ist der Cloud-Anbieter selbst verantwortliche Stelle, etwa wenn er Daten eigenständig erhebt, verarbeitet oder nutzt (beispielsweise auf seinen Servern gespeicherte Daten zu Werbezwecken auswertet oder im Rahmen eines Cloud-Dienstes weitere Daten des Cloud-Nutzers, bemerkt oder unbemerkt, verarbeitet), sind Betroffenenrechte gleichsam Pflichten des Cloud-Anbieters gegenüber den Betroffenen. Die Einhaltung der Betroffenenrechte ist in diesem Fall eine Frage der Rechtmäßigkeit und nicht der Rechtsverträglichkeit.⁷

Der verantwortliche Cloud-Anbieter kann im Hinblick auf die Rechtsverträglichkeit dennoch die Ausübung der Betroffenenrechte durch den Betroffenen erleichtern. So kann er beispielsweise durch automatisierte Online-Portale, auf denen die oben genannten Informationen über den Status der Datenverarbeitung abrufbar sind, gegenüber dem Cloud-Nutzer Transparenz herstellen. Auch die Ausübung der Gestaltungsrechte wie Berichtigung, Löschung oder Sperrung sollte hierüber möglich sein. Hierbei sollte der Cloud-Anbieter, wie schon im Rahmen der Verschlüsselung, die Möglichkeit bieten, Daten, ihre Wege und mögliche Backups vollständig nachvollziehen zu können, um eine Berichtigung oder Löschung vollständig und sicher durchführen zu können.

Ist der Cloud-Anbieter dagegen nur Auftragnehmer und insofern keine verantwortliche Stelle, könnte eine rechtsverträgliche Cloud so ausgestaltet werden, dass sie trotz der eigentlichen Verantwortung des Cloud-Nutzers die Betroffenenrechte wie Benachrichtigung, Auskunft, Berichtigung, Löschung oder Sperrung im Auftrag des Cloud-Nutzers gegenüber den Betroffenen direkt erfüllt.

23.3 Vertragsrechtsverträglichkeit

Ein Cloud-Computing-Vertrag bedarf einer angemessenen Risikoverteilung zwischen den Vertragsparteien. Standard-Angebote, die der Cloud-Anbieter zum Abruf bereithält, sind meist an Allgemeine Geschäftsbedingungen

⁷ S. zu den (rechtlichen) Begriffsbestimmungen beim Cloud-Computing Kapitel 2.

(AGB) des Cloud-Anbieters gebunden. Das Recht der AGB ist nicht nur gegenüber Verbrauchern, sondern auch im unternehmerischen Geschäftsverkehr an strenge gesetzliche und gerichtliche Grenzen gebunden. Damit ist der Cloud-Anbieter grundsätzlich gehalten, bei seinen Vertragsbedingungen eine angemessene Risikoverteilung zu beachten.

Dennoch führt dies im Cloud-Kontext zu Schwierigkeiten hinsichtlich der Haftung bei Datenverlust oder bei (vorübergehender) Nicht-Verfügbarkeit der Cloud-Angebote, da die mietrechtliche Ausgestaltung von Cloud-Computing grundsätzlich eine hundertprozentige Verfügbarkeit voraussetzt. Durch Service Level Agreements (SLA) kann vertragsrechtlich das hohe Risiko der Cloud-Anbieter angemessen abgebildet werden. Die dadurch möglichen Haftungsreduzierungen kann der Cloud-Anbieter insbesondere bei seiner (günstigeren) Preisgestaltung an den Cloud-Nutzer weitergeben.

Bei einem Cloud-Vertrag sind insbesondere folgende Vereinbarungen zu treffen:

- Gerichtsstand und eventuelle Schiedswahlklauseln,
- Änderungsvorbehalte,
- Einsatz von Subunternehmern,
- Softwarelizenzen und Verwendung von Open-Source-Software,
- Vertragspflichten (nach dem gesetzlichen Leitbild des Mietrechts),
- Verfügbarkeitswerte im Rahmen von SLA,
- Gewährleistung für Mängel und Haftung für Schäden,
- Beendigung und Rückabwicklung,
- IT-Compliance-Anforderungen.

Darüber hinaus sollte der Cloud-Anbieter auch den Vertrag über die Auftragsdatenverarbeitung, der eigentlich im Verantwortungsbereich des Cloud-Nutzers liegt, bereitstellen und bereits die für Cloud-Computing erforderlichen technischen und organisatorischen Maßnahmen berücksichtigen.

Kann der Cloud-Anbieter rechtliche Anforderungen erfüllen und die Risikoverteilung innerhalb der AGB gerecht abbilden, wird der Cloud-Nutzer dem Cloud-Computing ein höheres Vertrauen entgegenbringen.

23.4 Strafrechtsverträglichkeit

Beim Cloud-Computing folgt das Strafbarkeitsrisiko insbesondere aus der Nutzung von Cloud-Angeboten, da durch die Cloud-Nutzung das Risiko der Kenntnisnahme von Daten durch Dritte entsteht. Weitere Fälle einer möglichen Strafbarkeit im Cloud-Kontext sind die unbefugte Kenntnisnahme von Inhalten sowie die Zugangsvereitelung zu den Cloud-Daten gegenüber dem Cloud-Nutzer.

Der Cloud-Anbieter kann Strafbarkeitsrisiken für sich selbst wie auch den Cloud-Nutzer minimieren, indem er seinen Zugriff auf Dateninhalte ausschließt.⁸ Bei technisch bedingten Zugriffen auf Cloud-Server sollte die Möglichkeit der Kenntnisnahme von Dateninhalten der Cloud-Nutzer durch Mitarbeiter des Cloud-Anbieters vollständig ausgeschlossen werden.

Das mögliche Risiko einer Strafbarkeit des Cloud-Anbieters für Zugangshindernisse zur Cloud kann im Wege vertraglicher Vereinbarungen für den Fall eines Zahlungsverzugs des Cloud-Nutzers oder für die Rückabwicklung nach Beendigung des Vertrages abgebildet werden.

Zwar obliegt die Klärung der Frage, ob die Cloud-Nutzung zulässig ist, grundsätzlich dem Cloud-Nutzer. Aufgrund des Wissensdefizits über Cloud-Angebote und eigene Pflichten und Verbote fällt die Entscheidung des potenziellen Cloud-Nutzers häufig jedoch zu Lasten des Cloud-Computing aus. Der Cloud-Anbieter kann dieses Defizit bei seinem Angebot aufgreifen und den Cloud-Nutzer über bestehende Risiken und mögliche Vermeidungskonzepte wie etwa Verschlüsselung der Daten informieren.

Damit Cloud-Computing nicht zu Strafbarkeitsrisiken führt, ist zu prüfen, ob

- besondere Pflichten die Cloud-Nutzung hemmen,
- Verschlüsselung der Daten Abhilfe bringt,

⁸ S. hierzu das Konzept des Trusted-Cloud-Projekts „Sealed Cloud“.

- vertragliche Vereinbarungen für technisch bedingte Zugriffe vorliegen und
- Kenntnisnahme der Cloud-Anbieter ausgeschlossen ist.

Der Cloud-Anbieter kann durch Hinweise auf das strafrechtliche Risiko und seine getroffenen Maßnahmen zur Vermeidung für Vertrauen beim Cloud-Nutzer sorgen.

23.5 Strafprozessrechtsverträglichkeit

Cloud-Computing ist nur eine andere Möglichkeit zur Bereitstellung und zum Bezug von IT-Ressourcen. Die grundlegenden Möglichkeiten zu strafprozessualen Ermittlungen bei Verdacht von Straftaten bestehen daher auch beim Cloud-Computing. Die Daten in der Cloud sind aus strafprozessualer Sicht weder unsicherer noch sicherer.

Grundsätzlich sind folgende Ermittlungen im Cloud-Kontext möglich:

- Auskunft beim Cloud-Anbieter über Benutzername und Passwort (meist nur als Hashwert vorhanden und daher unbrauchbar),
- Durchsuchung beim Cloud-Nutzer vor Ort einschließlich seines Cloud-Speichers,
- Kopie der Daten beim Cloud-Anbieter und anschließende Durchsuchung innerhalb der Cloud-Daten.
- Rechtlich *nicht* möglich ist ein Zugriff auf die Datenübertragung in und aus der Cloud.

Dass die Daten nicht in eigener Verfügungsgewalt sind, erweckt den Eindruck eines einfacheren staatlichen Zugriffs. Der Cloud-Anbieter sollte daher den Cloud-Nutzer über seine bestehenden Kooperationspflichten unter Verweis auf die lokalen Ermittlungswege beim Cloud-Nutzer vor Ort informieren. Zusätzlich sollte der Cloud-Anbieter sich klar positionieren, dass eine Zusammenarbeit mit den Ermittlungsbehörden über die gesetzlichen Pflichten hinaus nicht stattfinden wird. Zusätzliches Vertrauen kann er auch da-

durch erzeugen, dass er im Rahmen der gesetzlichen Erlaubnisse den Cloud-Nutzer über stattfindende Ermittlungen informiert.

Um die Daten seiner Cloud-Nutzer bestmöglich vor zufälligen Zugriffen zu schützen, sollte der Cloud-Anbieter strafprozessuale Ermittlungen gegen sich selbst vermeiden, damit die Daten der Cloud-Nutzer nicht im Ermittlungskontext einbezogen werden können. Weist der Cloud-Anbieter den Cloud-Nutzer auf die nutzerseitige Verschlüsselung von Daten hin, fördert er den besten Schutz vor strafprozessualen Ermittlungen in der Cloud.

Den besten Schutz gegen strafprozessuale Ermittlungen bieten

- Verschlüsselung durch den Cloud-Nutzer,
- Geheimhaltung von Benutzernamen und Passwort und
- keine überobligatorische Zusammenarbeit des Cloud-Anbieters mit den Ermittlungsbehörden.

Ermittlungen müssen zur Wahrung der effektiven Strafverfolgung auch beim Cloud-Computing erfolgreich möglich sein, allerdings muss sich das Risiko einer Straftataufdeckung durch Cloud-Nutzung nicht vergrößern.

24 Fallstudie: Werkzeug-unterstützte Analyse und Bewertung von Cloud-Services aus Anwendersicht

J. Wollersheim, A. Keller, F. Glatz

24.1 Einleitung

Im Rahmen des Projektes wurde ein Workshop-Konzept erarbeitet, um die Projektergebnisse rund um Fragen der IT- und insbesondere der Cloud-Beschaffung rasch und themenzentriert in die Praxis kleiner und mittelständischer Unternehmen (KMU) zu transferieren. Das Konzept wurde so ausgelegt, dass sich im Workshop Vortragelemente zur Wissensvermittlung und die Bearbeitung verschiedener Aufgabenstellungen in Kleingruppen im Laufe eines Tages abwechseln. So ermöglichen die Workshops zum Themenbereich IT- und Cloud-Beschaffung nicht nur die Vermittlung neuester Erkenntnisse aus der Forschung in einer für die Teilnehmer ansprechenden Atmosphäre, sondern auch ein Höchstmaß an Austausch untereinander.

Das Workshop-Konzept zur Vermittlung der im Projekt erarbeiteten Ergebnisse rund um das Thema Beschaffung ist auf die Dauer eines Arbeitstages ausgelegt. Im Anschluss an eine einleitende Vorstellungsrunde werden zunächst beispielhafte Herausforderungen aus der Unternehmenspraxis vorgestellt, die im Verlauf zu einem Beschaffungsszenario führen und im Workshop bearbeitet und gelöst werden sollen. Auf Basis der persönlichen Interessen der Teilnehmer werden aus den vorgestellten Beschaffungsszenarien die im Workshop zu bearbeitenden Szenarien ausgewählt und Teams zur Bearbeitung gebildet. Haben sich die Teams konstituiert und erste Fragen gesammelt, werden die Details der Geschäftsszenarien und enthaltene Herausforderungen, sowie die im Projekt entwickelten Unterstützungswerkzeuge sukzessive vorgestellt. Diese Werkzeuge können im Workshop von den Teilnehmern im Rahmen ihrer individuellen Lösungsfindung eingesetzt werden, auch unterstützt durch Handouts, gedruckte Templates sowie einen Software-

Abbildung 1: Didaktisches Workshop-Framework (Eigene Darstellung).

Zugang. Der Workshop ist in Anlehnung an die Erkenntnisse von Pivec (2014) und Garris et al. (2002) strukturiert. [Abbildung 1](#) visualisiert die wesentlichen Bausteine und den Ablauf.

Die nachfolgenden Abschnitte erläutern zunächst die drei vorgestellten Geschäftsszenarien etwas detaillierter. Es folgt die Analyse und Gliederung enthaltener Problemstellungen entlang eines typischen IT-Beschaffungsprozesses sowie, zu den einzelnen Phasen des Beschaffungsvorgangs, die Vorstellung von im Projekt entwickelten Werkzeugen, die bei der Bearbeitung unterstützen können.

