Förderkreis der
Angewandten
Informatik
an der
Westfälischen
Wilhelms-Universität Münster e.V.

Working Paper No. 3

Database-as-a-Service für kleine und mittlere Unternehmen

Till Haselmann
Gottfried Vossen

25. November 2010

Westfälische
Wilhelms-Universität
Münster

Till Haselmann
Gottfried Vossen

Database-as-a-Service für kleine und mittlere Unternehmen

Ein praxistauglicher Leitfaden für KMU, die „in die Cloud gehen“ möchten

DBIS Group
Institut für Wirtschaftinformatik
Westfälische Wilhelms-Universität Münster
Leonardo-Campus 3
D-48149 Münster

http://dbis-group.uni-muenster.de/

Prof. Dr. Gottfried Vossen, Till Haselmann
Lehrstuhl für Informatik
Institut für Wirtschaftsinformatik
Westfälische Wilhelms-Universität Münster
Leonardo-Campus 3
D-48149 Münster
http://dbis-group.uni-muenster.de/

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

ISSN 1868-0801

Printed in Germany

Vorwort

Der Begriff „Cloud-Computing“ ist derzeit – zumindest innerhalb der IT-Welt – in aller Munde. Nach Ansicht bekannter Branchengrößen stellt das Cloud-Computing einen grundsätzlichen Richtungswechsel für das Angebot und den Einsatz von IT dar – einige sprechen sogar von einer Revolution. Angebote aus der Cloud seien nach Expertenmeinung besonders für kleine und mittlere Unternehmen (KMU) interessant, weil diese überproportional profitieren könnten. Zum jetzigen Zeitpunkt ist allerdings unklar, wie dies von den KMU selbst gesehen wird. Auch ist die Einführung von Cloud-Services in KMU anders anzugehen als für große Unternehmen.

Dieser Leitfaden untersucht die Frage, wie KMU vorgehen sollten, um Cloud-Computing einzuführen und ob es sich überhaupt lohnt. Dabei liegt der Fokus auf dem Bereich Cloud-Datenbanken, im Englischen als Database-as-a-Service bezeichnet. Dieser Themenfokus sollte aber auf keinen Fall abschrecken: Die meisten Ergebnisse dieses Berichts sind nämlich leicht zu verallgemeinern und können ebenso für andere Cloud-Projekte verwendet werden.

Der vorliegende Leitfaden ist ein weiterer Arbeitsbericht, der durch den Förderkreis für Angewandte Informatik an der Westfälischen Wilhelms-Universität Münster finanziert wurde. Der Förderkreis wird von rund 30 Unternehmen aus der Region und der Industrie- und Handelskammer Nord Westfalen getragen. Sein Hauptziel ist die Förderung der praxisorientierten Forschung und Lehre, sowie der schnelle Wissenstransfer. Um dieses sicherzustellen, gelingt es regelmäßig, interessierte Mitgliedsunternehmen zu finden, die sich aktiv am Projekt beteiligen. Großer Dank gilt daher diesen Unternehmen für ihre Beteiligung am Projekt und die Bereitschaft der Mitarbeiter, für Gesprächsrunden, individuelle Interviews und Erhebungen per Fragebogen zur Verfügung zu stehen. Diese Bereitschaft bildet die Basis des Leitfadens.

Besonderer Dank gebührt dem Leiter der Arbeitsgruppe für Datenbanken und Informationssysteme (DBIS Group), Herrn Professor Dr. Gottfried Vossen, und seinem Mitarbeiter, Herrn Till Haselmann, für die außerordentlich engagierte und praxisnahe Umsetzung des Projektes.

Bei der Darstellung der Inhalte wurde versucht, die Waage zu halten zwischen detaillierten Erläuterungen und Praxisrelevanz. Zusätzlich haben wir zahlreiche Maßnahmen ergriffen, um ein schnelles Erfassen der Inhalte zu ermöglichen: Regelmäßige Zusammenfassungen, Einschübe, die „Das Wichtigste in Kürze“ wiedergeben und Fragenkataloge am Ende der Kapitel bieten hoch aggregierte Informationen. Zudem liegt diesem Bericht ein Faltblatt bei, das als schneller Überblick und Gedächtnisstütze dient. Wir wünschen viel Spaß bei der Lektüre.

Martin Kittner
Vorsitzender des Förderkreises
für Angewandte Informatik

Dr. Christoph Asmacher
Industrie- und Handelskammer
Nord Westfalen

Inhaltsverzeichnis

Executive Summary **1**

1 Einleitung **3**

2 Grundlagen des Cloud-Computing **5**
2.1 Was ist Cloud-Computing? 5
2.1.1 Historische Entwicklung und Grundlagen 5
2.1.2 Evolution zum Cloud-Computing 8
2.1.3 Fünf zentrale Charakteristika von Cloud-Computing 10
2.1.4 Servicemodelle: XaaS 14
2.1.5 Arten des Cloud-Betriebs 16
2.2 Abgrenzung zum klassischen IT-Outsourcing 18
2.3 Spezialfall Database-as-a-Service (DaaS) 19
2.3.1 Definition und Abgrenzung 19
2.3.2 Der Cloud-Aspekt von DaaS 21
2.3.3 Mangelnde Elastizität der Daten 23
2.4 Zusammenfassung der Grundlagen 23

3 Grundsatzentscheidung „Cloud oder nicht?“ **25**
3.1 Cloud Computing in vier Dimensionen 25
3.1.1 Wirtschaftliche Dimension 26
3.1.2 Technische Dimension 29
3.1.3 Rechtliche Dimension 31
3.1.4 Organisatorische Dimension 33
3.2 Typische Szenarien für Cloud-Nutzung durch KMU 35
3.2.1 Szenario 1: KMU ↔ Cloud 35
3.2.2 Szenario 2: KMU ↔ Cloud ↔ Endkunde 37
3.3 Entwicklung einer Cloud-Strategie und deren Umsetzung 38
3.4 Zusammenfassung 39

4 Auswahl eines DaaS-Anbieters **43**
4.1 Wirtschaftliche Dimension 44
4.1.1 Reputation des Anbieters 44
4.1.2 Preismodell 45
4.1.3 Lock-in-Effekte über die Daten 46

4.1.4 Lock-in-Effekte über die Prozesse . . . 47
4.2 Technische Dimension . . . 48
4.2.1 Sicherung und Wiederherstellung von Daten . . . 48
4.2.2 Leistungsfähigkeit der Cloud . . . 49
4.2.3 Integration in bestehende Systeme . . . 51
4.3 Rechtliche Dimension . . . 52
4.3.1 Erfüllung der gesetzlichen Anforderungen . . . 52
4.3.2 Ausstiegsszenarien . . . 53
4.3.3 Weitere Aspekte . . . 54
4.3.4 Handlungsempfehlungen zur rechtlichen Dimension . . . 55
4.4 Organisatorische Dimension . . . 55
4.4.1 Vorgehen zur und Dokumentation der Anbieterwahl . . . 55
4.4.2 Support-Leistungen des Anbieters . . . 56
4.4.3 Kommunikation mit dem Anbieter im Problemfall . . . 58
4.5 Zusammenfassung . . . 58

5 Sicherheitaspekte von DaaS-Angeboten 61
5.1 Vorgehen für die Bewertung der Risiken in der Cloud . . . 62
5.1.1 Analyse der eigenen Anforderungen . . . 62
5.1.2 Analyse der Anbieter . . . 64
5.2 Das kleine Einmaleins . . . 65
5.3 Organisatorische Aspekte . . . 66
5.3.1 Sensibilisierung der Mitarbeiter für das Thema . . . 66
5.3.2 Integration in ein bestehendes Sicherheitskonzept . . . 67
5.3.3 Herstellen einer Vertrauensbeziehung zwischen Cloud-Konsument und Cloud-Anbieter . . . 68
5.3.4 Verwaltung von kryptographischen Schlüsseln . . . 68
5.3.5 Einsatz von Service-Level-Agreements (SLAs) . . . 69
5.3.6 Überprüfung und Einhaltung des Sicherheitskonzepts . . . 69
5.3.7 Einbindung des Anbieters . . . 70
5.4 Technische Aspekte . . . 70
5.4.1 Sicherheit der Infrastruktur . . . 70
5.4.2 Sicherheit und Schutz der Daten . . . 73
5.5 Zusammenfassung . . . 76

6 Zusammenfassung 79

Literaturverzeichnis 81

Abkürzungsverzeichnis

AES Advanced Encryption Standard
API Application Programming Interface
ASP Application Service Provider
BDSG Bundesdatenschutzgesetz
BGP Border Gateway Protocol
BSI Bundesamt für Sicherheit in der Informationstechnik
CAPEX Capital Expenditure
CC Cloud-Computing
CDN Content Delivery Network
CDS Cloud Data Service
CERT Computer Emergency Response Team
CIO Chief Information Officer
CISO Chief Information Security Officer
COO Chief Operating Officer
CPU Central Processing Unit
CSIRT Computer Security Incident Response Team
CSV Comma-separated Values
DaaS Database-as-a-Service
DBMS Datenbankmanagementsystem
DBS Datenbanksystem
DNS Domain Name System
DoS Denial-of-Service
DSG Datenschutzgesetz
EC2 Elastic Compute Cloud
EDoS Economic-Denial-of-Sustainability
HP Hewlett-Packard
HTTP Hypertext Transfer Protocol
IaaS Infrastructure-as-a-Service
IEC International Electrotechnical Commission
IPS Intrusion Prevention System
IS Informationssystem
ISMS Informationssicherheits-Managementsystem
ISO International Organization for Standardization
ISO/IEC 27001 IT-Sicherheitsverfahren – ISMS – Anforderungen
ISO/IEC 27002 IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management
ISP Internet Service Provider
IT Informationstechnik
ITIL IT Infrastructure Library
JSON JavaScript Object Notation
KMU kleines oder mittleres Unternehmen
LAN Local Area Network
MAC Message Authentication Code
MPLS Multiprotocol Label Switching
NDA Non-disclosure Agreement
NIST National Institute of Standards and Technology
NoSQL Not only SQL
NRW Nordrhein-Westfalen
OLTP Online Transaction Processing
OPEX Operational Expenditure
PaaS Platform-as-a-Service
PDA Personal Digital Assistant
PDF Portable Document Format
RDBS relationales Datenbanksystem
RDS Relational Database Service
REST Representational State Transfer
RSS Really Simple Syndication
S3 Simple Storage Service
SaaS Software-as-a-Service
SAS 70 Statement on Auditing Standards No. 70
SLA Service-Level-Agreement
SOA Service-oriented Architecture
SPI Software, Plattform und Infrastruktur
SQL Structured Query Language
SSL Secure Socket Layer
SSO Single Sign On
TCO Total Cost of Ownership
TLS Transport Layer Security
URL Uniform Resource Locator
VM virtuelle Maschine
VPN Virtual Private Network
WAN Wide Area Network
XaaS Anything-as-a-Service
XML Extensible Markup Language

Executive Summary

Dieser Leitfaden richtet sich an Entscheider und IT-Leiter in kleinen und mittleren Unternehmen (KMU), die über den Einsatz von Database-as-a-Service-Angeboten bzw. anderen Cloud-Diensten im eigenen Unternehmen nachdenken. Das Dokument gibt einen ersten Eindruck von den Einsatzmöglichkeiten von Cloud-Computing. Insbesondere werden die zu erwartenden Maßnahmen beschrieben, die mit der Einführung von Cloud-Computing im Unternehmen einhergehen. Dabei werden – soweit möglich – konkrete Schritte oder Maßnahmen empfohlen. Wegen der hohen Diversität der Cloud-Dienste kann jedoch keine allgemeingültige Empfehlung für oder gegen die Cloud gegeben werden.

