

Inhaltsverzeichnis

Vorwort	ix
1 Einführende Beispiele	1
1.1 Beispiele für unternehmerische Anwendungen in der Cloud	3
1.1.1 Software-Dienst Gliffy	3
1.1.2 Plattformdienst Force.com	4
1.1.3 Infrastrukturdienst AWS	5
1.2 Relevanz des Cloud-Computing	7
1.3 Fragestellungen	9
1.4 Bibliografische Hinweise und Ergänzungen	11
2 Definitionen, Begriffe, Geschäftsmodelle	13
2.1 Historische Entwicklung der letzten Jahrzehnte	13
2.1.1 Verteilte Systeme und Skalierbarkeit	13
2.1.2 Cluster-Computing	15
2.1.3 Grid-Computing	15
2.1.4 Outsourcing	16
2.1.5 Das Application-Service-Provider-Modell	16
2.1.6 Virtualisierung	17
2.1.7 Utility-Computing	19
2.2 Was macht Cloud-Computing aus?	19
2.2.1 Evolution zum Cloud-Computing	19
2.2.2 Die fünf zentralen Charakteristika des Cloud-Computings ..	21
2.2.3 Vergleich zwischen Cluster-, Grid- und Cloud-Computing ..	25
2.2.4 Abgrenzung zum klassischen IT-Outsourcing	26
2.3 Klassifikation von Cloud-Services	27
2.4 Arten von Clouds	30
2.5 Cloud-Services aus Nutzersicht	32
2.5.1 Warum lohnt sich die Cloud aus Nutzersicht?	32
2.5.2 Was ändert sich für den Nutzer durch Cloud?	34
2.6 Geschäftsmodelle für Cloud-Services	35
2.6.1 Ertragsmodelle	36
2.6.2 Service-Modelle	38

2.6.3	Modelle der Bereitstellung	40
2.7	Entwicklung und Umsetzung einer Cloud-Strategie	40
2.7.1	Inhalt, Umfang und Motivation	41
2.7.2	Vorgehen zur Strategieerstellung	44
2.7.3	Umsetzung	45
2.8	Bibliografische Hinweise und Ergänzungen	47
3	Technische Aspekte	49
3.1	Anforderungen	49
3.2	Replikation, Datenkonsistenz, Recovery	55
3.2.1	Replikation zur Steigerung der Verfügbarkeit	55
3.2.2	Klassische ACID-Konsistenzgarantien	58
3.2.3	Synchronisation von Transaktionen	59
3.2.4	Crash-Recovery	62
3.2.5	Daten in verteilten Systemen: das CAP-Theorem	63
3.2.6	Konsequenzen aus dem CAP-Theorem	66
3.3	Sicherung und Wiederherstellung von Daten	68
3.3.1	Grundsätzliches	68
3.3.2	Datensicherungsstrategie	70
3.3.3	Arten der Datensicherung und Speichermedien	71
3.3.4	Datensicherung durch Cloud-Service-Provider	74
3.4	Elastizität und Datenlokalität	75
3.4.1	Grundsätzliches	75
3.4.2	Test und Bewertung einer Cloud-Infrastruktur	77
3.5	IT-Architekturkonzepte für die Cloud	80
3.6	Integration in bestehende Systeme und Migration	84
3.6.1	Problemfelder einer Cloud-Integration	84
3.6.2	Beispielhafte Ausprägungen	90
3.7	Eigenes Cloud-Data-Center – ja oder nein?	91
3.7.1	Lohnt sich der Schritt zum Cloud-Service-Provider?	91
3.7.2	Der Schritt vom Rechenzentrum zum Cloud-Data-Center ..	93
3.7.3	Eigenes Cloud-Data-Center? Nein!	96
3.8	Bibliografische Hinweise und Ergänzungen	97
4	Wirtschaftliche und organisatorische Aspekte	101
4.1	Anforderungen	101
4.2	Anbieterauswahl	104
4.2.1	Lock-in-Effekte	104
4.2.2	Anbieterreputation	107
4.2.3	Vereinbarkeit mit Qualitätsanforderungen	112
4.3	Cloud-spezifische Wirtschaftlichkeitsbetrachtungen	118
4.3.1	Chancen und Risiken eines IT-Fremdbezugs	119
4.3.2	Kostenbetrachtungen zu Pay-per-Use	124
4.3.3	Kostenbetrachtungen zur Elastizität	128