24.2 Das Geschäftsszenario der Fallstudie

Zu Beginn des Workshops wird ein fiktives Geschäftsszenario vorgestellt, das Fragestellungen der IT-Unterstützung eines mittelständischen Unternehmens und seiner Abteilungen thematisiert. Der IT-Bedarf eines fiktiven Unternehmens „Alpha“ dient im Workshop als Ausgangspunkt. Die detaillierte Analyse des Bedarfs und damit verbundener Herausforderungen lenken dann auf Cloud-Services als eine mögliche Lösung zur Bedarfsdeckung, sowie Tools und Templates zur Unterstützung im Beschaffungsprozess. Die

Vermittlung und Sensibilisierung für Herausforderungen bei der Beschaffung von IT-Services und insbesondere Cloud-Services sind Ziele des Workshops.

Szenario 1: Kollaborativer Teamspeicher

Die Zusammenarbeit in Teams, insbesondere das gemeinsame Erarbeiten von Dokumenten und der Austausch größerer Datenmengen wird im Unternehmen Alpha als umständlich und zeitraubend empfunden. Der Dokumentenversand erfolgt aktuell via Email, da der Zugriff auf gemeinsame Laufwerke im Unternehmen schwierig ist. Um den Dokumentenaustausch im Team zu vereinfachen und eine effizientere Arbeit zu ermöglichen, wurde die IT-Abteilung von der Geschäftsführung mit der Suche nach einer Lösung beauftragt, die eine teamorientierte Speicherung von Dateien ermöglicht. Federführend wurde Alpha's IT-Abteilung mit der Beschaffung und Integration einer solchen Lösung von der Geschäftsführung beauftragt, da die Lösung alle Fachabteilungen des Unternehmens adressieren soll und somit der von der IT-Abteilung betreuten IT-Infrastruktur von Alpha zugerechnet wird. Die Lösung soll mindestens folgende Funktionalitäten abdecken:

- Datenablage online, um Dokumente zu speichern und auszutauschen,
- Zugriffsrechte für Mitarbeiter und Externe sollen möglich sein,
- Team-Verzeichnisse sollen ad-hoc gebildet werden können,
- automatische Synchronisation mit Rechner/Device jedes Team-Mitglieds.

Ein erstes Marktscreening identifizierte die in [Abbildung 2](#) genannten Angebote als möglicherweise passende Cloud-Lösungen und somit als Ausgangspunkt der Analyse und etwaiger Problemlösungsschritte.

Aufgabe der IT-Abteilung ist es nun, den Beschaffungsprozess zu strukturieren, zu berücksichtigende Rahmenbedingungen zu identifizieren, benötigte Akteure einzubinden, eine Schutzbedarfsanalyse der betroffenen Daten durchzuführen, einen detaillierten Katalog funktionaler und nicht-funktionaler Anforderungen aufzustellen und eine Zuordnung von Anforderungen zu bewertenden Akteuren vorzunehmen, eine Gewichtung der Kriterien

Abbildung 2: Szenario kollaborativer Teamspeicher – Serviceangebote-Auswahl 2013 (Eigene Darstellung).

durchzuführen (Muss/Kann-Kriterien) sowie bereits Vorkehrungen für eine kontinuierliche Qualitätsüberwachung während der Service-Nutzung zu treffen. Die so entstehende Entscheidungsvorlage soll dann der Geschäftsführung als Basis für eine Auswahlentscheidung dienen.

Szenario 2: Customer Relationship Management (CRM)-Anwendung

Im Hause Alpha beschwerten sich die Abteilung Marketing und die Abteilung Kundenservice seit geraumer Zeit über Abstimmungsprobleme bezüglich der Aktualität und Pflege der Kundendaten, etwa welche Produkte von welchem Kunden aktuell genutzt werden. Die Marketingabteilung stellt bei Kundengesprächen fest, dass die Daten in ihrem System nicht korrekt sind und durchgeführte Wartungen und behobene Probleme nicht im Marketing-Com-

putersystem auftauchen. Folglich werden Kunden mit unpassenden Produkten und Produkterweiterungen adressiert. Gleichzeitig besteht im Kundensupport das Problem, dass Kunden im Zeitverlauf von unterschiedlichen Support-Mitarbeitern bedient werden, diese jedoch nicht auf die Support-Historie zurückgreifen können. Somit sind bei identischen Problemen eines Kunden immer neue Lösungswege zu entwickeln. Es ist nahezu unmöglich für Kundendienstmitarbeiter, auf Lösungen der Kollegen zurückzugreifen. Um diese Herausforderungen zu adressieren, wünschen sich beide Abteilungen ein gemeinsam genutztes CRM-System. Dieses soll folgende Funktionalität abdecken:

- gemeinsame Stammdatenverwaltung, inkl. Kundenhistorie, Produkthistorie und bestehender Kontaktpunkte des Kunden in das Unternehmen Alpha,
- teilautomatisierte Vertriebsprozesse (Kampagnen für vorselektierte Kundengruppen, Unterstützung bei der Angebotserstellung),
- Datenbank mit „Musterlösungen“ für häufige Kundenprobleme,
- Suchmöglichkeit für Kundendienstmitarbeiter in Kundenproblemen und Lösungen, die von Kollegen erarbeitet wurden.

Ein erstes Marktscreening identifizierte die in [Abbildung 3](#) genannten Angebote als möglicherweise passende Cloud-Lösungen und somit als Ausgangspunkt der weiteren Analyse und Problemlösung.

Aufgabe der Fachabteilungsmitarbeiter ist es nun, zunächst den Beschaffungsprozess zu strukturieren, zu berücksichtigende Rahmenbedingungen zu identifizieren, benötigte Akteure einzubinden und das OK der Geschäftsführung einzuholen. Darauf folgen eine Schutzbedarfsanalyse der betroffenen Daten, die Erstellung eines detaillierten Katalogs funktionaler und nicht-funktionaler Anforderungen und eine Zuordnung von Anforderungen zu bewertenden Akteuren, eine Gewichtung der Kriterien (Muss/Kann-Kriterien) sowie bereits Vorkehrungen für eine kontinuierliche Qualitätsüberwachung während der Service-Nutzung. Die so entstehende Entscheidungsvorlage soll dann der Geschäftsführung als Basis für eine Auswahlentscheidung dienen.

Abbildung 3: Szenario CRM-Anwendung – Serviceangebote-Auswahl 2013 (Eigene Darstellung).

Szenario 3: Enterprise Resource Planning (ERP)-Anwendung

Der Kundendienst des Unternehmens Alpha soll in Kürze nicht nur kostenpflichtig werden, sondern auch in Form eines eigenständigen Geschäftsbereichs geführt werden. Entsprechend ergeben sich neue Herausforderungen in den Abteilungen Finanzbuchhaltung, Rechnungswesen und Controlling. Neue Kontenstrukturen sind zu etablieren und eigene Buchungskreise aufzubauen. Um dennoch das im Unternehmen Alpha etablierte ERP-System nicht zu sehr anpassen zu müssen, favorisiert die Geschäftsleitung von Alpha den Aufbau eines hiervon nahezu unabhängigen ERP-Systems. Lediglich die Stammdaten sollen abgeglichen werden und abschließende Reports der Ergebnisse des neuen Geschäftsbereichs sollen per Schnittstelle in das Kernsystem des Unternehmens eingelesen werden. Das ERP-System für den Bereich soll neu aufgebaut werden, um den Bedarf der neuen Abteilung passgenau abzudecken und einer agilen Erweiterung des Geschäftsbereichs Rechnung

tragen zu können. Auch sollen Mitarbeiter für das Controlling des Geschäftsbereichs durch moderne IT-Unterstützung motiviert und an das Unternehmen Alpha gebunden werden. Die funktionalen Anforderungen umfassen somit:

- Stammdatenverwaltung (Kunden, Lieferanten, Artikel),
- Warenwirtschaft (Anlegen, Status und Abwicklung von Support-Aufträgen),
- Finanzen & Controlling (Preislisten, Provisionierung, Mahnwesen, Unternehmensplanung, Berichtswesen),
- Abgleich mit Stammdaten in Alphas existierendem ERP-System und Export von Berichten in einem Format, das in das bereits vorhandene ERP-System von Alpha eingelesen werden kann.

Ein erstes Marktscreening identifizierte die in [Abbildung 4](#) genannten Angebote als möglicherweise passende Cloud-Lösungen und somit als Ausgangspunkt einer tiefergehenden Analyse und Gliederung etwaiger Problemlösungsschritte.

Abbildung 4: Szenario ERP-Anwendung – Serviceangebote-Auswahl 2013 (Eigene Darstellung).

Aufgabe der betroffenen Mitarbeiter der Fachabteilungen ist es nun zunächst, den Beschaffungsprozess für das neue ERP-System zu strukturieren, zu berücksichtigende Rahmenbedingungen zu identifizieren, benötigte Akteure aus der IT und weiterer Abteilungen einzubinden und das OK der Geschäftsführung einzuholen, eine Schutzbedarfsanalyse der betroffenen Daten durchzuführen, einen detaillierten Katalog funktionaler und nicht-funktionaler Anforderungen aufzustellen und eine Zuordnung von Anforderungen zu bewertenden Akteuren vorzunehmen, eine Gewichtung der Kriterien durchzuführen (Muss/Kann-Kriterien) sowie bereits Vorkehrungen für eine kontinuierliche Qualitätsüberwachung während der Service-Nutzung zu treffen. Die so entstehende Entscheidungsvorlage soll dann der Geschäftsführung als Basis für eine Auswahlentscheidung dienen.

24.3 Szenario-Analyse und Strukturierung enthaltener Problemstellungen

Aus den vorgestellten drei Szenarien wählen sich die Workshop-Teilnehmer ein individuell für sie Interessantes aus und bearbeiten dies in der Gruppe von Teilnehmern mit gleichem Interesse. Nach ihrer Auswahl und der Konstitution der Gruppen widmen sich die Workshop-Teilnehmer nun der detaillierteren Analyse des skizzierten Szenarios.

Die Beschaffung von IT kann prinzipiell eine Vielzahl von Produkten und Dienstleistungen umfassen, von Hardware wie Drucker, Arbeitsplatzrechner oder Netzwerkkomponenten bis zur Beschaffung von Programmierleistungen, die nach Spezifikation von einem Dienstleister im Werkvertrag gefertigt werden. Die Bandbreite reicht also von hochgradig standardisierten Produkten ohne Dienstleistungskomponente bis zur individualisierten Auftragsfertigung. Cloud-Services verbinden einen hohen Dienstleistungsgrad mit einem hohen Standardisierungsgrad, [Abbildung 5](#) zeigt beispielhaft die Bandbreite und Einordnung auf.

Besonderheiten von Dienstleistungen wie etwa eine vergleichsweise schwierigere Spezifikation des Leistungsumfangs sind bei der Beschaffung von Cloud-Services ebenso zu beachten, wie Besonderheiten von Gütern mit

Abbildung 5: Standardisierte IT-Dienstleistungen – eine Abgrenzung (Eigene Darstellung).

hohem Standardisierungsgrad. Diese können sich etwa durch vom Hersteller vorgegebene Produkteigenschaften ergeben, die sich nicht individuell an den eigenen Bedarf anpassen lassen. Entsprechende Besonderheiten sind bei der Beschaffung von Cloud-Services, oder auch schon dann, wenn Cloud-Services als eine mögliche Lösung in Betracht gezogen werden, zu berücksichtigen.

Die Beschaffung von Informationstechnik oder IT-Services für ein Unternehmen erfordert in den meisten Fällen Wissen aus unterschiedlichen Domänen und somit eine Einbindung unterschiedlichster Fachabteilungen. Es ist bei einer Vielzahl von Beschaffungsvorgängen notwendig, nicht nur die IT-Abteilung, sondern auch betroffene Fachabteilungen, den zentralen Einkauf oder den Finanzbereich eines Unternehmens und seine jeweilige Expertise in den Beschaffungsprozess zu integrieren. Funktionsbereich-übergreifende Beschaffung ist also nichts vollständig Neues. Unternehmen können zur Strukturierung der anfallenden Aktivitäten bspw. auf das Rahmenwerk der Arbeitsgruppe IT-Beschaffung der Society for Information Management (SIM)

Abbildung 6: Der IT-Beschaffungsprozess (In Anlehnung an Heckman 2003)

zurückgreifen (Heckman 2003). Nach Heckman (2003) beginnt die Beschaffung von IT generell mit der **Anforderungsspezifikation**, also der Bedarfsermittlung und sukzessiven Spezifikation der vom Beschaffungsobjekt zu erfüllenden Anforderungen. Die Bedarfsermittlung umfasst dabei den Prozess der geschäftlichen Rechtfertigung des Bedarfs, die Organisation des Beschaffungsteams, die Spezifikation der Anforderungen, das Eruiere alternativer Lösungsvorschläge und das Einholen von Freigaben, um mit dem Beschaffungsprozess fortzufahren.

Es folgen Aktivitäten zur **Akquisition** und zur kontinuierlichen Überwachung und Steuerung der **Vertragserfüllung**. Die Akquisition umfasst dabei die detaillierte Analyse des Angebots, die Bewertung der Alternativen sowie den Abschluss einer Beschaffungsvereinbarung und somit die Auswahl eines geeigneten Lieferanten zur Deckung des Bedarfs. Die abschließende Phase der Vertragserfüllung erfordert Aktivitäten wie etwa die kontinuierliche Qualitätsüberwachung der empfangenen Leistungen. Ergänzend wird der Beschaffungsprozess von nebenläufigen Managementprozessen flankiert, wie [Abbildung 6](#) zeigt.