Cloud-Computing ist keine technische Revolution, sondern eine neuartige Kombination aus vielen bekannten und einigen neuen Ansätzen. Charakterisiert wird es durch fünf Merkmale:

1. Gemeinsame Nutzung physischer Ressourcen durch mehrere Anwender
2. Unverzügliche Anpassbarkeit an den dynamischen Ressourcenbedarf
3. Selbstbedienung nach Bedarf
4. Umfassender Netzwerkzugriff
5. Messung der Servicenutzung

Die Definition des Begriffs anhand dieser fünf Merkmale hat sich in der Fachwelt etabliert. Eine direkte Konsequenz aus diesen Merkmalen ist die Anwendung von Virtualisierungstechnologien, so dass manchmal auch dieser Aspekt genannt wird. In Folge arbeitet der Cloud-Anwender nur noch mit virtuellen Ressourcen, die vom Anbieter auf physische Ressourcen abgebildet werden.

Servicemodelle

Im Bereich des Cloud-Computing unterscheidet man typischerweise drei verschiedene Servicemodelle: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) sowie Software-as-a-Service (SaaS). Database-as-a-Service (DaaS), der Fokus dieses Leitfadens, bezeichnet eine Klasse von Diensten, die Funktionalitäten eines Datenbanksystems in der Cloud bereitstellen. DaaS kann dabei basierend auf einem der drei Servicemodelle angeboten werden. Die meisten Aspekte aus diesem Leitfaden lassen sich direkt auf andere Arten von Diensten übertragen und sind nicht spezifisch für DaaS. Es gibt zudem vier verschiedene Arten des Cloud-Betriebs: die öffentliche und die nichtöffentliche Cloud sowie die Community-Cloud und die hybride Cloud. Trotz der vielen neuen Begriffe ist Cloud-Computing nicht allzu verschieden vom klassischen IT-Outsourcing. Allerdings verschiebt sich die Gewichtung der zu beachtenden Aspekte.

Dimensionen

Die Betrachtung von Cloud-Computing geschieht in vier Dimensionen: wirtschaftlich, technisch, rechtlich und organisatorisch. Wirtschaftlich kann Cloud-Computing je nach Anwendungsfall sehr attraktiv sein – muss es aber auch nicht. Insbesondere für maßgeschneiderte Cloud-Dienste, die von der „Stangenware“ abweichen, fordern die Anbieter hohe Gebühren, so dass die Vorteile schnell schwinden. Technisch birgt Cloud-Computing für das Anwenderunternehmen nur wenig wirklich neue Herausforderungen, fordert aber oft eine Anpassung

bestehender Systeme. Organisatorisch erfordert es stringente Abläufe, die gegebenenfalls im Unternehmen erst noch einzuführen sind. Das Hauptproblem ist jedoch die rechtliche Unsicherheit, die der Tatsache geschuldet ist, dass die meisten Aspekte des Cloud-Computing juristisch noch ungeklärt sind. In jedem Fall muss auf Managementebene eine Cloud-Strategie entwickelt werden. Sie ist eine essentielle Voraussetzung für jedes Cloud-Projekt.

Bei der Auswahl des Anbieters müssen alle vier Dimensionen des Cloud-Computing betrachtet werden. Besondere Aufmerksamkeit sollte den erwarteten Lock-in-Effekten, der Integration in bestehende Systeme und der Erfüllung rechtlicher Rahmenbedingungen gewidmet werden. Auch die Support-Leistungen und die Kommunikation mit dem Anbieter sind wichtige Aspekte. Auf jeden Fall ist ein strukturiertes Vorgehen zur Anbieterauswahl inklusive Dokumentation gefordert. Darüber hinaus muss eine regelmäßige Überprüfung des Marktes auf Änderungen statt finden, um neue, bessere Angebote zu identifizieren.

Sicherheit

Die Sicherheit in der Cloud ist für alle Unternehmen ein zentrales Thema und muss explizit in der Cloud-Strategie behandelt werden. Einige einfache Maßnahmen verhelfen bereits zu einer soliden Grundsicherheit. Selbstverständlich müssen die eigenen Anforderungen an die Sicherheit im Vorfeld genau geklärt werden. Aus technischer Sicht müssen sowohl die Infrastruktur als auch die Daten geschützt werden. Ansätze für ersteres sind bekannt, der Aspekt der Datensicherheit stellt oft eine größere Hürde dar, da viele Anbieter nur ein durchschnittliches, aber kein hohes Schutzniveau erbringen. Trotz ungeklärter technischer Fragestellungen überwiegen die organisatorischen Probleme. Unter anderem müssen die Mitarbeiter sensibilisiert und geschult sowie bestehende und neue Sicherheitskonzepte integriert werden. Insgesamt ist die Sicherheit von Cloud-Diensten nicht notwendigerweise niedriger als von Lösungen im eigenen Haus.

Beim Cloud-Computing verhält es sich nicht anders als bei anderen Fragestellungen der IT: der Einsatz kann sehr sinnvoll sein, aber dies ist abhängig vom konkreten Szenario. Auch ein sicherer und zuverlässiger Betrieb ist möglich. Je höher allerdings die Anforderungen an den Dienstleister werden, desto unattraktiver wird eine Cloud-Lösung. Als Faustregel lässt sich daher festhalten, dass Cloud-Computing vor allem für standardisierte Produkte attraktiv ist. Trotzdem sollte sich jedes Unternehmen mit dem Thema auseinander setzen und eine individuelle Cloud-Strategie erarbeiten – selbst wenn das Ergebnis die Festlegung ist, dass Cloud-Computing vermieden wird.

1 Einleitung

Die Begriffe „Cloud-Computing“ und „die Cloud“ sind derzeit in aller Munde. Einige bezeichnen damit tatsächliche Computing-Dienste, also den Bezug reiner Rechenleistung z. B. in Form von virtuellen Maschinen über das Internet. Amazons Dienst Simple Storage Service (S3) ist in dieser Disziplin ein Pionier, viele andere Hosting-Anbieter haben inzwischen ähnliches im Programm. Für andere umfasst der Begriff Cloud-Computing jedoch jegliche Webapplikation, die nicht auf eigener Hardware läuft. Somit ist alles, was heutzutage unter die Stichworte „Web 2.0“ bzw. „Dynamic Web“ fällt, Cloud-Computing. Eine umgangssprachliche Definition zeigt anschaulich die breite Spannweite des Begriffs:

> “*Cloud computing* is using the internet to access someone else’s software running on someone else’s hardware in someone else’s data center while paying only for what you use.” – *Lewis Cunningham*[1]

Ein erstes Ziel dieses Leitfadens ist deshalb die Begriffsklärung und die Abgrenzung des Konzepts. Zusätzlich liegt der Fokus in diesem Leitfaden auf Database-as-a-Service (DaaS), also der Klasse von Cloud-Datenbankdiensten. Nichtsdestotrotz sind viele der behandelten Aspekte allgemeingültig für Cloud-Computing an sich. Dieser Leitfaden behandelt die Grundlagen in Kapitel 2.

Nachdem ein Grundverständnis der Begrifflichkeiten geschaffen wurde, können die Chancen und Risiken in den Vordergrund treten. Cloud-Computing wird von allen Anbietern als Universallösung zur Kosteneinsparung bei gleichzeitigem Übertragen des Risikos beworben. Das dies nicht so sein muss, wird schnell klar, wenn die Angebote einem kritischen Blick unterzogen werden. Auch ein Blick auf die rechtlichen Anforderungen ist ernüchternd. Kapitel 3 widmet sich der Grundsatzfrage, ob ein Unternehmen den Schritt in die Cloud wagen soll oder nicht, und thematisiert unter anderem diese Aspekte.

Hat sich ein Unternehmen für eine Cloud-Lösung entschieden, so ist die Frage, welcher Anbieter und welches Angebot am geeignetsten ist. Dabei ist die Auswahl des richtigen Anbieters alles andere als einfach. Kapitel 4 gibt einige wichtige Handlungsempfehlungen für die bestmögliche Wahl.

Schließlich spielt die Sicherheit für die meisten Cloud-Anwender eine entscheidende Rolle. Viele Unternehmen trauen sich nicht, eine Cloud-Lösung einzusetzen, weil sie die Befürchtung haben, ihre Daten könnten nicht mehr sicher sein. Welche Ängste in dieser Hinsicht berechtigt sind und welche zerstreut werden können, zeigt das Kapitel 5. Die Struktur dieses Berichts wird in der Abbildung 1.1 visualisiert. Die Kreise bezeichnen dabei die entsprechenden Kapitel im Bericht.

[1] `http://it.toolbox.com/blogs/oracle-guide/cloud-computing-defined-28433`

Abbildung 1.1: Struktur des Berichts mit Kapitelnummern.

Dieser Leitfaden richtet sich an Entscheider und IT-Leiter in kleinen und mittleren Unternehmen (KMU), die über den Einsatz von Database-as-a-Service-Angeboten bzw. anderen Cloud-Diensten im eigenen Unternehmen nachdenken. Während des gesamten Leitfadens wird daher – wo nötig – auf Database-as-a-Service fokussiert. Außerdem sind die Empfehlungen vor dem Hintergrund der Situation von KMU entwickelt worden. Viele Aussagen sind jedoch auch auf beliebige Cloud-Dienste oder größere Unternehmen verallgemeinerbar. Alle Empfehlungen zu rechtlichen Fragestellungen sind nur als informative Hinweise zu sehen. Die Autoren können keine Rechtsberatung bieten und weisen ausdrücklich darauf hin, dass alle problematischen rechtlichen Fragen mit ordentlichem Rechtsbeistand zu klären sind.

Wenn bereits ein gutes Verständnis von Cloud-Computing vorhanden ist oder gar die Entscheidung für den Schritt in die Cloud schon getroffen wurde, so kann direkt im Kapitel 3 bzw. Kapitel 4 eingestiegen werden. Ansonsten empfiehlt sich die Lektüre des Leitfadens von Anfang an. Die wichtigsten Punkte der Kapitel 3, 4 und 5 werden jeweils am Ende des Kapitels in Form von zehn Leitfragen aufbereitet dargestellt.

> **Tipp:**
> Wenn Sie diesen Bericht als PDF am Bildschirm lesen, so können Sie oft auf URLs, Abkürzungen oder Verweise klicken, um direkt zur entsprechenden Stelle zu springen. Probieren Sie es doch einfach direkt bei „URL" und „PDF" aus.