4.4	Der »Chief Cloud Officer (CCO)«	130
4.4.1	Organisatorische Aspekte eines Fremdbezugs	131
4.4.2	Cloud-Controlling	133
4.5	Zusammenfassende Betrachtung der Sourcing-Modelle	136
4.6	Bibliografische Hinweise und Ergänzungen	140
5	Rechtliche Aspekte	143
5.1	Datenschutzrechtliche Anforderungen	143
5.2	Cloud und Telekommunikationsgesetz	150
5.2.1	Telekommunikationsdienst (z. B. E-Mail-Dienst, VoIP)	151
5.2.2	Anders geartete Software-Dienstleistung	155
5.3	Cloud und Abgabenordnung	155
5.3.1	Finanzbuchführung im Inland	155
5.3.2	Finanzbuchführung im Ausland	155
5.3.3	Folgen einer fehlerhaften Buchführung	157
5.4	Cloud und Versicherungsaufsichtsrecht	157
5.5	Cloud und Strafgesetzbuch	160
5.6	Cloud und Betriebsverfassungsgesetz	163
5.7	Vertragsrecht	164
5.7.1	Rechtsnatur	165
5.7.2	Vermietung: urheberrechtlich – vertragsrechtlich	165
5.7.3	Hauptleistungspflichten	166
5.7.4	Nebenleistungspflichten	168
5.8	Zusammenfassung und Handlungsempfehlungen	169
5.9	Bibliografische Hinweise	171
6	Informationssicherheit in der Cloud	175
6.1	Risiken in der Cloud	175
6.1.1	Allgemeine Risiken	176
6.1.2	Cloud-spezifische Risiken	176
6.2	Technische Sicherheitsmaßnahmen	180
6.2.1	Grundbegriffe	181
6.2.2	Sicherheit der Infrastruktur	182
6.2.3	Sicherheit und Schutz der Daten	187
6.3	Vertrauensbildende und organisatorische Maßnahmen	191
6.3.1	Sensibilisierung der Mitarbeiter für das Thema	191
6.3.2	Herstellen einer Vertrauensbeziehung zu einem CSP	192
6.3.3	Verwaltung von kryptografischen Schlüsseln	193
6.3.4	Weitere Sicherheitsmaßnahmen	194
6.3.5	Integration in ein bestehendes Sicherheitskonzept	195
6.3.6	Überprüfung und Einhaltung des Sicherheitskonzepts: Audits und Compliance	196
6.4	Bibliografische Hinweise	197

7	Entscheidungshilfen in Kürze	199
7.1	Vorgehen für ein konkretes Cloud-Sourcing-Vorhaben	199
7.2	Grundsätzliche Entscheidungen	203
7.2.1	Zehn Leitfragen zur Grundsatzentscheidung	203
7.2.2	Entscheidung für eines der drei Servicemodelle	204
7.3	Anbieterauswahl	206
7.3.1	Zehn Leitfragen zur Wahl des Anbieters	206
7.3.2	Anbieterreputation	207
7.4	Checklisten zur rechtlichen Dimension	208
7.4.1	Telekommunikationsgesetz (TKG)	208
7.4.2	Bundesdatenschutzgesetz (BDSG)	208
7.4.3	Strafgesetzbuch (StGB)	211
7.4.4	Abgabenordnung (AO)	212
7.4.5	Versicherungsaufsichtsgesetz (VAG)	212
7.4.6	Betriebsverfassungsgesetz (BetrVG)	213
7.5	Cloud-Sicherheit	213
7.5.1	Drei grundlegende Maßnahmen für Sicherheit in der Cloud	214
7.5.2	Zehn Fragen zur Cloud-Sicherheit	215
8	Ausblick auf weitere Entwicklungen	217
8.1	Verschmelzung von Privat- und Berufsleben	217
8.1.1	Persönliche Clouds	218
8.1.2	Konsequenzen für Unternehmen	220
8.2	Vom Cloud-Flickenteppich zur Eine-für-Alle-Cloud	221
8.2.1	Inter-Cloud-Computing	222
8.2.2	Standardisierung	223
8.2.3	Cloud-Service-Supply-Chains	225
8.3	Erschließung neuer Anwendungsgebiete	226
8.3.1	Supply-Chain-Management	226
8.3.2	eHealth	227
8.3.3	IT-gestützte Dienstleistungen	227
8.3.4	»Computation-Offloading« in die Cloud	228
8.4	Rechtliche Entwicklungen	228
8.5	Alternativen zur Cloud	229
8.6	Bibliografische Hinweise	230
	Literaturverzeichnis	231
	Abkürzungsverzeichnis	239
	Index	241