Der skizzierte Prozess eignet sich als Analyserahmen. Für die enthaltenen Elemente des Beschaffungsprozesses ergeben sich folgende Fragestellungen, die als Leitlinie für durchzuführende Aktivitäten gelten können:

Anforderungsspezifikation

- Welche Faktoren innerhalb des beschaffenden Unternehmens und unternehmensextern sind bei der Beschaffung zu berücksichtigen?
- Welche Akteure sind in den Beschaffungsprozess einzubinden?

Akquisition

- Welcher Schutzklasse unterliegen die vom Service genutzten Unternehmensdaten und welche Anforderungen sind somit an die Sicherheit des zu beschaffenden Services zu stellen?
- Welche Aspekte des Bedarfs sind essentiell wichtig und für wen? Hier gilt es auch die Service-Integration und den Support zu bedenken.
- Wie sind die Qualitätskriterien zu gewichten? Was sind Muss-, was sind Kann-Kriterien?

Vertragserfüllung

- Wie ist die Leistung kontinuierlich zu überwachen? Was sind die richtigen „Qualitätsmesspunkte“?

Der skizzierte IT-Beschaffungsprozess und die aufgeführten Fragen innerhalb der einzelnen Bereiche dienen den Teilnehmern als Analyserahmen für die weitere Bearbeitung der zuvor vorgestellten Szenarien. In den Gruppen versuchen die Workshop-Teilnehmer nun, die durch das Szenario vorgegebene Aufgabe unter Berücksichtigung enthaltener Rahmenbedingungen und entlang des skizzierten Beschaffungsprozesses umzusetzen. Um Fragestellungen zu adressieren, die vor dem Hintergrund von Cloud-Services besondere Beachtung verdienen, wurden im Projekt unterschiedliche Werkzeuge entwickelt. Diese Werkzeuge unterstützen das Beschaffungsteam auf vielfältige Art und Weise, wie nachfolgend vorgestellt.

24.4 Einsatz unterstützender Werkzeuge zur Problemlösung

Im Projekt entwickelte Werkzeuge zur Thematisierung der im Beschaffungsprozess zu berücksichtigenden Besonderheiten von Cloud-Services werden nachfolgend vorgestellt. Die Werkzeuge sind dabei in Form von Templates und Checklisten verfügbar und werden im Workshop in Papierform verwendet. Ein Teil wurde ergänzend in eine Software überführt, die im Workshop von den Gruppen unterstützend eingesetzt werden kann. Alle Werkzeuge werden nachfolgend in der Reihenfolge der durch sie unterstützten Aktivitäten des Beschaffungsprozesses vorgestellt; angefangen bei der Analyse von Einflussfaktoren, gefolgt von der Festlegung von Verantwortlichkeiten, der Festlegung der zu berücksichtigenden Schutzklasse bis zur detaillierten Ausarbeitung der Anforderungen in Form eines Kriterienkatalogs.

24.4.1 *Werkzeug A: Analyserahmen für den Beschaffungsprozess beeinflussende Faktoren*

Zu Beginn eines jeden Beschaffungsvorgangs ist zu untersuchen, welche Faktoren bei der Gestaltung des Beschaffungsprozesses besonders zu berücksichtigen sind. [Abbildung 7](#) ordnet den im Projekt entwickelten Analyserahmen für solche beeinflussende Faktoren in das Framework von Heckman (2003) ein.

Der in Kapitel 10 dieses Buchs vorgestellte Analyserahmen umfasst sechs wesentliche Aspekte, die die Ausgestaltung des Beschaffungsprozesses beeinflussen und somit zu Beginn eines jeden Beschaffungsvorgangs bei der Prozessgestaltung berücksichtigt werden sollten. Der Analyserahmen steht den Workshop-Teilnehmern auf Papier wie auch in elektronischer Form zur Verfügung.

Um Abhängigkeiten zwischen Faktorausprägungen zu visualisieren, wurde eine Softwareanwendung entwickelt, die eine individuelle Zusammenstellung von Anforderungen im Workshop auch spielerisch ermöglicht. Wird die

Abbildung 7: Der IT-Beschaffungsprozess / Anforderungsspezifikation (In Anlehnung an Heckman 2003).

Ausprägung eines Einflussfaktors in der Software ausgewählt, erfolgt eine Vorauswahl von Kriterien. Wie bereits in Kapitel 10 dieses Buches erläutert, führen einzelne Faktorausprägungen dazu, dass bestimmte Kriterien an Wichtigkeit im Beschaffungsprozess gewinnen oder verlieren. Dieser Zusammenhang kann so mittels der Softwareanwendung erfahren werden. Bestehende Abhängigkeiten, die für den ersten Einflussfaktor „Service-Typ“ in [Tabelle 1](#) beispielhaft aufgeführt werden, sind etwa in der softwaretechnischen Umsetzung berücksichtigt.

Die Workshop-Teilnehmer werden durch die Anwendung dieses Analyserahmens für Faktoren die den Beschaffungsprozess beeinflussen, sensibilisiert und angehalten, individuelle Schlüsse für ihr Unternehmen daraus zu ziehen. Es werden somit erste Anforderungskriterien zur Auswahl eines IT-Services festgelegt und es wird klarer, welche Akteure aus dem Unternehmen Alpha oder darüber hinaus in den Beschaffungsprozess aufgrund noch offener Anforderungen einzubinden sind.

Tabelle 1: Qualitätseigenschaften nach Cloud-Service-Typen – Suchprofile

Service-Typ	Qualitätseigenschaft
IaaS, PaaS-Beschaffungen	<ul style="list-style-type: none"> ■ Haftung und Verantwortung im Fall von SLA-Verletzungen ■ Ort der Servicebereitstellung (e.g. der Ort der Datenverarbeitung) ■ Ort (Gerichtsstand) ■ Zertifikate ■ Auditierbarkeit des Anbieters durch den Kunden ■ Ergänzende Beratungsdienstleistungen
SaaS-Beschaffungen	<ul style="list-style-type: none"> ■ Initiale Bereitstellungszeit ■ Zugesicherte Kommunikationskanäle für Kundenanfragen ■ Internationalität in Supportangelegenheiten ■ Anzahl von Unternehmenskunden, die den Service bereits nutzen ■ Feedback von Nutzern bzgl. Service ■ Nutzung und Unterstützung offener Standards ■ Training ■ Ort (Rechenzentrum, Büros des Anbieters)

24.4.2 *Werkzeug B: Template zur Festlegung von Verantwortlichkeiten im Beschaffungsprozess*

Um die am Beschaffungsprozess zu beteiligenden Akteure verantwortlich in den Prozess einzubinden und Zuständigkeiten festzuhalten, empfiehlt es sich, im Team eine klare Vereinbarung von Zuständigkeiten zu treffen. Um das Ergebnis zu fixieren und typischerweise einzubindende Abteilungen oder einzelne Prozessschritte nicht zu übersehen, wurde im Projekt ein Template entwickelt. Das Template lässt sich im Beschaffungsframework von Heckman (2003) ebenfalls der Phase der Anforderungsspezifikation zuordnen.

Abbildung 8 visualisiert das den Workshop-Teilnehmern in Papierform zur Verfügung gestellte Template (s. auch Kapitel 19). Es umfasst eine feingranulare Darstellung des Beschaffungsprozesses sowie bereits vorformulierte Abteilungen oder Anspruchsgruppen, die typischerweise zu berücksichti-

	Grobe Spezifikation (funkt. & techn.)	Schutzklasse identifizieren	Bedarfsspezifikation			Abgleich von Bedarf und Angebot	Priorisierung der Angebote	Verhandlung und Vertrag
			Funktional	Technisch	Rechtlich			
Fachabteilung	R		R	C	C	R		C
IT-Abteilung		R		R		I		
Legal					R	I		
Geschäftsführung		I	I	I	I	I	R	R
...								

Legende: A = Accountable C = Consulted I = Informed R = Responsible

Abbildung 8: Template zur Zuordnung von Verantwortlichkeiten (In Anlehnung an Heckman 2003; Van der Valk/Rozemeijer 2009).

gen sind. Im Workshop sind von den Teilnehmern zunächst weitere Anspruchsgruppen hinzuzufügen und die Verantwortlichkeiten festzulegen. Hierfür wird das in Kapitel 19 vorgestellte RACI-Schema vorgeschlagen.

24.4.3 Werkzeug C: Schema zur Identifikation und Klassifizierung des Schutzbedarfs

Wurden die ersten Aktivitäten im Beschaffungsprozess von den Workshop-Teilnehmern erfolgreich durchlaufen, die Einflussfaktoren eruiert und Verantwortlichkeiten festgelegt, wird im Workshop ein weiteres Werkzeug vorgestellt, das bei der Ausdifferenzierung und Detaillierung der Anforderungen unterstützt. Im Projekt wurde ein Schema entwickelt, um Unternehmen im IT-Beschaffungsprozess für den Schutzbedarf der von einer Beschaffung betroffenen Daten zu sensibilisieren. Dieses Werkzeug lässt sich wie folgt in das Beschaffungsframework von Heckman (2003) einordnen ([Abbildung 9](#)).

Abbildung 9: Der IT-Beschaffungsprozess / Akquisition
(in Anlehnung an Heckman 2003)

Informations- und Kommunikationstechnik spielt für eine Vielzahl von Unternehmen eine bedeutende Rolle und die Abhängigkeit von Informationstechnik nimmt zu, trotz eines ebenso stetig wachsenden Gefährdungspotenzials. Bei der Suche nach Antworten auf entstehende Fragen der Informationssicherheit ist zu bedenken, dass Informationssicherheit „eine Kombination aus technischen, organisatorischen, personellen und baulich-infrastrukturellen Aspekten ist“ (BSI 2011, S. 13). Wie in Kapitel 19 dargestellt, hängt das Ausmaß, in dem entsprechende Aspekte zu adressieren sind, vom Schutzbedarf der durch die IT-Systeme verarbeiteten oder gespeicherten Daten ab.

Das in Kapitel 19 vorgestellte Template zur Analyse und Klassifizierung des Schutzbedarfs und die vermittelten Zusammenhänge sollen im Workshop die Teilnehmer für den Schutzbedarf der Daten sensibilisieren, die von der jeweiligen Beschaffungsentscheidung betroffen sein können. Sie regen somit die Diskussion im Team an und ermuntern, ggf. eine eigene Klassifizierung vorzunehmen und gegebenenfalls eine Liste notwendiger Sicherheitsmaßnahmen auf Basis des IT-Grundschiebkatalogs (BSI 2011) oder vergleichbarer Kataloge zu diskutieren.

24.4.4 *Werkzeug D: Der Kriterienkatalog CloudServiceCheck als Template in der Anforderungsspezifikation*

Abschließend wird im Workshop der im Projekt entwickelte Kriterienkatalog CloudServiceCheck als Werkzeug zur Unterstützung der Anforderungsdefinition vorgestellt.

Die Informationsbeschaffung zur Vorbereitung einer Beschaffungsentscheidung erfordert ein strukturiertes Vorgehen in Form des Vergleichs einzelner Lösungen anhand einheitlicher, vordefinierter Kriterien. Ein Kriterienkatalog kann bei der systematischen Zusammenstellung der für die Beschaffungsentscheidung relevanten Kriterien helfen. Auf diese Weise können Lücken in der Anforderungsbeschreibung aufgedeckt und verhindert werden. Ziel des CloudServiceCheck ist es, den an einer Nutzung von Cloud-Services interessierten Unternehmen eine Orientierung bei der Frage zu bieten, welche Informationen für die Entscheidung für ein Service-Angebot relevant sein können. Der hier beschriebene Kriterienkatalog für Cloud-Services kann wie eine Checkliste eingesetzt werden. Diese hilft bei der Identifikation relevanter Auswahlkriterien. Darüber hinaus bietet sie Unterstützung bei der nachfolgenden Analyse und Bewertung von Serviceangeboten, damit keine als entscheidungsrelevant identifizierten Kriterien außer Acht gelassen werden. Zur Systematisierung der Anforderungsanalyse wurde eine zielgruppenspezifische Strukturierung von Eigenschaften in fünf Sichten gewählt (siehe [Abbildung 1](#) in Kapitel 9).

Zur detaillierten Vorstellung der Kriterien sei an dieser Stelle auf Kapitel 9 dieses Buches verwiesen. Im Workshop kann der Kriterienkatalog zum einen in Form einer Zeitschrift verwendet werden oder auch in elektronischer Form, implementiert in gleicher Art und Weise wie das in Kapitel 7 vorgestellte Werkzeug zur Analyse der den Beschaffungsprozess beeinflussenden Faktoren.