2 Grundlagen des Cloud-Computing

In diesem Abschnitt wird ein kurzer Überblick über den Themenkomplex „Cloud-Computing“ gegeben, um eine Grundlage für die späteren Kapitel zu schaffen. Dazu werden zuerst die Grundlagen des Cloud-Computings behandelt einschließlich eines kurzen historischen Abrisses der Entwicklung bis dato. Im Anschluss erfolgt eine Abgrenzung zum klassischen IT-Outsourcing. Entsprechend dem Thema dieses Leitfadens wird dann auf den Spezialfall Database-as-a-Service (DaaS) fokussiert.

Das Wichtigste in Kürze

- Cloud-Computing ist keine technische Revolution, aber eine neue Kombination aus Bekanntem und Neuem.
- Es gibt drei Servicemodelle: IaaS, PaaS, SaaS.
- DaaS bezeichnet eine Klasse von Cloud-Diensten, die Funktionalitäten eines DBS bereitstellen.
- Es gibt vier Arten des Cloud-Betriebs: die öffentliche und nichtöffentliche Cloud, die Community-Cloud sowie die hybride Cloud.
- Cloud-Computing ist ähnlich dem klassischen IT-Outsourcing, verschiebt aber die Gewichtung der problematischen Aspekte.

2.1 Was ist Cloud-Computing?

Der Begriff „Cloud-Computing“ ist derzeit in aller Munde und wird als Symbol für eine bahnbrechende Neuerung verwendet. Bei vielen als revolutionär beworbenen Merkmalen des Cloud-Computings handelt es sich aber eigentlich um alten Wein in neuen Schläuchen. Um die tatsächlich neuartigen Facetten unterscheiden zu können, beginnt dieses Kapitel daher mit einem kurzen Überblick über die historischen Vorläufer des Cloud-Computings. Dabei werden relevante Konzepte dargestellt, die sich heute in leicht abgewandelter oder sogar identischer Form im Rahmen des Cloud-Computings wieder finden.

Im Anschluss wird eine generelle Definition des Begriffs gegeben und die relevanten Konzepte und Begrifflichkeiten des Themenfelds erklärt. Darauf aufbauend werden die für kleine und mittlere Unternehmen (KMU) relevanten Aspekte des Cloud-Computings anhand von vier Dimensionen vorgestellt, die eine strukturierte Betrachtung des komplexen Felds ermöglichen.

2.1.1 Historische Entwicklung und Grundlagen

Bereits früh in den 1960er Jahren kamen erste Überlegungen auf, dass große Berechnungsprobleme effizienter lösbar sein könnten, wenn man sie in viele kleine Teile zerlegt und getrennt berechnet. Dies führte zu der Idee, das Problem nicht mit einem einzigen immer größeren Supercomputer, sondern mit vielen kleinen „zusammengeschalten“ Computern zu lösen. Einen

solchen Verbund von unabhängigen Computern, der nach außen hin als einzelnes, kohärentes System erscheint, nennt man *verteiltes System*. Die einzelnen Teil-Systeme nennt man *Knoten*, engl. *Node*. Es gibt verschiedene Klassen verteilter Systeme, von denen im Folgenden der Cluster und das Grid erläutert werden. Vorher gehen wir jedoch auf ein gemeinsames, fundamentales Konzept aller verteilten Systemen ein.

Skalierbarkeit

Die *Skalierbarkeit* eines Systems beschreibt dessen Laufzeitverhalten bei einer Änderung verschiedener Input- oder Problemgrößen. Die Skalierbarkeit kann in drei Dimensionen gemessen werden [21]. Für das heutige Cloud-Computing sind besonders die ersten beiden Dimensionen relevant.

1. Das System kann skalierbar sein in Hinblick auf seine *Größe*. In diesem Fall können dem System einfach weitere Ressourcen (oder Benutzer) hinzugefügt werden, ohne dass die Leistung signifikant einbricht.

2. Das System kann skalierbar sein in Hinblick auf die *geografische Verteilung* der Ressourcen (oder Benutzer). In diesem Fall können die einzelnen Ressourcen weit verteilt auseinander liegen, ohne dass die Leistung des Systems stark beeinträchtigt wird.

3. Das System kann skalierbar sein in Hinblick auf seine *Verwaltung*. Solch ein administrativ skalierbares System erstreckt sich über viele unabhängige Organisationen, ohne dass die Komplexität der Verwaltung überproportional zunimmt.

Im Fall der Größenskalierung unterscheidet man außerdem die *vertikale Skalierbarkeit* und die *horizontale Skalierbarkeit* (vgl. Abbildung 2.1). Im ersteren Fall wird die Anzahl der Ressourcen pro Knoten variiert; man verwendet also einen „stärkeren Arbeiter“. Dieses Skalieren bezeichnet man daher auch als „scale up“. Ein Beispiel für vertikales Skalieren ist, wenn ein Arbeitsplatz-PC durch eine leistungsfähige Workstation ersetzt wird. Im zweiten Fall, der horizontalen Skalierung, erweitert man das System, indem mehr Knoten hinzugefügt werden. Die Arbeit wird also „auf mehr Schultern“ verteilt. Daher bezeichnet man dieses Vorgehen als „scale out“. Ein Beispiel hierfür ist das zusätzliche Bereitstellen weiterer Berechnungsknoten in einem Grid. Generell spricht man von einem skalierbaren System, wenn es proportional von horizontaler oder vertikaler Skalierung profitiert. In anderen Worten: Wenn die Ressourcen eines Systems um einen Faktor α vergrößert werden, so sollte sich die Verarbeitungszeit bei konstanter Problemgröße um etwa den Faktor α verringern.

Cluster-Computing

Eine der ersten Arten von verteilten Systemen war das *Cluster*. In den 1960er Jahren verband man zahlreiche identische Knoten über ein Hochgeschwindigkeitsnetzwerk. In vielerlei Hinsicht erschien der Zusammenschluss als ein kohärentes System und ermöglichte so die einfache Ausführung hochverteilter Berechnungen. Durch die große Anzahl an Knoten wurde eine bis dato unbekannte Verfügbarkeit und Leistungsfähigkeit erreicht, die im Vergleich zu einer Lösung

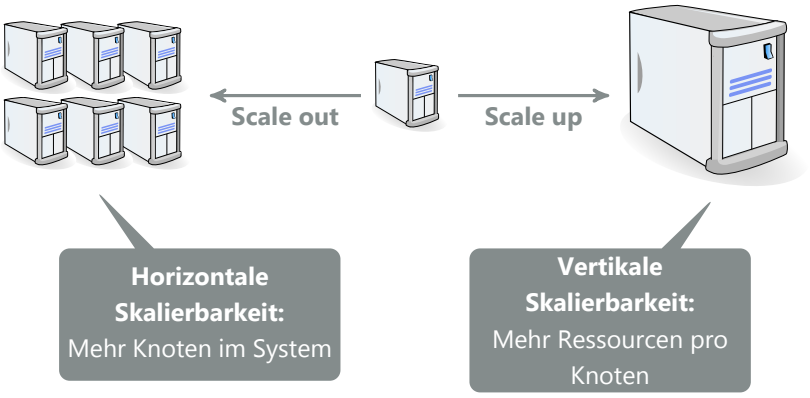

Abbildung 2.1: Vertikale und horizontale Skalierung eines Systems.

aus einem einzelnen Großrechner auch noch deutlich günstiger war. Typische Anwendungen fanden sich bei großen, stark verbundenen Berechnungen, besonders in der Wissenschaft. Auch heute werden die meisten Supercomputer als Cluster konzipiert.

Grid-Computing

Eine Verallgemeinerung des Cluster wird durch das *Grid-Computing* realisiert. Statt der Homogenität eines Cluster weist das Grid einen hohen Grad an Heterogenität auf. So können sich die Knoten sowohl in Hardware und Software als auch in der Art der Anbindung an das Grid und in diversen weiteren Aspekten, wie z. B. Sicherheitsrichtlinien, unterscheiden. Hinzu kommt, dass Knoten sich zu einem beliebigen Zeitpunkt in das Grid ein- oder aus dem Grid ausklinken können. Ein Grid wird häufig durch die Ausnutzung der untätigen CPUs in vielen Rechnern gebildet (sogenanntes *CPU-Scavenging*). Es eignet sich besonders für aufwändige Berechnungen, bei denen nicht viele Daten transportiert werden müssen und deren Teilberechnungen weitgehend unabhängig ausgeführt werden können. Bekannte Vertreter von Grids sind Projekt wie SETI@home[1] oder Folding@home[2].

Utility-Computing

Zeitgleich zu den Ideen des verteilten Rechnens kam auch das Konzept des *Utility-Computings* auf. Hinter diesem Namen verbirgt sich die technologische Vision, Rechenleistung „wie Strom aus der Steckdose“ zu beziehen und nur nach Verbrauch zu bezahlen. Die Vision wurde von John McCarthy geprägt, der in einem Vortrag auf dem MIT Centennial 1961 vorhersagte, dass Rechenleistung zu einem Teil der öffentlichen Versorgung werden könnte, wie auch der Telefonanschluss oder das Stromnetz:

> “If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone

[1] `http://setiathome.berkeley.edu/`
[2] `http://folding.stanford.edu/`

> system is a public utility … The computer utility could become the basis of a new and important industry." [40]

Tatsächlich gab es auch Ansätze, diese Vision umzusetzen. Im Betriebssystem MULTICS wurden die Ideen realisiert, allerdings ohne kommerziellen Erfolg. Das lag in der Rückschau hauptsächlich daran, dass weder ein allgemeiner Zugang zum Internet, noch ausreichend günstige Hardware existierte. Mit dem Aufkommen von Cloud-Computing und „On-Demand"-Applikationen in den 1990er Jahren, wurde allerdings auch diese Vision wieder aufgegriffen und in das Cloud-Computing-Konzept integriert.

Das Application-Service-Provider-Modell

Die Vorteile eines Outsourcing von Software-Anwendungen waren schon früh bekannt.[3] Als erster Versuch, die Vorteile zu realisieren, wurde das Modell des Application Service Provider (ASP) eingeführt. Ein ASP bietet einem anderen Unternehmen üblicherweise eine einzelne Anwendung „on-demand", also „bei Bedarf", per Terminal-Server-Zugang an. Die Anwendung läuft auf der Hardware und im Rechenzentrum des Betreibers. Dieser übernimmt auch sämtliche Wartungs- und Entwicklungsaufgaben. Klar ist, dass bei einer richtigen Umsetzung die Wartungskosten aufseiten des Anwenderunternehmens entfallen. Außerdem werden die einmaligen Zahlungen, wie die Lizenzgebühr für die Software, durch den Provider in eine periodische Nutzungsgebühr umgewandelt. Trotz der theoretischen Vorzüge schlug das Konzept fehl, weil die Anbieter die notwendigen Skaleneffekte (noch) nicht erreichen konnten. Dies lag vor allem daran, dass noch zu viel dedizierte Infrastruktur pro Kunde eingesetzt wurde und zu wenig gemeinsame Nutzung der physischen Ressourcen vorlag. Zudem war die Netzwerkbandbreite in vielen Fällen noch zu knapp, was eine weitere Verbreitung verhinderte. Insgesamt konnten beide Seiten nicht die erhofften monetären Einsparungen erzielen, so dass das ASP-Konzept in seiner ursprünglichen Form als gescheitert angesehen werden muss. Nichtsdestotrotz sind die Ideen ein direkter Vorläufer des Cloud-Computings, welches nun erläutert werden soll.