24.5 Zusammenfassung und Teilnehmer-Rückmeldungen

Auf Basis der vorgestellten Geschäftsszenarien, ihrer detaillierten Analyse und Strukturierung sowie der anschließenden Bearbeitung im Team entlang der Phasen eines typischen IT-Beschaffungsprozesses, unter Zuhilfenahme der im Projekt entwickelten Werkzeuge, ermöglicht der Workshop den Teilnehmern das spielerische Kennenlernen von Beschaffungsherausforderungen rund um Cloud-Services. Die Workshop-Teilnehmer erlernen Tools und Templates zur Strukturierung von Beschaffungsherausforderungen sowie Werkzeuge kennen, um innerhalb einzelner Beschaffungsphasen strukturiert und mit Übersicht zu agieren. Die im Projekt entwickelten Werkzeuge werden im Workshop praxisnah eingesetzt und adressieren somit gerade den Bedarf mittelständischer Unternehmen. Der Werkzeugeinsatz im Workshop und darüber hinaus in der Unternehmenspraxis ist somit nicht nur geeignet, die Projektergebnisse in die Unternehmen zu transferieren, sondern auch den Cloud-Services-Markt in Deutschland insgesamt zu fördern, da Hemmnisse und Unsicherheiten im Beschaffungsprozess abgebaut werden.

Bisherige Workshops haben gezeigt, dass etwa die Anregung, zunächst die Einflussfaktoren und Gegebenheiten zu untersuchen, als hilfreich angesehen wird. Auch wurde das Konzept der Schutzbedarfsanalyse der von der Beschaffung betroffenen Daten, insbesondere von Kleinunternehmen, als „guter Hinweis“ aufgenommen. Der vorgestellte Kriterienkatalog, CloudServiceCheck, wurde demgegenüber sowohl von kleinen, wie auch von Großunternehmen als willkommene Checkliste im Beschaffungsprozess und als Unterstützung bei der Festlegung eigener Anforderungen angesehen. Insbesondere die enthaltene Gliederung in Sichten (Basis-Sicht, technische Sicht, funktionale Sicht, operative Sicht, rechtliche Sicht) wurde als gute Struktur aufgefasst. Auch wurden insbesondere die enthaltenen Kriterien-Bündel zum Themenbereich „Sicherheit und Datenschutz“ von den Workshop-Teilnehmern mit Interesse aufgenommen. In den Workshops wurden darüber hinaus weitere Herausforderungen und Problemstellungen diskutiert, etwa:

- Welches Abstraktionsniveau reicht für SLA's? Welche Erfahrungen wurden diesbezüglich gemacht?

- Wie genau ist der Bedarf an „Dienstleistung“ zu beschreiben und zu spezifizieren?
- Warum sind Daten und ihr Schutzbedarf bei Cloud-Services so wichtig und warum ist es besonders relevant, wo meine Daten gespeichert sind?
- Wie bekomme ich meine Daten wieder aus etwaigen Cloud-Services zurück? Welche Erfahrungen haben andere bereits mit Datenexporten und Schnittstellen sammeln können?

24.6 Literaturverzeichnis

- BSI (2011):** IT-Grundschutz-Kataloge, Bundesamt für Sicherheit in der Informationstechnik – BSI, Bonn, Germany 2011.
- Garris, R.; Ahlers, R.; Driskell, J.E. (2002):** Games, Motivation, and Learning: A Research and Practice Model. In: Simulation & Gaming, Vol. 33 (2002) No. 4, S. 441-467.
- Heckman, R.L. (2003):** Managing the IT Procurement Process. In: IS Management Handbook. Brown, C.V.; Topi, H. (Hrsg.). 8. Aufl. Auerbach Publications, Washington D.C., USA 2003, S. 73-88.
- Hoberg, P.; Reidt, A.; Wollersheim, J.; Krcmar, H. (2014):** CloudServiceCheck, Ausgabe 1, 2014.
- Hoberg, P.; Wollersheim, J.; Krcmar, H. (2012):** Service Descriptions for Cloud Services – The Customer’s Perspective. Präsentiert auf der ConLife Academic Conference 2012, Köln, Deutschland.
- ohne Autor (2014):** RACI. <http://de.wikipedia.org/wiki/RACI>, zugegriffen am 28.07.2014.
- Pivec, P. (2014):** Game-based learning or game-based teaching? <http://core.kmi.open.ac.uk/display/4151799>, zugegriffen am 28.07.2014.
- Van der Valk, W.; Rozemeijer, F. (2009):** Buying business services: towards a structured service purchasing process. In: Journal of Services Marketing, Vol. 23 (2009) No. 1, S. 3-10.

25 Fallstudie: Open-Innovation

Anwendung der Methode in Kunden-Workshops durch einen Cloud-Service-Anbieter

R. Eberlein, A. Eberl

25.1 Einleitung

Unabhängig von der gewählten Branche sind Unternehmen meist bemüht, angebotene Produkte und Leistungen stets nahe am Kunden auszurichten. Häufig geschieht dies jedoch ohne direkte Einbeziehung des Kunden selbst, bzw. es wird versucht, über Marktbeobachtung/-forschung allgemeine Trends zu antizipieren und daraus Produkte zu entwickeln. Durch diese eher oberflächliche Betrachtung kommt es so immer wieder zu Produktentwicklungen, die vom Markt nicht angenommen werden.

Der Ansatz der „Open Innovation“ geht einen Schritt weiter. Hierbei versucht der Anbieter nicht nur, den Kunden zu analysieren, sondern ihn aktiv in die Produktentwicklung einzubinden. Es werden aber nicht nur die Kunden berücksichtigt, sondern auch alle anderen Stakeholder (z.B. Lieferanten). Durch den direkten Input erfolgt die Entwicklung deutlich näher am Markt, was zu einer Reduktion von Fehlschlägen bei der Produktentwicklung führen soll.

Ein Ziel des Forschungsprojektes Value4Cloud war die Evaluierung von Open-Innovation-Methoden in der Praxis. Die Umsetzung erfolgte durch die SpaceNet AG als Anbieter von IT-Business-Produkten und die Universität Kassel als Forschungspartner. Dieser Text konzentriert sich auf die Erkenntnisse der SpaceNet AG.

25.2 SpaceNet AG – ein Überblick

25.2.1 Das Unternehmen

Im Jahr 1993 gegründet zählt die SpaceNet AG als einer der ersten deutschen Internet-Provider zu den Pionieren dieses Geschäftsfeldes. Lag der Fokus in den Gründungsjahren insbesondere auf dem Bereich Internet Access, wurde das Portfolio rasch um weitere Business-Produkte wie Hosting, Housing, virtuelle Webserver und später auch eine eigene Maillösung sowie schließlich das Hosting virtueller Maschinen, quasi dem Kern des Cloud-Computings, erweitert.

25.2.2 Produktentwicklung

Auf den ersten Blick umfasst die Produktliste der SpaceNet AG das übliche Standardportfolio im Bereich der Business-IT. Daher ist es ein wichtiger Aspekt der Leistungserbringung, durch individuelle Komponenten in der Konzeption die vom Kunden gewählte Lösung weiter zu optimieren. Der durch die Kundennähe gesicherte stetige Zufluss neuer Impulse für Produkt-(weiter)entwicklungen und die Erfahrungen aus dem IT-Projektgeschäft, erlauben es der SpaceNet AG, die eigenen Produkte kontinuierlich zu verbessern sowie schnell auf Markttrends zu reagieren.

Der Forschungs- und Entwicklungsabteilung fällt bei der Erweiterung des Produktportfolios natürlich ein besonderer Stellenwert zu. Neben den direkt von Stakeholdern eingebrachten Ideen werden hier auch technische Neuerungen am Markt analysiert und in Zusammenarbeit mit dem Produktmanagement hinsichtlich ihrer Relevanz für das Segment kleiner und mittelständischer Unternehmen (KMU) sowie eine mögliche wirtschaftliche Umsetzung geprüft. Schließlich ist die Teilnahme an Forschungsprojekten wie aktuell Value4Cloud ein weiterer wesentlicher Baustein der SpaceNet-Produktentwicklung. Dies ermöglicht den aktiven Austausch mit Forschungseinrichtungen sowie Vertretern der Industrie und erlaubt die Mitgestaltung moderner zukunftssträchtiger Technologien.

25.2.3 *Virtualisierung vs. Cloud*

Auch wenn sich bereits seit langem Produkte im Portfolio der SpaceNet befinden, die unter dem Oberbegriff „Cloud-Computing“ zusammengefasst werden können, wurde bis vor kurzem die Verwendung des Terminus „Cloud“ zur Beschreibung der angebotenen Virtualisierungsprodukte vermieden. Wesentlichen Anteil an dieser Entscheidung hat v.a. die Art und Weise der Vermarktung Cloud-basierter Produkte. So werden diese dem Kunden gegenüber nur zu gerne von den Marketingabteilungen der IT-Anbieter undifferenziert als ideale Lösung für jedwede Herausforderung in der Business-IT angepriesen. Dies führt dazu, dass die „Cloud“ dem Kunden profillos erscheint bzw. dass die tatsächlichen Vor- und Nachteile einer solchen Lösung nicht greifbar sind. In Kombination mit den ersten Kundenerfahrungen, die dem von Anbietern gezeichneten Bild oft nicht oder nur zu einem geringen Teil gerecht wurden, führte dies bereits vor den inzwischen bekanntgewordenen, internationalen, nachrichtendienstlichen Abhörvorfällen zu einem verstärkten Misstrauen gegenüber Cloud-Produkten bei den Kunden.

Unter dem Motto „Wir erden die Cloud“ arbeitet SpaceNet nun seit 2012 daran, Kunden die „Cloud“ näherzubringen. Dies geschieht vor allem über umfassende Kommunikation bzgl. des Funktionsumfangs im Vergleich zu alternativen Lösungen sowie den zugehörigen sicherheitstechnischen und ökonomischen Aspekten. In diesem Kontext wird den Kunden ein transparentes Portfolio von Cloud-Produkten mit klarem Nutzen offeriert.

25.3 **Praxisevaluation: Workshops**

25.3.1 *Übersicht*

Zur Evaluierung von Open-Innovation wurden verschiedene Workshops ausgerichtet:

- Lead-User-Kundenworkshop
- Kunden- und Anbieterworkshop
- Online-Workshop (Test mit Studenten)

- Anbieterworkshop mit gate (als Anbieter u.a. für Infrastruktur von Unternehmensgründern innerhalb der Räumlichkeiten von gate)

Im Mittelpunkt der Open-Innovation-Evaluierung stehen die Workshops für Lead-User sowie Kunden- und Anbieter in diesem Kapitel. Im Anschluss werden die Möglichkeiten einer Online-Community für Open-Innovation separat betrachtet.

25.3.2 Methodik, Umsetzung, Ablauf

Methodik und Ablauf wurden in Zusammenarbeit mit der Universität Kassel festgelegt, die federführend für den wissenschaftlichen Teil der Open-Innovation-Workshops war.

Da Entscheider bei kleinen und mittelständischen Unternehmen vom Tagesgeschäft stark beansprucht werden, wurde die Workshopdauer auf rund einen Arbeitstag (6-8 Stunden, inkl. Pausen) festgelegt. Je Workshop wurde eine Teilnehmeranzahl von ca. 20 Personen anvisiert. Veranstaltungsort waren die Räumlichkeiten der SpaceNet AG in München. Bei den Teilnehmern handelte es sich um SpaceNet-Kunden und/oder -Partner (Anbieter), die per Email-Newsletter über die Veranstaltung informiert wurden.

Die Durchführung des Workshops erfolgte durch die Universität Kassel und wurde von SpaceNet-Mitarbeitern begleitet. Die wesentlichen Punkte der Agenda waren dabei wie folgt:

- Vorstellung
- Erwartungen der Kunden an den Workshop
- Einführung in das Thema Cloud-Computing
- Sammlung der Alltagsherausforderungen der Teilnehmer in Bezug auf IT
- Ausarbeitung von Lösungskonzepten für ausgewählte Alltagsherausforderungen in Gruppen inkl. Diskussion

Für die gemeinschaftliche Ausarbeitung der Lösungskonzepte kam hierbei Workshop-übergreifend das Business Model Canvas nach Osterwalder zum Einsatz (Osterwalder 2014a). Im Kunden- und Anbieterworkshop wurde er-

gänzend das Value Proposition Canvas, ebenfalls nach Osterwalder, mit hinzugenommen (Osterwalder 2014b).

Während bei ersterem die strukturierte Entwicklung einer Produktidee bis hin zum tragenden Geschäftskonzept im Mittelpunkt steht, konzentriert sich Letzteres auf die Analyse des Kunden, also: Vor welchen Herausforderungen steht dieser, was bereitet Kopfzerbrechen bzw. wie kann diesem anbieterseitig (Produkte/Leistungen) das Tagesgeschäft erleichtert werden?

25.3.3 *Ergebnisse*

Natürlich steht im Rahmen dieser Fallstudie die Evaluation von Open-Innovation in der Praxis im Mittelpunkt, jedoch sollen im Sinne des Forschungsprojekts als Ganzem hier auch wichtige Beobachtungen zur Kundenwahrnehmung der „Cloud“ erwähnt werden, die im Rahmen der Workshops gemacht wurden. Zudem sind die gewonnenen Erkenntnisse auch ein wichtiges Bewertungskriterium für den gewählten Open-Innovation-Ansatz.

25.3.3.1 Kundenwahrnehmung der Cloud

Wie bereits eingangs erwähnt, setzt sich der IT-Markt häufig eher undifferenziert mit dem Begriff „Cloud“ auseinander. Dies spiegelt sich auch in den Reaktionen im Rahmen der Workshops wieder. So fiel auf, dass es starke Unterschiede in der Wahrnehmung des Begriffes im Umfeld kleiner und mittelständischer Unternehmen gab. Insbesondere wurde dies im ersten Workshop deutlich, der ein recht heterogenes Teilnehmerfeld aufwies. Allgemein kann festgehalten werden, dass sich viele Teilnehmer bereits im Cloudumfeld bewegten, sich dessen aber relativ häufig gar nicht bewusst waren. Konkret als Cloudprodukte wurden hier insbesondere Lösungen aus dem Endnutzer-Umfeld (z.B. Dropbox) benannt – Business-Anwendung waren weniger geläufig bzw. bewusst. Während der detaillierten Auseinandersetzung mit der „Cloud“ im Laufe der Veranstaltung stand Workshopübergreifend die Sicherheit der eigenen Daten, insbesondere durch den Standort Deutschland, im Vordergrund. Hierbei ging es wohlgemerkt nicht nur um die Sicherheit vor Fremdzugriff, sondern auch um den störungsfreien Zugriff auf die im Rechenzentrum des Service-Providers liegenden Daten. Insgesamt ist es für viele Kunden lt. eigener Aussage aber v. a. wichtig, einen FullService-

Provider zu haben, der sich um ein möglichst großes Spektrum der Kunden-IT kümmert und zu dem ein vertrauensvolles Verhältnis besteht. Die beste Lösung für ein Problem steht im Vordergrund, der Weg dahin (dediziert vs. virtualisiert) ist zweitrangig.

Die von SpaceNet geladenen Partnerunternehmen bzw. Anbieter lieferten hier weitere interessante Einblicke in die Marktsituation. So wurde festgestellt, dass allein die Verwendung des Wortes „Cloud“ im Produktnamen bzw. die eindeutige Zuordnung eines Produkts zu dieser Kategorie dessen Vermarktung deutlich erschwert. Dies ist ein weiterer Beleg für die Verunsicherung der Kunden bzgl. dieses Begriffs und dessen Inhalten, sowie eine Bestätigung der Zielsetzung des Value4Cloud-Projekts zur Schaffung von mehr Transparenz für den Mittelstand.

25.3.3.2 Einschätzung Open-Innovation

Die durchgeführten Open-Innovation-Workshops förderten interessante Informationen zu Tage, ließen aber auch gleichzeitig Schwachpunkte in der Methodik erkennen. Positiv sind v. a. die verschiedenen Herangehensweisen hinsichtlich der bearbeiteten Problemstellungen zu nennen. Der wissenschaftliche Blickwinkel der Universität Kassel in Kombination mit der Praxis, repräsentiert durch SpaceNet und Kunden, eröffnete allen Teilnehmern neue Perspektiven bzgl. möglicher Lösungskonzepte. Bezogen auf Innovation und eine konkrete Produktumsetzung waren die Ergebnisse jedoch nur bedingt tragfähig. Zum einen war dies dem breiten Branchenspektrum des Teilnehmerfeldes geschuldet, deren Herausforderungen im Arbeitsalltag sich teils deutlich unterscheiden. So wurden die Teilnehmer in der Gruppenarbeit ggf. mit Problemen konfrontiert, die im eigenen Unternehmen so nicht gegeben sind bzw. zu denen sie nur wenig beizusteuern hatten. Zudem variierten auch die Vorkenntnisse zum Thema „Cloud“ unter den Teilnehmern.

Weiterhin weist das Business Model Canvas Bereiche auf, die durch Kunden nur bedingt bearbeitet werden können. Gerade Informationen wie Kostenstruktur, Schlüsselpartner oder benötigte Ressourcen fehlen natürlich, womit die Erstellung eines wirtschaftlich tragfähigen Konzepts im Rahmen der Workshops erschwert wurde.

Auf jeden Fall sieht die SpaceNet AG die Erweiterung des direkten Austausches mit den Kunden als erstrebenswert an. Wurde bisher im Rahmen der „Business-Frühstück“ genannten Rechenzentrumsführungen bereits regelmäßig Kundenkontakt abseits aktueller Projekte gepflegt, wird – nach den Erfahrungen aus den Workshops – über weitere Möglichkeiten für einen gezielten Austausch nachgedacht.

25.4 Exkurs: Open-Innovation mittels Online-Community

Im Laufe der Durchführung der Präsenzworkshops stellte sich die Frage, inwieweit Kunden online in die Produktentwicklung mit eingebunden werden könnten. Konkret verfügte die Universität Kassel mit „SAPiensi“ bereits zu diesem Zeitpunkt über ein voll funktionsfähiges Online-Portal, welches die Durchführung kollaborativer Projekte gestattete.

25.4.1 Umsetzung Testworkshop mit Studenten

Um die Möglichkeiten von Online-Portalen für Open-Innovation-Zwecke zu überprüfen, transferierte die Universität Kassel das Konzept der Praxisworkshops in SAPiensi. Grundvoraussetzung war die Bildung von Gruppen zur gemeinsamen Erstellung eines Business-Models. Das Canvas selbst wurde direkt im Portal zur Befüllung vorgehalten. Ein gruppenübergreifender Zugriff auf die Konzepte war nicht möglich – es konnten nur die Inhalte des eigenen Teams eingesehen bzw. verändert werden. Als Mittel zur Kommunikation stand jeder Gruppe ein Kommentarbereich zur Verfügung, der jeden Beitrag mit Autor, Datum und Uhrzeit aufführte.

Um die tatsächliche Funktionstüchtigkeit der Plattform für diesen Einsatzzweck zu überprüfen, wurde ein Testworkshop mit IT-Studenten der Universität Kassel durchgeführt. Für einen schnellen Einstieg in die Materie sollten sich die Studentengruppen in die Rolle von Mitarbeitern eines IT-Anbieters versetzen, der sein Portfolio um Cloud-Produkte erweitern will. Jede Gruppe war dazu angehalten, nach einer kurzen Marktanalyse ein Produkt auszuwählen und hierfür ein Geschäftsmodell auszuarbeiten. Nach einer gemeinsamen Einführungsveranstaltung der Universität Kassel und von SpaceNet hatten die Studenten dabei einen Monat Zeit, ihre individuellen Konzep-

te umzusetzen. Während dieser Zeit standen stets Mitarbeiter der Universität Kassel bzw. von SpaceNet als Tutoren zur Verfügung, um auf etwaige Fragen der Studenten einzugehen. Die Tutoren hatten zudem Zugriff auf alle Gruppenkonzepte und konnten bei Bedarf Einfluss auf die Entwicklung nehmen.

25.4.2 Einschätzung Online-Portal

Während grundsätzlich alle Hilfsmittel zur erfolgreichen Umsetzung eines Produktkonzepts vorhanden waren, zeigte der Studentenworkshop jedoch einige Schwächen auf.

Trotz der ausdrücklichen Bitte, die gesamte Kommunikation im Rahmen der Plattform durchzuführen, erfolgte die Bearbeitung mehrheitlich offline. In Kombination mit der stichpunkthaften Befüllung der Business Model Canvas war es somit seitens der Tutoren schwierig zu bewerten, in welche Richtung eine Ausarbeitung ging und ob ein Eingreifen notwendig war. Weiterhin konnte so nicht erfasst werden, wie sich die Gruppendynamik gestaltete bzw. wer welche Punkte beisteuerte. Bei einigen Gruppen gab es des Weiteren bewertungsfähige Konzepte erst kurz vor Abschluss des Workshops, was steuernde Maßnahmen zusätzlich erschwerte.

Natürlich sind einige der o.g. Schwierigkeiten insbesondere dem studentischen Umfeld geschuldet, dennoch verdeutlichen diese in Kombination mit den Erfahrungen aus den Präsenzveranstaltungen mit Kunden auch Problemfelder für potenzielle Kundenworkshops. Hier sind u.a. zu nennen:

25.4.2.1 Zeit

Während sich Kunden für einen Präsenzworkshop bewusst Zeit nehmen bzw. aus dem Arbeitsalltag zurückziehen, unterliegt ein Online-Workshop über die gesamte Dauer einer Abwägung gegenüber anderer Geschäftstätigkeiten. Hier hängt die Teilnahmebereitschaft stark vom empfundenen Nutzen ab, also z.B., ob das zu entwickelnde Lösungskonzept für den eigenen Geschäftsbetrieb überhaupt relevant ist.

25.4.2.2 Fachwissen

Bereits in den Präsenzworkshops wurde deutlich, dass es spürbare Unterschiede bzgl. des Wissens der einzelnen Teilnehmer zum Cloud-Computing gab. Während Präsenzveranstaltungen den Tutoren ermöglichen, hieraus resultierende Probleme schnell zu identifizieren und diesen entgegenzuwirken, ist dies im Rahmen eines Online-Portals bereits schwieriger umzusetzen. So besteht bspw. die Gefahr, dass sich Teilnehmer wegen eines empfundenen Wissensrückstandes nicht weiter einbringen.

Allgemein besteht die Herausforderung, dass Konzepte stark im Sinne eines oder einiger weniger Meinungsführer geprägt werden, womit sie als Basis für die Produktentwicklung, gerade in einem heterogenen Segment wie den kleinen und mittelständischen Unternehmen, kritisch zu hinterfragen sind.

Allerdings sind durchaus Szenarien denkbar, für die Open-Innovation mittels Online-Plattform umsetzbar ist. Dies erfordert insbesondere Kundengruppen, deren Bedürfnisse einander stark ähneln, also z.B. gleiche oder ähnliche Branche und Unternehmensgrößen, ggf. auch StartUp-Unternehmen.

25.5 Quellverzeichnis

Osterwalder, A. (2014a): Business Model Canvas. <http://www.businessmodelgeneration.com/canvas/bmc>, zugegriffen am 2014-07-28.

Osterwalder, A. (2014b): Value Proposition Canvas. http://www.businessmodelgeneration.com/downloads/value_proposition_canvas.pdf, zugegriffen am 2014-07-28.

Teil G:

Geschäftsmodelle

26 Geschäftsmodelle für marktunterstützende Mehrwertdienste im Cloud-Computing-Ökosystem

P. Hoberg, J. Wollersheim, H. Krcmar

26.1 Einleitung

Cloud-Computing ist ein Systemgeschäft, bei dem hoch-standardisierte IT-Services für einen anonymen Markt bereitgestellt werden. Kunden beziehen Cloud-Angebote häufig ohne einen direkten, persönlichen Kontakt zum Cloud-Anbieter als so genannten Self-Service über Marktplattformen wie Google Apps Market oder Force.com.

Cloud-Computing stellt damit sowohl potenzielle Cloud-Nutzer als auch Cloud-Anbieter vor neue Herausforderungen. Auf der einen Seite müssen Unternehmen, die IT-Services aus der Cloud als Self-Service beziehen wollen, alle für die Auswahlentscheidung relevanten Informationen selbst beschaffen. Ein kaum zu überblickendes Angebot an Cloud-Services stellt potenzielle Kunden vor das Problem, einen ihren Ansprüchen entsprechenden Service auszuwählen.

Auf der anderen Seite sehen sich die Cloud-Anbieter erheblichen Akzeptanzproblemen im Markt gegenüber. Diese Akzeptanzprobleme haben unterschiedliche Gründe. So konkurrieren etablierte IT-Serviceanbieter mit einer großen Zahl neuer Dienstleister auf dem Markt für Cloud-Services. Für diese neuen Dienstleister ist ihre fehlende Reputation eine große Hürde, um im Markt Fuß zu fassen. Darüber hinaus sind die am Markt verfügbaren Services nur schwer miteinander vergleichbar. Häufig fehlen in den Servicebeschreibungen der Cloud-Anbieter für die Auswahlentscheidung des Kunden relevante Informationen.

Das große Angebot an Services, deren eingeschränkte Vergleichbarkeit und das Fehlen relevanter Leistungsinformationen haben zu einem hochgradig intransparenten Markt geführt. Zuletzt haben die Enthüllungen um von

Geheimdiensten kompromittierte Kommunikationsverbindungen zu einer zusätzlichen, starken Verunsicherung bei potenziellen Cloud-Nutzern geführt.

Um Unternehmen bei der Auswahlentscheidung und kleine und mittelständische Anbieter von Cloud-Services bei der Etablierung ihres Angebotes im Markt zu unterstützen, bieten die Partner des Value4Cloud-Konsortiums einen auf die Bedürfnisse von Kunden und Anbietern abgestimmten Katalog an Beratungsleistungen und Auftragsarbeiten an. Das branchenunabhängige Angebot richtet sich an kleine und mittelständische Unternehmen sowie Start-ups, die den Einsatz oder das Angebot von Cloud-Computing planen.

Die Tätigkeit der Konsortialpartner soll nachhaltig und mit Gewinnerzielungsabsicht ausgeübt werden. Ein Handelsregistereintrag ist nicht vorgesehen. Möglicher Hauptsitz des Unternehmens ist München. Weitere Standorte wären in diesem Fall in Köln und Kassel vorgesehen. Die Anmietung gesonderter Geschäftsbereiche ist für die unternehmerische Tätigkeit nicht notwendig.