2.1.2 Evolution zum Cloud-Computing

Der Begriff *Cloud-Computing* beschreibt ein Feld, das sich derzeit noch im Wandel befindet. Viele bekannte Technologien und Vorgehensweisen aus dem IT-Bereich werden in ein neues Gesamtkonzept zusammengeführt. Dabei ist eine zentrale Stoßrichtung, die Applikationen und Informationen von der zugrunde liegenden physischen Infrastruktur und der Art, sie dem Service-Nutzer bereitzustellen, zu trennen. Eine direkte Konsequenz aus dieser Trennung ist, dass die verschiedenen IT-Ressourcen, wie Speicherkapazität und Rechenleistung, dynamischer als bisher ausgenutzt werden können. Zudem spielen Unternehmensgrenzen, zumindest aus technischer Sicht, nur noch eine untergeordnete Rolle. Im Normalfall – wenn kein eigenes Cloud-Rechenzentrum aufgebaut werden soll – ist Cloud-Computing auch gleichbedeutend mit dem Auslagern der Funktionalität zum Dienstanbieter, eine erweiterte Spielart des klassischen IT-Outsourcing.

[3] Die Vor- und Nachteile werden in Abschnitt 3.1 genauer erläutert.

Als allgemein akzeptierte und inzwischen als stabil zu betrachtende[4] Definition des Begriffs Cloud-Computing kann die des amerikanischen National Institute of Standards and Technology (NIST) herangezogen werden [20]. Dieses definiert Cloud-Computing als Modell, das den komfortablen Zugriff nach Bedarf und über ein Netzwerk auf einen Vorrat gemeinsam genutzter Ressourcen (z. B. Speicherplatz, Rechenleistung, Applikationen) erlaubt. Die Menge der bereitgestellten Ressourcen muss sich jederzeit unverzüglich in Selbstbedienung an den tatsächlichen Bedarf anpassen lassen. Der Benutzer erwartet dabei eine ständige Verfügbarkeit der Ressourcen.

Ähnlich sehen es auch Vaquero u. a. [34], die eine Übersichtsstudie über die verschiedenen Definitionen von Cloud-Computing durchgeführt haben. In ihrem Artikel kondensieren sie die Gemeinsamkeiten von über 20 verschieden Definitionen des Begriffs. In der Essenz besagt die Definition, dass Clouds ein großer Vorrat einfach zu benutzender und leicht zugreifbarer, virtualisierter Ressourcen (z. B. Hardware, Entwicklungsumgebungen oder Dienste) sind. Diese Ressourcen können dynamisch an den sich ändernden Bedarf angepasst werden („skalieren“), so dass die Ressourcen optimal ausgenutzt werden. Die Abrechnung erfolgt üblicherweise nach Nutzung („Pay-per-Use“) unter Beachtung vorher vereinbarter Service-Level-Agreements (SLAs).

Beide Definitionen enthalten im Wesentlichen dieselben Charakteristika, wobei sie teilweise unterschiedlich benannt werden. So sprechen Vaquero u. a. explizit von Virtualisierung, während das NIST dies durch den „Vorrat von gemeinsam genutzten Ressourcen“ nur indirekt fordert. Nichtsdestotrotz hat sich die Definition des NIST etabliert. Sie impliziert fünf zentrale Charakteristika von Cloud-Computing-Angeboten, die im Folgenden einzeln erläutert werden. Darüber hinaus grenzt das NIST drei Servicemodelle sowie vier Nutzungsmodelle für die Cloud ab. Auch diese werden weiter unten einzeln vorgestellt.

Zuerst definieren wir jedoch auf Basis der Definition des NIST für den Kontext dieses Leitfadens den Begriff des Cloud-Service:

> Ein *Cloud-Service* ist die service-orientierte Bereitstellung von virtuellen IT-Ressourcen, d. h. virtualisierter Hard- oder Software, durch einen Cloud-Anbieter unter Gewährleistung der fünf Cloud-Computing-Charakteristika:
>
> 1. Gemeinsame Nutzung physischer Ressourcen
> 2. Unverzügliche Anpassbarkeit an den Ressourcenbedarf
> 3. Selbstbedienung nach Bedarf
> 4. Umfassender Netzwerkzugriff
> 5. Messung der Servicenutzung

Abbildung 2.2 zeigt diese Merkmale in der Übersicht. Aus der in der Definition enthaltenen Serviceorientierung ergeben sich einige grundlegende Merkmale (vgl. [9]). Jeder Service ist somit unter anderem durch einen Servicevertrag, also eine Schnittstellenbeschreibung, nach außen spezifiziert und kann lose mit anderen Services gekoppelt werden. Die jeweiligen Implementierungsdetails und die für den Betrieb verwendete Hard- und Software bleiben gemäß dem Abstraktionsprinzip weitgehend verborgen, was die Services modular macht. Cloud-Services sind darüber hinaus zustandslos (engl. stateless) [20].

[4] Die aktuelle Version 15 der Arbeitsdefinition wurde seit Oktober 2009 nicht mehr geändert.

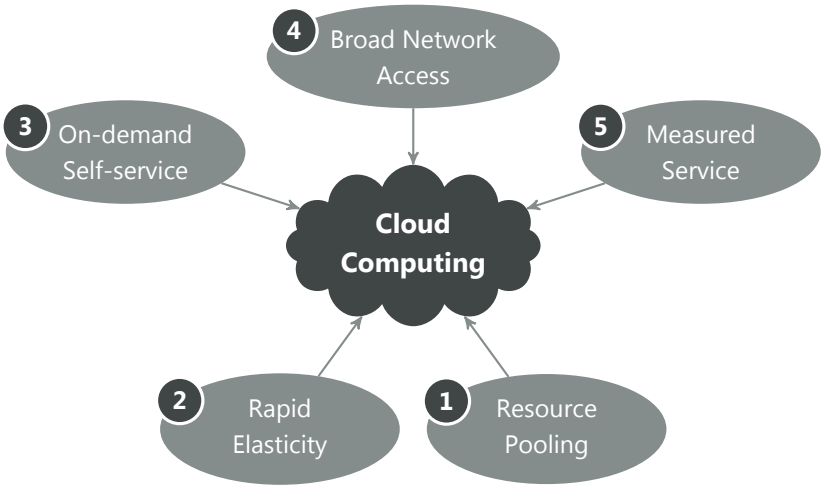

Abbildung 2.2: Die fünf Charakteristika des Cloud-Computings.

2.1.3 Fünf zentrale Charakteristika von Cloud-Computing

Um ein genaueres Verständnis dafür zu erhalten, was einen Cloud-Service auszeichnet, werden im Folgenden die oben eingeführten fünf charakterisierenden Eigenschaften genauer erläutert. Die Eigenschaften sind in der Abbildung 2.2 dargestellt und werden der Reihe nach behandelt.

Resource-Pooling – Gemeinsame Nutzung physischer Ressourcen

Das Konzept des *Resource-Pooling* beschreibt das Zusammenfassen von *physischen* Ressourcen zu einem gemeinsamen Vorrat, der dann je nach Bedarf auf die verschiedenen Dienstnutzer aufgeteilt wird. Die Dienstnutzer können dabei nur *logische* Ressourcen anfordern, welche die Cloud-Software des Anbieters je nach Situation auf verschiedene physische Ressourcen aus dem Vorrat abbildet. Beispiele für Ressourcen sind Rechenleistung, Speicherkapazität, Netzwerkbandbreite, virtuelle Maschinen oder Dienstinstanzen.

Virtualisierung

Das Konzept erfordert folglich zwingend die Trennung von logischen, d. h. virtuellen, und physischen Ressourcen. Auf Hardware-Ebene wird dies durch diverse Methoden der Virtualisierung realisiert. Einige Arten der Virtualisierung sind transparent, während andere spezielle Unterstützung durch die Hard- und Software erfordern. Für einen Überblick über die eingesetzten Technologien siehe [39]. Obschon der Anbieter zuweilen erheblichen Aufwand für eine effiziente Virtualisierung zu betreiben hat, ist die Virtualisierung für alle Cloud-Anbieter unverzichtbar, da nur durch diese Technologien die Hardware in den Rechenzentren so ausgelastet werden kann, dass für die Anbieter ausreichend große Skaleneffekte entstehen. Typischerweise können die Server in einem gut virtualisierten Rechenzentrum mit 70–80%iger Auslastung laufen, anstatt wie in traditionellen Rechenzentren oft nur zu 5–10% ausgelastet zu sein [26]. Dadurch steigt die Rentabilität der Geräte, es sinken die gesamten Hardware-Investitionen und auch die Kosten für Strom und Kühlung.

Während Virtualisierung sich mit physischen Ressourcen befasst, kommt im Bereich der Da-

tenhaltung ein ähnliches Konzept zum Einsatz. Hier wird von physischen Datentöpfen mit ihren Schemata abstrahiert und stattdessen auf logischen Einheiten gearbeitet. Für relationale Datenbanksysteme kann das beispielsweise bedeuten, dass physische Tabellen zwischen mehreren Kunden geteilt werden. Jeder Kunde – in diesem Kontext als *Mandant* bezeichnet – arbeitet dann mit einer logischen Version der Tabelle, in der scheinbar nur seine eigenen Daten vorhanden sind. Abstraktionen wie diese werden im Datenbankbereich unter dem Stichwort *Mandantenfähigkeit* (engl. *Multi-tenancy*) zusammengefasst.

Mandantenfähigkeit

Der Kern der Mandantenfähigkeit ist, dass nur eine einzige Software-Basis für alle Kunden eingesetzt wird, und die Kunden nur durch die Programmlogik separiert werden. So erscheint es dem Dienstnutzer, als stünde für ihn eine eigene, dedizierte Instanz des Systems bereit. Intern wird die Trennung jedoch normalerweise wieder aufgehoben, so dass Daten verschiedener Kunden „nebeneinander“ auf der Festplatte landen können. Daher ist die konkrete Implementierung der Mandantenfähigkeit für eine Sicherheitsanalyse durchaus relevant, zumal noch keine optimale Lösung für die technische Realisierung gefunden ist. Für Anbieter, insbesondere Software-as-a-Service-Anbieter, ist die Mandantenfähigkeit jedoch unverzichtbar, da nur dadurch die entsprechenden Skaleneffekte erzielt werden können.