Bei der Akquise von Neukunden, die den Einsatz oder das Angebot von Cloud-Computing bereits planen, wird das Value4Cloud-Konsortium von seiner starken Vernetzung in regionalen und nationalen Wirtschaftsverbänden sowie von seiner Nähe zur Gründerszene im universitären und außeruniversitären Umfeld profitieren können.

26.2 Das Produkt- und Leistungsprogramm

Das Projekt Value4Cloud adressiert die Herausforderungen von Anwendern und Anbietern von Cloud-Services gleichermaßen. Die in Teil E dieses Buches beschriebenen Projektergebnisse unterstützen Unternehmen in beiden Rollen, Nutzer wie Anbieter. Um die Unterstützung weiter zu verfeinern und die Anwendbarkeit der Ergebnisse in der Unternehmenspraxis zu verbessern, wurden bereits Workshops mit Unternehmen durchgeführt. Darauf aufbauend wurden Fallstudien und Tutorials entwickelt, die die Einbindung der im Projekt entwickelten Ergebnisse in die Prozesse und Abläufe im Unternehmen beispielhaft veranschaulichen (siehe hierzu Teil F, insbesondere Kapitel 24 und 25).

Abbildung 1: Organisatorische und fachliche Gliederung des Geschäftsmodells (Eigene Darstellung).

Aufbauend auf diesen Ergebnissen hat das Value4Cloud-Konsortium Leistungsbündel in den Bereichen Anwender- und Anbietercoaching sowie Beratung zusammengestellt, die nach Abschluss des Projekts am Markt angeboten werden.

Analog zur Gliederung der Projektergebnisse gliedert sich das Leistungsportfolio in zwei Bereiche:

- Anwenderservices und
- Anbieterservices.

Fachlich und organisatorisch kann jeder der beiden Bereiche wiederum in mehrere Service-Gruppen unterteilt werden. Jeder Service-Gruppe ist ein Konsortialpartner aus dem Projekt Value4Cloud zugewiesen, der die Gruppe leitet. Eine Übersicht über die Service-Gruppen bietet [Abbildung 1](#).

In den folgenden Abschnitten werden die einzelnen Service-Gruppen mit ihrem Leistungsangebot näher erläutert.

26.2.1 *Anwendercoaching*

Die Service-Gruppe Anwendercoaching bietet Anwenderunternehmen ein- bis zweitägige Workshops zum Thema Cloud-Service-Beschaffung an. Diese Beschaffung stellt Unternehmen vor erhebliche Probleme (Wollersheim/Krcmar 2013), nicht nur in Bezug auf Aspekte wie die Kostenkalkulation, sondern auch in Bezug auf die Bedarfsanalyse, das Abschätzen des Konfigurations- und Testaufwandes oder die notwendigen Supportstrukturen. Vor allem KMU fehlt es noch an Erfahrung im Bereich der IT-Beschaffung. Die Zielgruppe der Beratungsleistungen für Cloud-Service-Anwender sind deshalb IT-Anwenderunternehmen (Ansprechpartner: Unternehmensgründer, Geschäftsführer, Leiter der IT, Leiter von Fachabteilungen, IT-Einkäufer), die Cloud-Services zukünftig nutzen wollen.

In den Workshops erhalten Teilnehmer Informationen zur idealtypischen Durchführung des Beschaffungsprozesses für Cloud-Services und werden bspw. über möglicherweise relevante fachliche und rechtliche Kriterien zur Service-Auswahl informiert. Auch wird der Austausch der Teilnehmer untereinander in den Workshops gefördert.

Zur Schulung von KMU in der Cloud-Service-Beschaffung kann auf den im Projekt Value4Cloud entwickelten CloudServiceCheck¹ zurückgegriffen werden. Der CloudServiceCheck unterstützt KMU bei der Analyse und dem Vergleich von Cloud-Services. Zusätzlich können der selbstentwickelte Value4Cloud-Softwareprototyp und eine Datenbank mit Beispiel-Services eingesetzt werden, um die Schulungsteilnehmer bei der Kriterienfindung für die Service-Auswahl zu leiten.

Als Erlösmodell für das Schulungsangebot ist eine Teilnahmegebühr geplant. Diese soll variabel sein und wird sich nach der Anzahl der Teilnehmer und dem Typ der Schulung richten. Geplant sind Schulungsveranstaltungen mit unterschiedlicher Gruppengröße und unterschiedlichen Inhalten. Dabei werden die Schulungen jeweils thematisch aufeinander aufbauen und möglichst homogene Unternehmensgruppen zusammenfassen, um den Austausch der Teilnehmer auf Augenhöhe zu fördern.

1 Zu beziehen über www.value4cloud.de

Abbildung 2: Business Model Canvas / Anwendercoaching (In Anlehnung an Osterwalde/Pigneur 2010).

Eine Strukturierung der Elemente des Geschäftsmodells der Service-Gruppe „Anwendercoaching“ anhand des Business Model Canvas (Osterwalder/Pigneur 2010) bietet [Abbildung 2](#).

26.2.2 Service-Auswahl

Die Service-Gruppe Service-Auswahl bietet Unternehmen eine individuelle Beratung und Unterstützung bei der Cloud-Service-Auswahl. Zur Zielgruppe gehören Unternehmen, die eine Nutzung von IT-Services aus der Cloud erwägen und sich unabhängig über wirtschaftliche, technische und rechtliche Aspekte informieren möchten.

Bestandteile des Leistungsangebotes sind: (1) die Unterstützung bei der Durchführung einer methodengeleiteten fachlichen Anforderungsanalyse sowie der Identifikation individueller Kriterien für die Service-Auswahl, (2) Hilfe bei der Markterhebung und Markteingrenzung und (3) die Unterstützung bei der Vorauswahl relevanter Cloud-Services anhand der individuellen Kriterien des Anwenderunternehmens.

Abbildung 3: Business Model Canvas / Service-Auswahl (In Anlehnung an Osterwalde/Pigneur 2010).

Wie beim Anwendercoaching greift die Service-Gruppe Service-Auswahl auf den CloudServiceCheck als zentrale Ressource für die Erbringung der Beratungsdienstleistung zurück. Als Erlösmodell für das Beratungsangebot ist eine Beratungsgebühr auf Stundenbasis geplant.

Eine Strukturierung der Elemente des Geschäftsmodells der Service-Gruppe Service-Auswahl anhand des Business Model Canvas (Osterwalder/Pigneur 2010) bietet [Abbildung 3](#).

26.2.3 Anbietercoaching

Die Service-Gruppe Anbietercoaching bietet Cloud-Service-Anbietern ein- bis zweitägige Workshops (1) zur Vorbereitung auf eine Zertifizierung und zur konsumentengerechten Beschreibung von Cloud-Services oder (2) zu deren vertrauensförderlichen und rechtsverträglichen Gestaltung an.

Zur Zielgruppe von Workshop (1) gehören Vertreter von Unternehmen, die das Informationsangebot rund um das eigene Cloud-Angebot kundenorientiert gestalten wollen. In den Workshops erhalten die Teilnehmer einen Überblick über die Art und Weise einer anwendergerechten Beschreibung von Cloud-Services. Cloud-Service-Anbieter werden auf diese Weise bei der nut-

zergerechten Außendarstellung ihres Produktes im Markt unterstützt. Ob die Darstellung eines Cloud-Services den Anforderungen potenzieller Kunden entspricht, ist einerseits von der Beschreibung des Service anhand geeigneter Kriterien abhängig. Andererseits ist das Serviceportfolio eines Anbieters anhand geeigneter Kategorien zu strukturieren, um potenziellen Kunden das Auffinden der für sie geeigneten Services zu ermöglichen. Hierzu wird eine Beratung für die kundengerechte Beschreibung von Cloud-Services sowie für die Konzeptionierung eines Kriterienkatalogs für Cloud-Services angeboten.

Die Beratung hinsichtlich der Beschreibung und Kategorisierung von Cloud-Services erfordert Erfahrungswissen und Kenntnisse der Kundenanforderungen. Diese sind insbesondere abhängig vom Ablauf und dem Informationsbedarf im Beschaffungsprozess für Cloud-Services auf Kundenseite. Das Value4Cloud-Konsortium kann hier auf umfangreiche Erfahrungen aus der Erforschung organisationaler Beschaffungsprozesse sowie auf Erfahrungen in der Konzeption und Implementierung von Servicekatalogen zurückgreifen.

Vor dem Hintergrund der Akzeptanzprobleme, denen sich Cloud-Computing als neues IT-Bereitstellungsmodell im Markt gegenüber sieht, wird neben der kundengerechten Darstellung des Cloud-Angebotes eine Zertifizierung durch akkreditierte Prüfungsorganisationen immer wichtiger. Das Value4Cloud-Konsortium unterstützt Cloud-Anbieter beim Aufbau von Vertrauen im Markt durch das Angebot von Schulungen zur Vorbereitung der Zertifizierung des eigenen Cloud-Angebotes. Die Teilnehmer lernen mögliche Zertifizierungsprozesse für Cloud-Services und deren Anbieter kennen, erhalten einen Überblick über aktuelle Zertifizierungsmöglichkeiten sowie die Anforderungen für eine Zertifizierung.

Zur Zielgruppe von Workshop (2) gehören Vertreter von Unternehmen, die ihr Cloud-Angebot vertrauensförderlich sowie rechtmäßig und rechtsverträglich gemeinsam mit Experten und Vertretern anderer Unternehmen gestalten wollen. Neben Fragen zu vertrauensbeeinflussenden Faktoren und zu vertrauensförderlichen Maßnahmen werden Fragen zur rechtmäßigen und rechtsverträglichen Gestaltung von Cloud-Services mit Hilfe von Anforderungsmustern beantwortet.

Abbildung 4: Business Model Canvas / Anbietercoaching (In Anlehnung an Osterwalde/Pigneur 2010).

Als Erlösmodell für das Schulungsangebot ist eine Teilnahmegebühr geplant. Analog zum Anwendercoaching wird diese variabel sein und sich nach der Anzahl der Teilnehmer und dem Typ der Schulung richten. Es werden Schulungsveranstaltungen mit unterschiedlicher Gruppengröße und unterschiedlichen Inhalten geplant. Die Schulungen werden jeweils thematisch aufeinander abgestimmt sein.

Eine Strukturierung der Elemente des Geschäftsmodells der Service-Gruppe Anbietercoaching anhand des Business Model Canvas (Osterwalder/Pigneur 2010) bietet [Abbildung 4](#).

26.2.4 Marktanalyse und Innovation

Die Service-Gruppe Marktanalyse und Innovation bietet Cloud-Anbietern im Rahmen eines individuellen Forschungs- und Beratungsauftrages Unterstützung bei der Produktverbesserung mit Hilfe strukturierter Methoden (Nutzerbefragung, offener Innovationsprozess) sowie bei der Produktpositionierung (Wettbewerbsanalysen, Whitepapers) an. Zur Zielgruppe gehören Unternehmen, die ihre Cloud-Angebote innovativ und kundenorientiert weiterentwickeln wollen.

Abbildung 5: Business Model Canvas / Marktanalyse und Innovation (In Anlehnung an Osterwalde/Pigneur 2010).

Die Inhalte richten sich nach den individuell vereinbarten Fragestellungen, etwa Nutzungsmöglichkeiten von Open-Innovation-Methoden zur kundenorientierten Weiterentwicklung angebotener Leistungen oder Möglichkeiten zur Verbesserung von Service-Beschreibungen. Als Erlösmodell für das Beratungsangebot ist eine Beratungsgebühr auf Stundenbasis geplant.

Eine Strukturierung der Elemente des Geschäftsmodells der Service-Gruppe Marktanalyse und Innovation anhand des Business Model Canvas (Osterwalder/Pigneur 2010) bietet [Abbildung 5](#).

26.3 Allgemeine Marktlage

Für Deutschland wird für 2015 ein Umsatz von 14 Mrd. € prognostiziert, was einem Marktwachstum von 30 % (vgl. [Abbildung 6](#)) gegenüber dem Vorjahr entspricht (BITKOM 2013). Das Wachstum im Cloud-Markt ist ein Indikator dafür, dass Cloud-Computing die Art verändern wird, wie Leistungen der IT-Industrie zukünftig bereitgestellt werden. So illustrieren Riedl et al. (2010) anhand eines Teaching Case, der auf Basis einer Fallstudie bei einem multi-

Abbildung 6: Umsatz mit Cloud Computing in Deutschland in Mrd. EUR (BITKOM 2013)

nationalen Konzern entwickelt wurde, welchen strategischen Herausforderungen sich traditionelle Outsourcing-Dienstleister durch Cloud-Computing gegenüber sehen. Das traditionelle Bereitstellungsmodell des IT-Outsourcings wird in einigen Marktsegmenten durch das alternative Bereitstellungsmodell Cloud-Computing ergänzt oder sogar abgelöst.

Aktuellen Marktdaten einer Studie des KPMG, BITKOM und PAC folgend setzen derzeit 10 % der Unternehmen in Deutschland Public-Cloud-Lösungen ein (KPMG 2013). Obwohl die Nutzung von Public-Cloud-Services insbesondere für KMU vielversprechend erscheint, hält sich der deutsche Mittelstand trotz vieler Vorteile von Cloud-Computing mit der Einführung entsprechender Services zurück. Dies ist vor allem auf eine im deutschen Mittelstand verbreitete generelle Skepsis gegenüber dem neuen Bereitstellungsmodell zurückzuführen.

Nach dem starken Zuwachs, den der Markt für Cloud-Computing im vergangenen Jahr generieren konnte, ist KPMG, BITKOM und PAC zufolge auch in den nächsten Jahren mit einem weiteren großen Zuwachs zu rechnen (KPMG et al. 2013). Damit wird der Markt nicht nur weiter an Attraktivität

für mittelständische IT-Dienstleister gewinnen, sondern auch an Akzeptanz bei kleinen und mittelständischen Unternehmen.

26.4 Ausblick und Kommunikation

Um die identifizierten Kundensegmente mit dem Leistungsangebot und deren Nutzenversprechen zu erreichen, müssen geeignete Kommunikationskanäle ausgewählt werden. Zu diesem Zweck sollen sowohl direkte als auch indirekte Kanäle genutzt werden. Als indirekter Kanal wird das Internet in Form der Webseite des Konsortiums genutzt. Zur direkten Kontaktaufnahme mit potenziellen Kunden sollen hingegen Fachkonferenzen und Messeauftritte genutzt werden.

Der Bedarf an Möglichkeiten für einen Erfahrungsaustausch zwischen Konsumenten sowie der Schulungsbedarf zur Cloud-Service-Beschaffung wächst mit zunehmender Popularität von Cloud-Computing im professionellen Bereich. Die enormen Zuwachsraten im Markt für Cloud-Services bieten damit sehr gute Chancen für das vom Value4Cloud-Konsortium geplante Vorhaben.

26.5 Literaturverzeichnis

- BITKOM (2013):** Umsatz mit Cloud Computing steigt auf fast 8 Milliarden Euro. http://www.bitkom.org/de/markt_statistik/64086_75301.aspx, zugegriffen am 28.07.2014.
- KPMG (2013):** Cloud Monitor 2013, KPMG & BITKOM, Düsseldorf, Deutschland 2013.
- KPMG; BITKOM; PAC (2013):** Cloud-Monitor 2013: Cloud-Computing in Deutschland – Status quo und Perspektiven, 2013.
- Osterwalder, A.; Pigneur, Y. (2010):** Business model generation: A handbook for visionaries, game changers, and challengers, John Wiley & Sons 2010.
- Pring, B.; Brown, R.H.; Leong, L.; Couture, A.W.; Biscotti, F.; Lheureux, B.J.; Frank, A.; Roster, J.; Cournoyer, S.; Liu, V.K. (2010):** Forecast: Public cloud services, worldwide and regions, industry sectors, 2009-2014. Gartner, 2010.
- Riedl, C.; Leimeister, S.; Böhm, M.; Yetton, P. (2010):** Competing in the Clouds: A Strategic Challenge for ITSP Ltd. In: Communications of the Association for Information Systems, Vol. 27 (2010) No. 1, S. 725-742.
- Wollersheim, J.; Kremer, H. (2013):** Purchasing processes for cloud services – An exploratory study of process influencing factors. Präsentiert auf der 22nd Annual IPSERA Conference, Nantes, Frankreich.

Teil H:

Anhang

27 Veröffentlichungen

Bis zum Ende des Projektes Value4Cloud entstanden 61 wissenschaftliche Veröffentlichungen, davon 21 Zeitschriftenbeiträge. Darüber hinaus befinden sich derzeit noch zahlreiche Artikel im Begutachtungsprozess.

1. **Behling, T.; Bergner, J.; Borges, B.; Cellarius, M.; Duisberg, A.; Eckhard, J.; Glaus, A.; Hajek, B.; Hartmann, W.; Hilber, M.; Jäger, H.; Klodt, K.; Kramer, R.; Kroschwald, S.; Landvogt, J.; Lepper, U.; Marnau, N.; Meents, G.J.; Rüdiger, M.; Sädler, S.; Schiefer, G.; Schulz, G.; Taeger, J.; Trusch, B.; Ulmer, C.-D.; v. Bülow, T.(2012):** Datenschutzrechtliche Lösungen für Cloud Computing Rechtspolitisches Thesenpapier der AG Rechtsrahmen, Kompetenzzentrum Trusted Cloud – AG Rechtsrahmen des Cloud Computing (Hrsg.), 2012.
2. **Boos, C.; Kroschwald, Steffen; Wicker, Magda (2013):** Datenschutz bei Cloud Computing zwischen TKG, TMG und BDSG – Datenkategorien bei der Nutzung von Cloud-Diensten, Zeitschrift für Datenschutz (ZD) 2013, S. 205-210.
3. **Buch, Meike; Gebauer, Lysann (2014):** Maßnahmenkatalog zur Vertrauenserrhöhung im Cloud Computing. In: Jan Marco Leimeister (Hrsg.), Working Paper Series, Nr. 4, Kassel, Deutschland.
4. **Buch, Meike; Gebauer, Lysann; Hoffmann, Holger (2014):** Vertrauen in Cloud Computing schaffen – Aber wie?. WIRTSCHAFTSINFORMATIK & MANAGEMENT, Ausgabe 03/2014, S. 67-77.
5. **Gao, Fangjian; Schneider, Stephan (2012): Cloud-Frameworks:** Eine Übersicht aus der Wirtschaftsinformatik-Perspektive. ConLife 2012 Academic Conference, Köln, Deutschland, 2012.
6. **Gebauer, Lysann; Söllner, Matthias; Leimeister, Jan Marco (2012):** Hemmnisse bei der Nutzung von Cloud Computing im B2B-Bereich und die Zuordnung dieser zu den verschiedenen Vertrauensbeziehungen. ConLife 2012 Academic Conference, Köln, Deutschland, 2012.
7. **Gebauer, Lysann; Söllner, Matthias; Leimeister, Jan Marco (2013):** Towards Understanding the Formation of Continuous IT Use. 34th In-

- ternational Conference on Information Systems (ICIS), Milano, Italy, 2013.
8. **Kunz, Michael Marcin; Gebauer, Lysann; Ebel, Philipp Alexander; Leimeister, Jan Marco (2013):** Applying an Open Innovation Method for identifying Challenges in the Cloud Business Environment. ConLife 2013 Academic Conference, Berlin, Germany, 2013.
 9. **Kunz, Michael Marcin; Söllner, Matthias; Leimeister, Jan Marco (2012):** Untersuchung bestehender Geschäftsmodelle etablierter Cloud Anbieter. ConLife 2012 Academic Conference, Köln, Deutschland, 2012.
 10. **Kunz, Michael Marcin; Söllner, Matthias; Leimeister, Jan Marco (2013):** Exploring Business Models for IT-enabled Product-Service-Systems. DIBME 2013 Pre-ECIS Workshop on the Digitization in Business Models and Entrepreneurship, Utrecht, The Netherlands, 2013.
 11. **Kunz, Michael Marcin; Söllner, Matthias; Leimeister, Jan Marco (2014):** Successfully funded! – Welche Geschäftsmodelle machen crowdfinanzierte Cloud-Startups erfolgreich?. Multikonferenz Wirtschaftsinformatik (MKWI), Paderborn, Germany, 2014.
 12. **Glaus, A.; Hajek, B.; Hilber, M.; Klodt, K.; Reintzsch, D.; Riffer, C.; Städtler, S.; Wicker, M. (2012):** Lizenzierungsbedarf beim Cloud Computing – Welche Rechte zur Nutzung von Software benötigen Anbieter und Nutzer von Cloud Computing?, Arbeitspapier der AG Rechtsrahmen, Kompetenzzentrum Trusted Cloud – AG Rechtsrahmen des Cloud Computing (Hrsg.), 2012.
 13. **Grochol, P.; Schneider, S.; Sunyaev, A. (2014):** Cutting Through the Jungle of Cloud Computing Whitepapers: Development of an Evaluation Model. In: Trusted Cloud Computing. Springer, Berlin. ISBN 978-3-319-12717-0
 14. **Hilber, M.; Duisberg, A.; Glaus, A.; Hajek, B.; Kramer, R.; Reintzsch, D.; Städtler, S.; v. Bülow, T.; Wicker, M. (2014):** Cloud Computing und Open Source Software (zusammen mit), Arbeitspapier der AG Rechtsrahmen, Kompetenzzentrum Trusted Cloud – AG Rechtsrahmen des Cloud Computing (Hrsg.), 2014.

15. **Hoberg, Patrick; Wollersheim, Jan; Krcmar, Helmut (2012):** Service Descriptions for Cloud Services – The Customer's Perspective. ConLife 2012 Academic Conference, Köln, Deutschland, 2012.
16. **Hoberg, Patrick; Wollersheim, Jan; Krcmar, Helmut (2012):** The Business Perspective on Cloud Computing – A Literature Review of Research on Cloud Computing. 18th Americas Conference on Information Systems (AMCIS) 2012.
17. **Hoberg, Patrick; Wollersheim, Jan; Böhm, Markus; Krcmar, Helmut (2012):** Cloud Computing – Überblick und Herausforderungen für das Controlling. In: Controlling, Zeitschrift für erfolgsorientierte Unternehmenssteuerung, 2012, Vol. 24, Nr. 6, S. 294-300.
18. **Hoffmann, Holger; Söllner, Matthias (2014):** Incorporating Behavioral Trust Theory Into System Development for Ubiquitous Applications. Personal and Ubiquitous Computing, 18 (1), 117-128.
19. **Kroschwald, Steffen; Wicker, Magda (2012):** Tagungsbericht: Jahreskongress Trusted Cloud, Kommunikation & Recht (K&R) 2012, Heft 12, V-VI.
20. **Kroschwald, Steffen; Wicker, Magda (2012):** Kanzleien und Praxen in der Cloud – Strafbarkeit nach § 203 StGB, Computer und Recht (CR) 2012, S. 758-764.
21. **Kroschwald, Steffen; Wicker, Magda (2012):** Zulässigkeit von Cloud Computing für Berufsgeheimnisträger: Strafbarkeit von Anwälten und Ärzten durch die Cloud? (Tagungsband: Jürgen Taeger (Hrsg.), IT und Internet – mit Recht gestalten (Tagungsband DSRI Herbstakademie 2012, Wuppertal, 12.-15.09, Oldenburg 2012, S. 733-758).
22. **Kroschwald, Steffen (2013):** Kollektive Verantwortung für den Datenschutz in der Cloud – Datenschutzrechtliche Folgen einer geteilten Verantwortlichkeit beim Cloud Computing, Zeitschrift für Datenschutz (ZD) 2013, 388-394.
23. **Kroschwald, Steffen (2013):** Verschlüsseltes Cloud Computing – Anwendung des Daten- und Geheimnisschutzrechts auf „betreibersichere“ Clouds am Beispiel der „Sealed Cloud“, in: Taeger (Hrsg.), Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter (Tagungsband DSRI Herbstakademie 2013), Oldenburg 2013, S. 289-308.

24. **Kroschwald, Steffen (2014):** Datenschutz-rechtsverträgliches Cloud Computing zwischen Anbietern, Nutzern und Kunden, in: Deutscher Dialogmarketing Verband (Hrsg.), Dialogmarketing Perspektiven 2014; 2015 (Tagungsband zum 9. wissenschaftlicher interdisziplinärer Kongress für Dialogmarketing am 1. Oktober 2014), Wiesbaden 2014, i.E.
25. **Kroschwald, Steffen (2014):** Schutz von Persönlichkeitsrechten in der „versiegelten“ Cloud – Anwendung und Rechtsfolgen des Datenschutz- und Berufsgeheimnisrechts auf „betreibersicheres“ Cloud Computing in der „Sealed Cloud“, in: Unicon (Hrsg.), Wie macht man Cloud sicher? Sealed Processing – Schutz der Inhalte und Metadaten (Tagungsband zum Symposium am 24. September 2014), München 2014, S. 18-28.
26. **Kroschwald, Steffen (2014):** Verschlüsseltes Cloud Computing – Auswirkung der Kryptografie auf den Personenbezug in der Cloud, Zeitschrift für Datenschutz (ZD) 2014, S. 75-80.
27. **Kroschwald, Steffen; Wicker, Magda (2014):** Veranstaltungsbericht „Trusted Cloud Jahreskongress 2014“, Kommunikation & Recht (K&R) 2014, Heft 9;2014, S. VI.
28. **Kroschwald, Steffen; Wicker, Magda (2014):** Einwilligung des Betroffenen in den Umgang mit seinen Daten als Lösung für das Cloud Computing, Datenschutzberater (DSB), Newsletter zum 15. Euroforum Datenschutzkongress 2014, S. 12-13.
29. **Lansing, J.; Schneider, S.; Sunyaev, A. (2013):** Cloud Service Certifications: Measuring Consumers' Preferences for Assurances. In: Proceedings of the 21st European Conference on Information Systems (ECIS 2013), Utrecht, Netherlands, June 5-8.
30. **Leimeister, Jan Marco (2012)** Dienstleistungsengineering und -management, Berlin, Heidelberg: Springer
31. **Leimeister, Jan Marco; Söllner, Matthias; Gebauer, Lysann (2014):** Vertrauensleitfaden für Cloud-Computing-Dienste – Ein Leitfaden zur Förderung von Vertrauen durch die Gestaltung der Online-Produktpräsentation. Chair for Information Systems, Kassel University, Kassel, Germany, 2014.
32. **Roßnagel, Alexander; Kroschwald, Steffen (2014):** Was wird aus der Datenschutzgrundverordnung? – Die Entschlüsselung des Europäischen