Unabhängig davon, ob die Abstraktion auf Hardware- oder Software-Ebene erfolgt, hat der Dienstnutzer in beiden Fällen kein Wissen und keine Kontrolle darüber, wie die zugrunde liegenden physischen Ressourcen beschaffen sind oder wo sie sich befinden. Unter Umständen stellt der Cloud-Anbieter jedoch Möglichkeiten bereit, auf höherem Abstraktionsniveau auf die Beschaffenheit der physischen Ressourcen Einfluss zu nehmen. Beispielsweise bieten inzwischen viele Anbieter eine Einschränkung nach geografischer Region (z. B. „Europa“) oder nach Qualitätsstufen (z. B. „Paket XXL“) an.

Rapid Elasticity – Unverzügliche Anpassbarkeit an den Ressourcenbedarf

Cloud-Systeme können sehr dynamisch auf sich ändernde Last reagieren. Sie ermöglichen es üblicherweise, das Ressourcenangebot unverzüglich (oder zumindest mit sehr geringer Vorlaufzeit) nach oben oder unten anzupassen. Dabei kann der Dienstnutzer die Ressourcen aus einem scheinbar unerschöpflichen Vorrat beziehen. Dieses Konzept bezeichnet man auf Englisch als *Rapid Elasticity*.[5] Häufig muss der Dienstnutzer selbst aktiv werden und die bereitgestellte Ressourcenmenge, für die er ja auch zahlen muss, händisch anpassen. Für einige Diensttypen kann jedoch auch eine automatische Anpassung konfiguriert werden. In diesem Fall erkennt das Cloud-System automatisch, dass mehr oder weniger Ressourcen benötigt werden und passt die Zahl der aktiven Ressourcen an. Obwohl beide Arten der Skalierung denkbar sind, kommt im Bereich des Cloud-Computing eher die vertikale Skalierung (scale out) zur Anwendung. Profitieren tun die Cloud-Nutzer natürlich nur dann von dieser dynamischen Anpassung, wenn die jeweiligen Anwendungen auch tatsächlich skalierbar sind.

[5] Das Konzept der „Elasticity“ im Cloud-Kontext darf nicht verwechselt werden mit der Elastizität im wirtschaftswissenschaftlichen Sinne, z. B. der Preiselastizität der Nachfrage. In diesem Zusammenhang ist mit „Elastizität“ gemeint, dass sich das Ressourcenangebot „elastisch“ verhält, also nicht starr ist, sondern sich dem Bedarf recht dynamisch anpassen kann.

On-demand Self-Service – Selbstbedienung nach Bedarf

Eine wichtige Voraussetzung für die unverzügliche dynamische Anpassung der Ressourcen ist die Möglichkeit für den Kunden, die benötigte Menge jederzeit in Eigeninitiative und ohne Einbeziehung von Mitarbeitern des Anbieters ändern zu können. Die Services funktionieren dabei weitgehend autonom und benötigen keine großartige Konfiguration durch den Anbieter vor oder während des Betriebs. Sie sind mehr oder weniger selbstverwaltend und -optimierend (im Sinne des Autonomic Computing [15]). Dieser Aspekt ist sehr wichtig, denn nur durch eine weitgehende Automatisierung auf Anbieterseite kann dieses Selbstbedienungsmodell überhaupt funktionieren. Außerdem kann der Cloud-Anbieter auch nur mithilfe dieses Modells und dem verbundenen Verzicht auf Personal attraktive Preise realisieren. Art, Umfang und Qualität dieser Automatisierung sind, zumindest zurzeit noch, ein wichtiges Alleinstellungsmerkmal für einen Cloud-Anbieter.

Broad Network-Access – Umfassender Netzwerkzugriff

In der Cloud bezogene Ressourcen sind über ein Netzwerk, typischerweise das Internet, zu erreichen. Dabei kommen Standardprotokolle wie HTTP, XML, JSON etc. zur Anwendung. Für die Benutzung der Cloud-Angebote stellen die Betreiber häufig Web-APIs oder REST-Schnittstellen zur Verfügung. Durch diese Fokussierung auf standardisierte Netzwerkzugriffe wird auch eine breite Palette von Endgeräten unterstützt. So können Mobiltelefone, PDAs, Netbooks und Slates genauso wie herkömmliche Arbeitsplatzrechner oder Laptops auf die Dienste zugreifen.[6] Allerdings muss die Verbindung der Geräte mit dem Internet eine ausreichend große Bandbreite aufweisen, um die Dienste sinnvoll nutzen zu können.

Measured Service – Messung der Servicenutzung

Nach der ursprünglichen Idee des Utility-Computing sollten Cloud-Angebote streng nutzungsbezogen bezahlt werden. Dafür ist es nötig, dass der Anbieter die tatsächliche Ressourcennutzung genau misst. Welche Messverfahren und Messgrößen zum Einsatz kommen, hängt natürlich von der Art der Ressource ab. Beispiele sind auf der Platte gespeicherte GiB für Speicherplatz, benutzte CPU-Zyklen für Rechenleistung und gespeicherte Datensätze in einer Database-as-a-Service. Das System kann auf Basis der Messungen auch selbständig Aktionen ergreifen und z. B. physische Ressourcen anfordern oder umverteilen. Die Ressourcennutzung wird sowohl an den Kunden als auch an den Anbieter gemeldet, einerseits für Abrechnungszwecke, andererseits auch zur Kontrolle, falls z. B. durch Programmierfehler unerwartet hohe Kosten entstehen.

Die Kombination von dynamischer Anpassung der Ressourcenmenge und der genauen Messung der Servicenutzung ermöglicht eine nutzungsabhängige Abrechnung der Gebühren für die Servicenutzung. Dieser Aspekt wird häufig sogar als Charakteristikum für Cloud-Computing genannt, ist aber eigentlich nur eine logische Folge aus der Anwendung der vorgenannten Prinzi-

[6] Dies gilt vor allem für SaaS, wobei die Voraussetzung ist, dass auf dem Endgerät ein ausreichend umfangreicher Webbrowser zur Verfügung steht. Nur mit Einschränkungen gilt dies auch für PaaS und IaaS, weil hier die Schnittstellen eher auf einen programmatischen Zugriff, z. B. durch eine „App“ ausgelegt sind. Zur Klärung dieser Begriffe, siehe Abschnitt 2.1.4.

Tabelle 2.1: Vergleich der Eigenschaften von Cluster-, Grid- und Cloud-Computing.

Charakteristikum	Cluster	Grid	Cloud
Gemeinsame Nutzung physischer Ressourcen	✔	✔	✔
Allgemeiner Netzwerkzugriff	✔	✔	✔
Unverzügliche Anpassbarkeit an Bedarf	✖	✖	✔
Selbstbedienung nach Bedarf	✖	✖	✔
Messung der Servicenutzung	✖	✔	✔
Arbeiten mit virtuellen Ressourcen	✖	✖	✔

pien. Im Englischen hat sich der Begriff *Pay-per-Use* eingebürgert, um diese nutzungsabhängige Bezahlung zu beschreiben. Als Randbemerkung sei an dieser Stelle darauf hingewiesen, dass der Term „Pay-as-you-go“, den man in englischsprachigen Texten häufig synonym verwendet, nicht identisch ist. Das Pay-as-you-go-Prinzip bedeutet, dass statt einer einmaligen Lizenzzahlung eine periodisierte Zahlung anfällt. Diese Zahlung ist aber nicht notwendigerweise nutzungsabhängig, sondern häufig eine „Monatsmiete“, die auch anfällt, wenn keine Nutzung erfolgt ist. Das Pay-per-Use-Konzept schließt zwar auch eine Periodisierung der Zahlungen ein und ist insofern ähnlich zum Pay-as-you-go. Es verlangt aber zwingend eine Korrelation der Gebühr mit der tatsächlichen Dienst-Nutzung.

Pay-per-Use

Vergleich zwischen Cluster-, Grid- und Cloud-Computing

Um die Unterschiede zu den vorherigen Konzepten Cluster- und Grid-Computing zu verdeutlichen, sollen die jeweiligen Eigenheiten in diesem Abschnitt kurz hervorgehoben werden. Alle drei Systeme sind verteilte Systeme mit ähnlichen Eigenschaften. Tabelle 2.1 zeigt die Unterschiede zusammenfassend anhand der fünf Cloud-Charakteristika auf und bezieht zusätzlich explizit den Aspekt der Virtualisierung mit ein. Wie aus der Tabelle ersichtlich wird, sind die Konzepte vergleichbar in Bezug auf die gemeinsame Nutzung physischer Ressourcen (Resource-Pooling) und den Netzwerkzugriff. Allerdings erfolgt der Zugriff auf Clouds eher über öffentliche Netze, während der Zugriff auf ein Grid und besonders ein Cluster eher über ein Intranet geschieht.

Abgesehen davon sind Cloud-Systeme jedoch deutlich dynamischer als ihre Vorgänger. Während in Grid- und Cluster-Umgebungen meist eine Reservierung der Ressourcen im Vorfeld erfolgt, werden bei Cloud-Systemen diese je nach aktuellem Bedarf bereitgestellt. Auf Schwankungen des Bedarfs können daher auch nur Cloud-Systeme angemessen schnell reagieren. Bei der Messung der Servicenutzung lässt sich festhalten, dass Cloud- und Grid-Systeme diese unterstützen. Cluster-Systeme bieten i. d. R. jedoch keine ausgefeilten Messmöglichkeit. Darüber hinaus unterscheidet sich das Cloud-Computing dadurch, dass explizit und ausschließlich mit virtuellen Ressourcen gearbeitet wird. Beim Grid- und Cluster-Computing ist zwar auch eine Abstraktion von der physischen Hardware vorhanden. Jedoch fehlt der Aspekt der Virtualisierung der Ressourcen in der jeweiligen Softwareschicht, die stattdessen eine abstrakte Sicht auf die physischen Ressourcen des Systems bietet.

Höhere Dynamik

Unternehmen erhalten also durch Cloud-Computing eine deutlich flexiblere Lösung im Vergleich zu anderen verteilten Systemen wie Grid und Cluster. Außerdem ist es, bedingt durch die Natur des Cloud-Computings, sehr viel einfacher, die Dienste von externen Anbietern zu beziehen, so dass keine größeren Investitionen in die eigene Infrastruktur nötig werden.

Sicherheit

Jedoch gehen mit dem Einsatz von Cloud-Computing eine Reihe von Sicherheitsrisiken einher, deren Ursachen meist auf mangelnden Einsatz und Unterstützung von Sicherheitstechnologien zurückzuführen sind. Auch neu zu entwickelnde oder nicht ausgereifte Technologien können eine sichere Benutzung von Cloud-Services verhindern [13]. Daher müssen Unternehmen, die Cloud-Systeme einsetzen möchten, eine detaillierte Betrachtung der Sicherheitsrisiken durchführen, wenn sichergestellt sein soll, dass die neuen Cloud-Computing-Systeme dasselbe von internen Systemen gewohnte Sicherheitsniveau erfüllen. Diese Risiken können — beispielsweise bei Diebstahl vertraulicher Informationen — erheblichen Einfluss auf das Geschäftsmodell des Dienstnutzers haben. Die Cloud-Nutzung ist aktuell daher je nach Szenario nur eingeschränkt möglich. Weitere Details hierzu finden sich in Kapitel 5.

2.1.4 Servicemodelle: XaaS

Inzwischen gibt es eine nahezu unüberschaubare Vielfalt an Cloud-Services, die mannigfaltige IT-Ressourcen anbieten. Sprach man zuerst von Software-as-a-Service und Infrastructure-as-a-Service, so kamen bald weitere Angebote wie Storage-as-a-Service, Logic-as-a-Service oder Network-as-a-Service hinzu. Inzwischen gibt es sogar seltsam anmutende Auswüchse wie Human-as-a-Service. Wegen des gemeinsamen Suffix fasst man alle Arten von Cloud-Services gerne unter dem Begriff *Anything-as-a-Service (XaaS)* zusammen. Zwar sind viele dieser Service-Bezeichner durchaus sinnvoll – wie z. B. der Terminus Database-as-a-Service, der in diesem Leitfaden behandelt wird –, aber es haben sich drei Hauptbegriffe herausgebildet, mit deren Hilfe, Cloud-Angebote zumindest einigermaßen trennscharf kategorisiert werden können. Das NIST schlägt zur Einteilung drei sogenannte Servicemodelle vor, die eine Einteilung anhand der Art der angebotenen Dienstleistung erlauben:

- Software-as-a-Service (SaaS)
- Platform-as-a-Service (PaaS)
- Infrastructure-as-a-Service (IaaS)

Abgeleitet von den drei Anfangsbuchstaben spricht man manchmal auch vom SPI-Ordnungsrahmen. Abbildung 2.3 stellt die drei Servicemodelle im Zusammenhang dar. Dabei ist zu beachten, dass weiter unten liegende Servicemodelle nicht verpflichtend eingesetzt werden müssen. So ist es denkbar, dass eine SaaS direkt auf einer IaaS realisiert wird (ohne dazwischen liegende PaaS). Ebenso könnte eine PaaS direkt auf virtualisierter Hardware aufsetzen, ohne IaaS zu nutzen (etc.).

Obschon eine Einteilung aktueller Cloud-Angebote anhand dieser Klassen nicht trennscharf ist, bietet es sich an, die drei vom NIST vorgeschlagenen Klassen zur Grobeinteilung zu verwenden. Besonders die Grenze zwischen PaaS und SaaS verschwimmt jedoch aktuell noch.

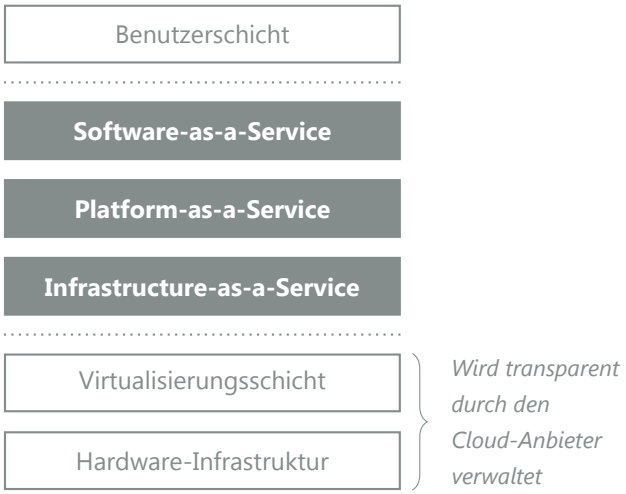

Abbildung 2.3: Die typische Dreiteilung in SaaS, PaaS und IaaS.

Software-as-a-Service (SaaS)

Beim SaaS-Modell bietet der Provider eine Software an, die der Endkunde direkt einsetzen kann. Der Betrieb der Software liegt vollständig beim Anbieter, der sich um alle Aspekte der Wartung, Aktualisierung, Weiterentwicklung oder Lizensierung der benötigten Soft- und Hardware kümmert. Üblicherweise werden mandantenfähige Programme eingesetzt, um die nötigen Skaleneffekte zu realisieren. Der Benutzer greift auf die Software per Webbrowser zu, anders als beim ASP-Modell, wo ein Terminalserver zum Einsatz kommt. Während der Benutzer nur seine Daten ins System eintragen muss und ggf. noch kleinere Einstellmöglichkeiten zur Individualisierung der Software hat, trägt der Anbieter Sorge, dass Backups der Daten gemacht werden. Softwareupdates erfolgen in der Regel vom Benutzer unbemerkt und in kleinen Inkrementen, anders als die großen Versionssprünge beim klassischen Software-Lizenzmodell. Beispiele für SaaS sind SalesForce CRM, Google Docs, die Zoho On-Demand Suite oder Gliffy.

Platform-as-a-Service (PaaS)

Im Fall von PaaS bietet der Provider den Nutzern die Möglichkeit, eigene Programme auf einer Plattform in der Cloud bereitzustellen. Die gesamte Infrastruktur – von der Plattformsoftware abwärts bis hin zur Hardware – wird vom Provider bereitgestellt und verwaltet. Dieser legt dabei gewisse Rahmenbedingungen, wie z. B. die Programmiersprache und verwendbare Bibliotheken oder Schnittstellen fest. Der Kunde kann innerhalb dieses Rahmens seine Programme frei gestalten. Oft wird nicht nur die Plattform für den Betrieb, sondern auch eine Umgebung für die Entwicklung der Programme angeboten. Durch den festen Rahmen kann der Provider bestimmte Annahmen treffen und dadurch eine umfassende Automatisierung ermöglichen. So ist es üblich, dass PaaS-Anbieter eine automatische Skalierung abhängig von der Nachfrage anbieten. Außerdem können leicht redundante Kopien der Programme auf andere Systeme verteilt werden, so dass eine sehr hohe Verfügbarkeit garantiert werden kann. Typische Vertreter aus

dem PaaS-Segment sind z. B. die Google App Engine, Heroku, Microsoft Windows Azure oder Force.com.

Infrastructure-as-a-Service (IaaS)

Das Modell, welches der Vision des Utility-Computing am nächsten kommt, ist das IaaS-Modell. Hierbei bietet der Cloud-Provider virtuelle Hardware oder Infrastrukturdienste an, wie z. B. Speicherplatz, Rechenleistung oder Netzwerkbandbreite. Der Cloud-Nutzer kann diese virtuelle Infrastruktur in seine IT-Landschaft einbauen und von hoher Verfügbarkeit, automatischen Backups und transparenter Wartung durch den Anbieter profitieren. Die Benutzung der Ressourcen ist dabei mit größtmöglicher Flexibilität möglich. Dafür muss der Nutzer aber auch alle Schichten oberhalb der Infrastrukturschicht (z. B. Betriebssystem, Webserver, Datenbankserver) selbst verwalten. Der prototypische Vertreter von IaaS ist die Rechenleistung („Compute“) aus der Cloud, was sich auch im Begriff „Cloud-*Computing*“ widerspiegelt. Angebote im Bereich IaaS sind z. B. die Amazon Web Services (EC2, S3, SimpleDB, …), GoGrid, RackSpace, ScaleUp und viele andere.

2.1.5 Arten des Cloud-Betriebs

Neben der Art der erbrachten Services unterscheidet man verschiedene Arten des Cloud-Betriebs in Bezug auf die Öffnung der Cloud nach außen. Dabei ergeben sich zwei elementare Typen:

- Eine sog. *öffentliche Cloud* (engl. *Public Cloud*) ist die typische Art von Cloud, in der jeder die angebotenen Services beziehen kann. Ggf. wird dafür eine Nutzungsgebühr erhoben, aber die Produktpalette an sich ist für die Allgemeinheit oder zumindest für eine hinreichend große Interessengruppe verfügbar. Verwaltet wird eine solche Cloud durch einen Anbieter, der sich darauf spezialisiert hat, Cloud-Services zu verkaufen. Ein Beispiel ist die Cloud von Amazon.

- Eine sog. *nichtöffentliche Cloud* (engl. *Private Cloud*) hingegen wird ausschließlich für eine einzige Organisation betrieben. Diese Organisation verwaltet die Cloud entweder selbst oder hat einen externen Dienstleister, der die Verwaltung übernimmt. Das Rechenzentrum kann dabei sowohl auf dem Gelände der Organisation als auch ausgelagert sein. In jedem Fall ist der Zugang zu den Cloud-Diensten auf Mitglieder der Organisation beschränkt. Dieses Modell ist in aller Regel nur für sehr große Organisationen attraktiv. Ein Beispiel wäre eine nichtöffentliche Cloud in einem Universitätsrechenzentrum, die ausschließlich Forschern dieser Universität zur Verfügung steht.

Neben diesen beiden elementaren Typen können noch zwei weitere, abgeleitete Typen des Cloud-Betriebs unterschieden werden:

- Eine sog. *Community-Cloud* ist eine Art nichtöffentliche Cloud, die sich mehrere Organisationen mit ähnlichen Anforderungen teilen. Beispielsweise könnte es wegen bestimmter gesetzlicher Anforderungen im Gesundheitswesen sinnvoll sein, eine Cloud speziell für eine Gruppe von Krankenhäusern bereitzustellen. Die beteiligten Organisationen verwalten die Cloud entweder selbst oder geben diese Aufgaben an externe Dienstleister ab.

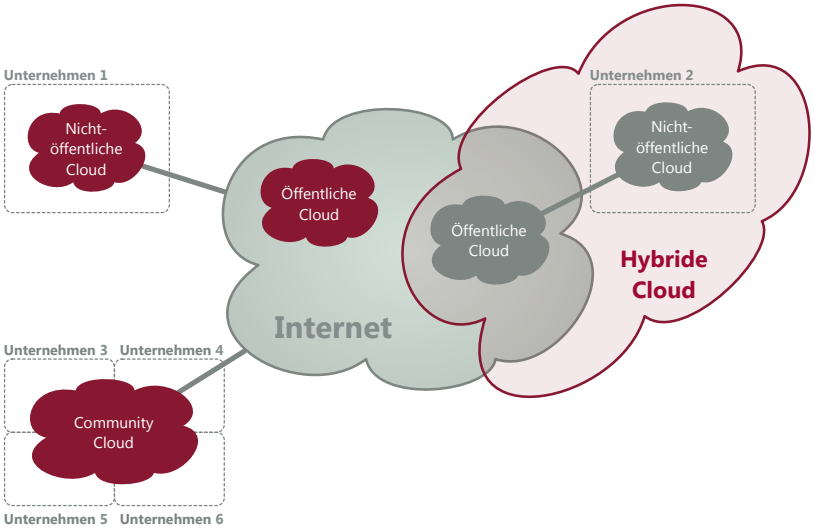

Abbildung 2.4: Die vier Arten des Cloud-Betriebs: öffentliche, nichtöffentliche, hybride und Community-Cloud.

Das Rechenzentrum kann sich dabei sowohl auf dem Gelände einer der Organisationen als auch bei einem externen Dienstleister befinden.