- Parlaments über ein Verhandlungsdokument, Zeitschrift für Datenschutz (ZD) 2014, S. 495-500.
33. **Sädtler, S.; Klodt, K.; Eble, G.; Glaus, A.; Duisberg, A.; Hajek, B.; Meents, J. G.; Borges, G.; Hilber, M.; Wicker, M. (2014):** Leitfaden – Vertragsgestaltung beim Cloud Computing, Arbeitspapier der AG Rechtsrahmen, Kompetenzzentrum Trusted Cloud – AG Rechtsrahmen des Cloud Computing (Hrsg.), 2014.
 34. **Schneider, S.; Lansing, J.; Gao, F.; Sunyaev, A. (2014):** A Taxonomic Perspective on Certification Schemes: Development of a Taxonomy for Cloud Service Certification Criteria. In: Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS 2014), Big Island, Hawaii, USA, January 6-9.
 35. **Schneider, S.; Lansing, J.; Sunyaev, A. (2013):** Empfehlungen zur Gestaltung von Cloud-Service-Zertifizierungen. In: Industrie Management. Volume 29, Issue 4, 13–17.
 36. **Schneider, S.; Sunyaev, A. (2014):** Determinant Factors of Cloud-Sourcing Decisions: Reflecting on the IT Outsourcing Literature in the Era of Cloud Computing. In: Journal of Information Technology (JIT) advance online publication. DOI: 10.1057/jit.2014.25.
 37. **Söllner, Matthias; Hoffmann, Axel; Hoffmann, Holger; Wacker, A.; Leimeister, Jan Marco (2012):** Understanding the Formation of Trust in IT Artifacts. 33rd International Conference on Information Systems (ICIS), Orlando Florida, USA, 2012.
 38. **Söllner, Matthias; Leimeister, Jan Marco (2013):** What We Really Know About Antecedents of Trust: A Critical Review of the Empirical Information Systems Literature on Trust. In: David Gefen (ed.), Psychology of Trust: New Research, Nova Science Publishers, Hauppauge, NY, USA, 2013, 127-155.
 39. **Söllner, Matthias; Pavlou, Paul; Leimeister, Jan Marco (2013):** Understanding Trust in IT Artifacts – A new Conceptual Approach. Academy of Management Annual Meeting, Orlando, Florida, USA, 2013.
 40. **Stein, Fabian; Schneider, Stephan; Sunyaev, Ali (2012):** ITIL als Grundlage zur Zertifizierung von Cloud-Services und -Anbietern. In: HMD – Praxis der Wirtschaftsinformatik (288), S. 33–41.

41. **Sturm, B.; Lansing, J.; Sunyaev, A. (2014):** Moving in the Right Direction?: Mapping Literature on Cloud Service Certifications' Outcomes with Practitioners' Perceptions. In: Proceedings of the 22nd European Conference on Information Systems (ECIS 2014), Tel Aviv, Israel, June 9-11.
42. **Sunyaev, Ali; Schneider, Stephan (2013):** Cloud Services Certification. In: Communications of the ACM (56, 2), S. 33-36.
43. **Wicker, Magda (2012):** Denk ich an Clouds in der Nacht, bin ich um den Schlaf gebracht, Hessisches Ministerium für Wissenschaft und Kunst, Science Tour 2012, Crossover Mottoslam: Soziale Vernetzung, 22. August 2012, Kassel.
44. **Wicker, Magda (2012):** Geheimnisschutz nach StGB in der Cloud, Verbraucherzentrale Bundesverband (VZBV), Seminar: Datenschutz ist Verbraucherschutz, 17.-18. September 2012, Kassel.
45. **Wicker, Magda; Glaus, A.; Hajek, M.; Hilber, M.; Klodt, K.; Reintzsch, C.; Riffer, C.; Städtler, S. (2012):** Lizenzierungsbedarf beim Cloud Computing – Welche Rechte zur Nutzung von Software benötigen Anbieter und Nutzer von Cloud Computing?, Arbeitspapier der AG Rechtsrahmen, Kompetenzzentrum Trusted Cloud – AG Rechtsrahmen des Cloud Computing (Hrsg.), 2012.
46. **Wicker, Magda; Kroschwald, Steffen; Behling, T.; Bergner, J.; Borges, G.; Cellarius, M.; Duisberg, A.; Eckhard, J.; Glaus, A.; Hajek, B.; Hartmann, W.; Hilber, M.; Jäger, H.; Klodt, K.; Kramer, R.; Lanndvogt, J.; Lepper, U.; Marnau, N.; Meents, G.; Rüdiger, M.; Sädtler, S.; Schiefer, G.; Schulz, G.; Taeger, J.; Trusch, B.; Ulmer, C.-D.; v. Bülow, T. (2012):** Datenschutzrechtliche Lösungen für Cloud Computing, Rechtspolitisches Thesenpapier der AG Rechtsrahmen, Kompetenzzentrum Trusted Cloud – AG Rechtsrahmen des Cloud Computing (Hrsg.), 2012.
47. **Wicker, Magda; Kroschwald, Steffen (2012):** Veranstaltungsbericht „Jahreskongress Trusted Cloud 2012“, Geheimnisschutz nach StGB in der Cloud, Kommunikation & Recht (K&R) 2012, Heft 12/2012, S. V-VI.

48. **Wicker, Magda (2012):** Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MultiMedia und Recht (MMR), 2012, S. 783-788.
49. **Wicker, Magda (2013):** Ermittlungsmöglichkeiten in der Cloud – Ver-eitelt das Speichern in der Cloud die Zuständigkeit deutscher Ermitt-lungsbehörden?, in: Jürgen Taeger (Hrsg.), IT und Internet – mit Recht gestalten Tagungsband Herbstakademie 2013, Edeweicht 2013, S. 981-1000.
50. **Wicker, Magda (2013):** Durchsuchung in der Cloud – Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermitt-lungsbehörden, MultiMedia und Recht (MMR), 2013, S. 765-769.
51. **Wicker, Magda (2014):** Haftungsbegrenzung des Cloud-Anbieters trotz AGB-Recht? Haftungsfragen in der Cloud, MultiMedia und Recht (MMR) 2014, Heft XI;2014, i.E.
52. **Wicker, Magda (2014):** Rechtskonforme Gestaltung von Cloud-Ser-vices für die öffentliche Verwaltung, Voraussetzung der Cloud-Nutzung durch Behörden, in: Flach, G., Frenzel, C., 9. Rostocker eGovernment-Forum „Sicheres eGovernment: Herausforderung und Notwendigkeit“, Rostock-Warnemünde, 2014, S. 3-10.
53. **Wicker, Magda (2014):** Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzers? Haftungsfragen in der Cloud, MultiMedia und Recht (MMR) 2014, S. 715-719.
54. **Wicker, Magda (2014):** Die Neuregelung des § 100j StPO auch beim Cloud Computing? – Zugriff auf Zugangsdaten zur Cloud nach der neu-en Bestandsdatenauskunft? MultiMedia und Recht (MMR), 2014, S. 298-302.
55. **Wollersheim, Jan; Konstantinidis, Christos; Krcmar, Helmut (2012):** Sicherheitskriterien bei Auswahl von ERP-Systemen. In: ERP-Management, 2012, Vol. 8, Nr. 3, S. 26-28.
56. **Wollersheim, J.; Teufl, S.; Hoberg, P.; Wolf, P.; Krcmar, H. (2012):** Mechanisms to gather customer-feedback – Requirements in the cloud service ecosystem, In: Buxmann, P., Jansen, S., Kude, T., Popp, K.M., Przewloka, M. (Eds.), Proceedings of the European Workshop on Soft-ware Ecosystems 2012, Walldorf, S. 38-45.

-
57. **Wollersheim, Jan; Krcmar, Helmut (2013):** Purchasing processes for cloud services. An exploratory study of process influencing factors. In: 22nd Annual IPSERA Conference, Nantes, France, S. 1285-1295.
 58. **Wollersheim, Jan; Hoberg, Patrick; Krcmar, Helmut (2013):** “Procurement of Cloud Services – Seven Principles to Success.” In: Proceedings of the QUIS13 International Research Symposium on Service Excellence in Management, Karlstad, Sweden, S. 423-431.
 59. **Wollersheim, Jan; Hoberg, Patrick; Krcmar, Helmut (2013):** “How to specify cloud service demand - An approach recognizing planned application.” In: ConLife Academics 2013, Berlin, Germany.
 60. **Wollersheim, Jan; Pfaff, Matthias; Krcmar, Helmut (2014):** Information Need in Cloud Service Procurement – An Exploratory Case Study. In Proceedings of 15th International Conference on Electronic Commerce and Web Technologies (EC-Web), Springer, Heidelberg, Germany, S. 26-33.
 61. **Wollersheim, J.; Krcmar, H. (2014):** Quality analysis approaches for cloud services - Towards a framework along the customer's activity cycle. In: Trusted Cloud Computing. Eds.: Krcmar, H.; Reussner, R.; Rumpe, B. Springer, Heidelberg, Germany, S. 109-124.

Die Autoren

Philipp Alexander Ebel, Universität Kassel, Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Fachgebiet Wirtschaftsinformatik, Kassel, Deutschland, Ph.Ebel@uni-kassel.de

Andreas Eberl, SpaceNet AG, München, Deutschland, AEberl@space.net

Robert Eberlein, SpaceNet AG, München, Deutschland, re@space.net

Fangjian Gao, Universität zu Köln, Juniorprofessur für Wirtschaftsinformatik und Information Systems Quality, Köln, Deutschland, Gao@wiso.uni-koeln.de

Lysann Gebauer, Universität Kassel, Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Fachgebiet Wirtschaftsinformatik, Kassel, Deutschland, Lysann.Gebauer@uni-kassel.de

Michael Marcin Kunz, Universität Kassel, Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Fachgebiet Wirtschaftsinformatik, Kassel, Deutschland, Michael.Kunz@uni-kassel.de

Dr. Franz Glatz, GATE – Garchinger Technologie- und Gründerzentrum GmbH, München, Deutschland, Franz.Glatz@gategarching.com

Patrick Hoberg, fortiss GmbH – An-Institut Technische Universität München, München, Deutschland, Hoberg@fortiss.org

Dr. Silke Jandt, Universität Kassel, Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Projektgruppe Verfassungsverträgliche Technikgestaltung (provet), Kassel, Deutschland, S.Jandt@uni-kassel.de

Anette Keller, GATE – Garchinger Technologie- und Gründerzentrum GmbH, München, Deutschland, Anette.Keller@gategarching.com

Prof. Dr. Helmut Krcmar, Technische Universität München, Lehrstuhl für Wirtschaftsinformatik, München, Deutschland, Krcmar@in.tum.de

Dr. Steffen Kroschwald, Universität Kassel, Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Projektgruppe Verfassungsverträgliche Technikgestaltung (provet), Kassel, Deutschland, Steffen.Kroschwald@uni-kassel.de

Jens Lansing, Universität zu Köln, Juniorprofessur für Wirtschaftsinformatik und Information Systems Quality, Köln, Deutschland,
Lansing@wiso.uni-koeln.de

Prof. Dr. Jan Marco Leimeister, Universität Kassel, Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Fachgebiet Wirtschaftsinformatik, Kassel, Deutschland, Leimeister@uni-kassel.de
und Universität St. Gallen, Institut für Wirtschaftsinformatik (IWI-HSG), St. Gallen, Schweiz, JanMarco.Leimeister@unisg.ch

Andreas Reidt, fortiss GmbH – An-Institut Technische Universität München, München, Deutschland, Reidt@fortiss.org

Prof. Dr. Alexander Roßnagel, Universität Kassel, Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Projektgruppe Verfassungsverträgliche Technikgestaltung (provet), Kassel, Deutschland, A.Rossnagel@uni-kassel.de

Dr. Stephan Schneider, Universität zu Köln, Juniorprofessur für Wirtschaftsinformatik und Information Systems Quality, Köln, Deutschland, Schneider@wiso.uni-koeln.de

Dr. Matthias Söllner, Universität Kassel, Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Fachgebiet Wirtschaftsinformatik, Kassel, Deutschland, Soellner@uni-kassel.de

Prof. Dr. Ali Sunyaev, Universität Kassel, Lehrstuhl für Wirtschaftsinformatik und Systementwicklung, Kassel, Deutschland, Sunyaev@uni-kassel.de

Dr. Magda Wicker, Universität Kassel, Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Projektgruppe Verfassungsverträgliche Technikgestaltung (provet), Kassel, Deutschland, Magda.Wicker@uni-kassel.de

Jan Wollersheim, fortiss GmbH – An-Institut Technische Universität München, München, Deutschland, Wollersheim@fortiss.org