- Eine sog. *hybride Cloud* schließlich entsteht aus dem Zusammenschluss mehrerer anderer Clouds. Sie wird mehr oder weniger eng durch Standards oder proprietäre Technologien verknüpft und ermöglicht den Austausch von Daten und Programmen. Ein typischer Anwendungsfall ist das *Cloud-Bursting*, also das „Ausbrechen“ aus einer Cloud zusätzlich in eine weitere Cloud, wenn die Ressourcen der ersten nicht mehr ausreichen. Ein weiteres Szenario könnte sein, dass eine Lastbalancierung zwischen mehreren Clouds einer Organisation stattfinden soll.

Die vier Arten des Cloud-Betriebs sind in Abbildung 2.4 visualisiert. Es ist zu erwarten, das für absehbare Zeit die nichtöffentliche Cloud oder die Community-Cloud das für die meisten Unternehmen geeignete Modell ist. Nur diese beiden Modelle lassen die Auslagerung sensibler Daten und Funktionen zu, bis alle rechtlichen Unklarheiten beseitigt sind. Die hybride Cloud kann als Kompromiss ebenfalls eingesetzt werden, wenn sie nur aus nichtöffentlichen oder Community-Clouds besteht. Die öffentliche Cloud eignet sich derzeit nur für die Arbeit mit nicht-sensiblen Daten, z. B. höchst skalierbare Websites oder Massendatenverarbeitung auf anonymen Logfiles etc. Die Anwendungsmöglichkeiten für die öffentliche Cloud sind jedoch besonders im Bereich der KMU zurzeit noch nicht besonders vielfältig. Andererseits lohnt sich die Erstellung einer eigenen, nichtöffentlichen Cloud erst aber einer recht ordentlichen Mindestgröße, was diese Lösung für die meisten KMU unattraktiv macht.

2.2 Abgrenzung zum klassischen IT-Outsourcing

Die Verwendung von Cloud-Diensten ist im Wesentlichen eine Spielart des IT-Outsourcing. Unter dem Begriff IT-Outsourcing wird die Auslagerung der IT ganz oder in Teilen an externe Dienstleister verstanden. Werden nur einzelne IT-Funktionen ausgelagert, so spricht man von selektivem Outsourcing, wird hingegen die gesamte IT ausgelagert, so nennt man dies totales Outsourcing. Ja nach Variante können sich „ausgelagerte“ Infrastruktur und Software sowohl beim Kunden als auch beim Anbieter befinden. Wichtig ist, dass die Verantwortung für diese immer auf den externen Anbieter übertragen wird.

OLTP

Außer im seltenen Fall einer reinen nichtöffentlichen Cloud im eigenen Rechenzentrum, befinden sich Hard- und Software beim Cloud-Computing notwendigerweise in den Rechenzentren des Anbieters. Für den Anwendungsfall DaaS hat dies die direkte Konsequenz, dass sich Cloud-Dienste i. d. R. nicht gut eignen, um OLTP-artige Systeme auszulagern. Während man im klassischen Modell die Möglichkeit hat, den Datenbank-Server ins eigene Rechenzentrum zu stellen und nur die Verwaltung der Hard- und Software abzugeben, um weiterhin von schnellen Netzwerkverbindungen und niedriger Latenzzeit zu profitieren, ist dies beim Outsourcing in die Cloud nicht möglich. Hier muss der Zugriff auf das Datenbanksystem (DBS) immer über eine Internetverbindung erfolgen, welche häufig nicht ausreichend schnell für OLTP-Anwendungen ist.

Dynamik

Gleichzeitig bietet diese Entkopplung aber auch das Potential, die Erbringung der Cloud-Services dynamisch über zahlreiche Standorte zu verteilen. Außerdem erlaubt das Cloud-Computing eine sehr kurzfristige Anpassung an den tatsächlichen Bedarf, viel schneller als dies beim klassischen Outsourcing der Fall ist. Dabei bestimmt und konfiguriert der Cloud-Anwender einen Großteil der Funktionalität über eine Webseite ohne Involvierung des Anbieters.

Ein wichtiger Unterschied zwischen IT-Outsourcing und Cloud-Computing existiert auch im Hinblick auf die Anpassung der Geschäftsprozesse. Während im klassischen Fall üblicherweise der Anbieter dafür Sorge trägt, die angebotenen Systeme an die Geschäftsprozesse des Kunden anzupassen („Customizing“), bieten Cloud-Provider hauptsächlich standardisierte Produkte an, die geringe bis keine Anpassungsmöglichkeiten bieten. Der Kunde muss – je nach Art der Dienstleistung – die Angebote eigenständig anpassen (z. B. durch selbst programmierte Geschäftslogik) oder sogar die internen Abläufe ändern, um die Cloud-Services besser in die eigenen Prozesse zu integrieren.

Lock-in-Effekte

Je nach Umfang der Anpassungen an die Geschäftsprozesse kann es beim Outsourcing zu Lock-in-Effekten kommen, da der Anbieter nach den aufwändigen Anpassungen häufig eine lange Vertragslaufzeit erzwingt. Das klassische IT-Outsourcing ist daher durch mittel- bis langfristige Vertragsverhältnisse gekennzeichnet. Beim Cloud-Computing sind die Mindestlaufzeiten der Verträge häufig extrem kurz, z. B. monatlich kündbar. In der Praxis ist jedoch zu erwarten, dass die Auslagerungen in die Cloud auch eher einen mittel- bis langfristigen Horizont haben werden, da die Anpassungen auf Kundenseite zurzeit noch einen häufigen Anbieterwechsel nicht sinnvoll erscheinen lassen. Andererseits möchte vielleicht sogar der Kunde eine längere Laufzeit durchsetzen, um Sicherheit in der Planung seiner Systeme und Schnittstellen zu haben. Dies ist zumindest mit den Standardverträgen der aktuellen Angebote nicht möglich.

2.3 Spezialfall Database-as-a-Service (DaaS)

Einer der vielen Cloud-Services, die unter dem XaaS-Dach zusammengefasst werden, ist die Database-as-a-Service. Dieser Abschnitt erläutert die Details verschiedener Varianten dieses Konzepts und klärt über die Besonderheiten von Database-as-a-Service im Vergleich zu anderen Cloud-Services auf. Nach einer Definition und Abgrenzung des Begriffs, werden die fünf Cloud-Charakteristika beleuchtet und schließlich ein kritischer Ausblick auf das Problem der fehlenden Elastizität von Daten gegeben.

2.3.1 Definition und Abgrenzung

Nachdem in Abschnitt 2.1.4 die grundlegende Dreiteilung in SaaS, PaaS und IaaS vorgestellt wurde, soll nun der Begriff *Database-as-a-Service (DaaS)* geklärt werden. Wie der Begriff suggeriert, werden bei dieser Art von Diensten Funktionalitäten eines Datenbanksystems als Dienstleistung angeboten. Dies entspricht auch dem kleinsten gemeinsamen Vielfachen der in der Literatur vorherrschenden Definitionen.[7] Hinter DaaS steckt also die Bereitstellung eines Datenbank*systems* in einer service-orientierten Art und Weise. Präziser wäre es daher, den Begriff „Database-*System*-as-a-Service“ zu verwenden, da eine Datenbank nur eine Sammlung von Daten repräsentiert und keine Funktionalität im eigentlichen Sinne bereitstellt [36, S. 10]. In diesem Leitfaden benutzen wir trotzdem die zwar etwas unpräzise, aber inzwischen etablierte Bezeichnung Database-as-a-Service (DaaS) und meinen damit alle Cloud-Datenbanksysteme. Tatsächlich gibt es aber bereits Angebote, die ausschließlich Daten in einer Datenbank in der Cloud zur Verfügung stellen. Um diese explizit mit einzuschließen, sprechen manche Autoren auch von *Cloud Data Services (CDSs)* [31].

Bei konservativer Betrachtungsweise besteht der Kern von DaaS aus der Bereitstellung grundlegender Funktionalität eines relationalen Datenbanksystems (RDBS). Insbesondere ist die Vorgabe eines Datenmodells, das eine Strukturierung und Beschreibung der zu speichernden Daten ermöglicht, als elementar anzusehen. Damit verbunden sollten die bewährten drei Abstraktionsebenen (physische, logische und externe Ebene, vgl. [36]) und die Möglichkeit der Definition von Schemata für jede Ebene ermöglicht werden. Zudem muss die Möglichkeit gegeben sein, mittels einer Sprache – üblicherweise der Structured Query Language (SQL) – oder einer Programmierschnittstelle auf die Daten und Datendefinitionen des Systems zuzugreifen bzw. diese manipulieren zu können. Für den Einsatz im Unternehmensbereich wird darüber hinaus ein Benutzer- und Rechtekonzept benötigt, mit dem der Zugriff auf einzelne Datenelemente oder Gruppen von Datenelementen gesteuert werden kann. Gleichzeitig ist die Unterstützung eines Transaktionskonzept zu gewährleisten. Ein Beispiel für diese Art von DaaS-Dienst ist der Relational Database Service (RDS) von Amazon, bei dem mit MySQL ein klassisches RDBS als Cloud-Dienst angeboten wird.

Diese konservative Sicht wird allerdings bei aktuellen Cloud-Angeboten des öfteren abgelegt.

[7] Gelegentlich wird „Database-as-a-Service“ auch als „DAS“ abgekürzt. In Analogie zum SPI-Ordnungsrahmen („*X*aaS“) erscheint jedoch die Abkürzung „DaaS“ sinnvoller. Die ebenfalls in der (älteren) Literatur verwendete Bezeichnung „Outsourced Database (ODB) Model“ hat sich nicht durchgesetzt.

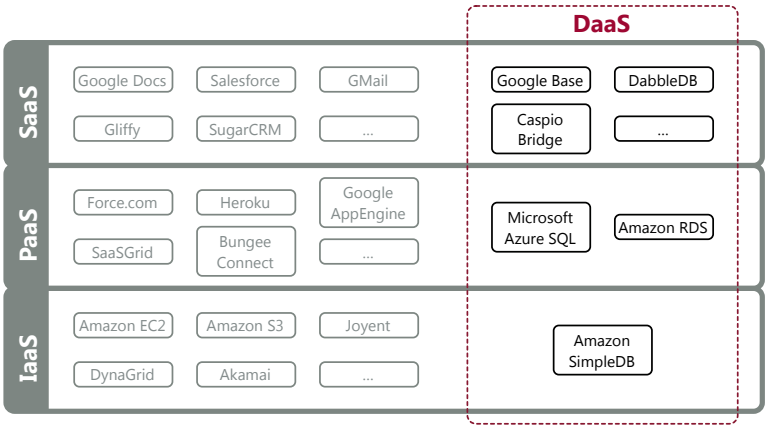

Abbildung 2.5: Die drei Servicemodelle des NIST im Vergleich zu DaaS.

Hier finden sich neue Konzepte, die keine Schemata unterstützen, nur eingeschränkte Abfragemöglichkeiten bieten oder die strenge Konsistenz der traditionellen RDBS aufweichen. Gerade im Bereich der Verarbeitung riesiger Datenmengen weichen Firmen wie Google oder Amazon auf sog. NoSQL-DBS aus, die z. B. laxere Konsistenzgarantien geben, dafür jedoch höchste Verfügbarkeit ermöglichen (vgl. Abschnitt 2.3.2 zur Eventual Consistency). Beispielhafte DaaS-Produkte, die vom Angebot eines klassischen relationales Datenbanksystem (RDBS) abweichen, sind z. B. Amazon SimpleDB, DabbleDB oder Google HBase.

Entsprechend der vielfältigen Ausgestaltungsmöglichkeiten des DBS-Aspektes eines DaaS-Dienstes ist es nicht möglich, DaaS insgesamt einer der drei Service-Klassen aus dem SPI-Ordnungsrahmen zuzuordnen. Vielmehr ist DaaS orthogonal zu den drei Klassen anzuordnen, wie Abbildung 2.5 zeigt. Viele konkrete DaaS-Dienste können aber eindeutig einer der drei Klassen zugeordnet werden. Beispielhafte Angebote für die jeweilige Schicht werden ebenfalls in der Abbildung 2.5 gezeigt.

Nicht immer gelingt die Einordnung eines DaaS-Dienstes im allgemeinen Fall, weil die Verwendungsmöglichkeiten des Dienstes zu vielfältig sind. Konkrete DaaS-Angebote können jedoch eindeutig einer der drei Schichten zugeordnet werden, wenn man nicht eine Analyse der technischen Merkmale des Dienstes durchführt. Stattdessen sollten die Services aus Benutzersicht kategorisiert werden, abhängig vom Verwendungszweck. Will der Benutzer als Endanwender eine eigenständige Software nutzen, die ihm DBS-Funktionalität bietet – z. B. als „erweitertes Excel“ für die Controlling-Abteilung – so fällt dieser DaaS-Dienst in die Kategorie Software-as-a-Service. Entsprechend können auch die übrigen beiden Klassen abgegrenzt werden. Abbildung 2.6 verdeutlicht das Vorgehen bei der Einordnung von DaaS-Diensten.

Zusammenfassend lässt sich der Begriff Database-as-a-Service wie folgt definieren:

> *Database-as-a-Service (DaaS)* ist ein Konzept, bei dem Datenbanksystemfunktionalität unterschiedlicher Granularitätsstufen, von Teilfunktionalität bis zur Gesamtfunktionalität, als Cloud-Service bereitgestellt wird. DaaS fasst Cloud-Services dabei durch ihre Funktion zu einer vierten Klasse zusammen, die orthogonal zu der SPI-Klassifikation ist. Konkrete DaaS-Dienste lassen sich jedoch abhängig vom

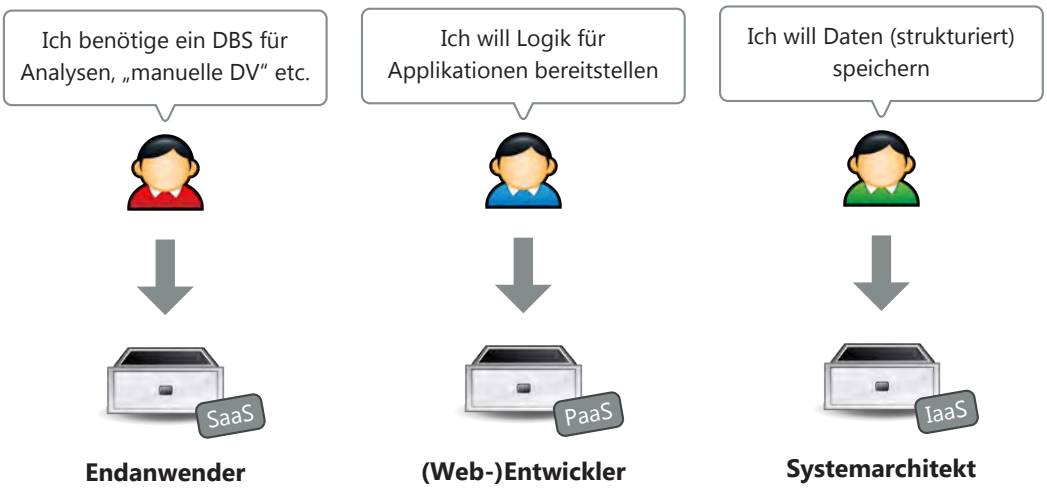

Abbildung 2.6: Die Spielarten von DaaS aus Benutzerperspektive.

Verwendungszweck einer der drei Klassen zuordnen.

Der Begriff des Cloud-Service wird dabei so verstanden, wie in Abschnitt 2.1.2 definiert.

2.3.2 Der Cloud-Aspekt von DaaS

Laut obiger Definition aus Abschnitt 2.3.1 weist ein DaaS-Dienst die fünf charakteristischen Merkmale für Cloud-Services aus Abschnitt 2.1.3 auf. Die konkrete Ausgestaltung für DBS wird im Folgenden genauer erläutert.

Resource-Pooling

Die physische Implementierung des Dienstes bleibt dem Benutzer verborgen. Diverse physische Hardwarekomponenten werden in einen gemeinsamen Topf geworfen. Die Benutzer arbeiten mit abstrakten Einheiten, z. B. logischen Tabellen oder Datentöpfen, die der Cloud-Anbieter beliebig auf konkrete Datenstrukturen und Hardwarekomponenten abbilden kann. Entsprechend kommt auch hier der Virtualisierungstechnologie eine Schlüsselrolle zu. Wird DaaS als SaaS angeboten, so werden die Systeme in aller Regel auch mandantenfähig konzipiert.

Rapid Elasticity

Entsprechend der Idee der flexiblen Anpassbarkeit des Ressourcenangebots kann das DBS scheinbar beliebig viele Daten aufnehmen und scheinbar beliebig viele Anfragen gleichzeitig bearbeiten. Die Skalierung sollte dabei völlig transparent erfolgen, da der Anbieter normalerweise ausreichend genaue Annahmen treffen kann, um den Vorgang komplett zu automatisieren. So kann vom Anbieter erwartet werden, dass die Verarbeitung der Anfragen per Lastbalancierung auf verschiedene Systeme verteilt wird und die Daten kontinuierlich auf andere Systeme repliziert werden.

Durch eine automatische Replikation der Systeme in andere Rechenzentren kann der Anbieter eine hohe Verfügbarkeit und Datensicherheit garantieren. Andererseits erfordern diese Garantien üblicherweise die Lockerung des verwendeten Konsistenzkonzepts.[8] Die meisten Anbieter setzen dabei auf die sog. *Eventual Consistency* – zu Deutsch etwa „letztendliche Konsistenz" –, bei der die Konsistenz der Daten erst nach einem gewissen Zeitfenster garantiert wird. Erfolgen keine Änderungen an den Daten, so bewegen sich alle Repliken hin zu einem einheitlichen, konsistenten Datenstand. Dieses Prinzip wird bereits seit langem im Domain Name System (DNS) verwendet und ist für viele Anwendungen (z. B. Online-Shops) durchaus ausreichend. Anwender müssen sich jedoch dessen bewusst sein, dass die ACID-Garantien der klassischen RDBS bei DaaS häufig nicht mehr gelten. Statt ACID[9] gilt im Internet oft BASE[10] mit einer der folgenden zwei typischen Garantien:[11]

- **Monotonic Reads** Hat ein Prozess einen bestimmten Wert gelesen, so ergeben nachfolgende Anfragen garantiert diesen oder einen neueren Stand, aber nie einen älteren.
- **Read-Your-Writes** Hat ein Prozess einen bestimmten Wert geschrieben, so sieht er garantiert diese eigene Änderung bei den nächsten Lesevorgängen und erhält nie eine ältere Version.

Pay-per-Use

Die Abrechnung erfolgt abhängig von der Nutzung. Typischerweise zahlt der Nutzer für den belegten Speicherplatz und den ein- und ausgehenden Datenverkehr (z. B. pro GiB) sowie für die verbrauchte Rechenleistung (z. B. pro CPU-Stunde). Oft sind diese eher physischen Größen jedoch nicht ganz passgenau zur Abstraktion durch das Resource-Pooling. Beispielsweise ist nicht ganz klar, wie viel Platz ein Datensatz auf dem Speichermedium beansprucht, weil Anbieter wie Amazon auch den durch interne Metadaten belegten Platz in Rechnung stellen. Eigentlich würde sich der Benutzer daher noch abstraktere Messgrößen wünschen, so dass die Servicenutzung z. B. pro Transaktion, pro Abfrage oder pro Datensatz bezahlt wird.

Measured Service

Um die Abrechnung abhängig von der Nutzung zu gewährleisten, muss natürlich der Ressourcenverbrauch erhoben werden. Außerdem können durch die Messung bestimmter Serviceparameter auch die Einhaltung von SLAs überwacht und ggf. Verstöße gegen diese gemeldet werden. Der Anbieter kann so physische Ressourcen umverteilen, um die SLAs der wertvolleren Kunden

[8] Das *CAP-Theorem* [12] besagt, dass ein verteiltes System (mit bestimmten Voraussetzungen), nicht gleichzeitig maximale Konsistenz (**C**onsistency), Verfügbarkeit (**A**vailability) und Toleranz in Bezug auf Netzwerkprobleme (**P**artition Tolerance) aufweisen kann. Nur zwei der drei Attribute können gleichzeitig maximiert werden. Daher nehmen hochverfügbare Cloud-DBS i. d. R. Abstriche bei der Konsistenz in Kauf, um den Ausfall einzelner Knoten und Netzwerkprobleme verkraften zu können.

[9] ACID steht für **A**tomic, **C**onsistent, **I**solated, **D**urable. Vgl. hierzu z. B. [36, S. 643 f.].

[10] BASE steht für **B**asically **A**vailable, **S**oft State, **E**ventually Consistent. Vgl. hierzu [29].

[11] Es gibt noch weitere Arten, Eventual Consistency zu garantieren.

einzuhalten, während nicht so hoch priorisierte Kunden dadurch ein schlechteres Serviceniveau erleben.

Broad Network-Access

Der Zugriff auf den Service erfolgt über das Internet unter Nutzung üblicher Webstandards. Normalerweise kommen hier Standards wie HTTP, REST, XML, SOAP, JSON, RSS etc. zum Einsatz. Dies ermöglicht die Nutzung auf diversen Plattformen und Endgeräten, einschließlich neuerer Smartphones oder Netbooks. Im Endeffekt kann jedes Endgerät, das über einen einigermaßen vollständigen Webbrowser verfügt, auf SaaS- und PaaS-Dienste zugreifen. IaaS-Dienste werden in der Regel nicht direkt vom Endanwender angesprochen, sondern (ebenfalls über Webstandards) in andere Dienste oder Anwendungen integriert.

2.3.3 Mangelnde Elastizität der Daten

Ein wichtiger Vorteil von Cloud-Diensten ist ihre oft beworbene „Elastizität“, die auch in Abschnitt 2.1.3 bereits vorgestellt wurde. Für echte *Computing*-Produkte in der Cloud ist diese Elastizität relativ einfach zu erlangen. Virtuelle CPUs oder auch virtuelle Maschinen können in kurzer Zeit an- und abgeschaltet werden. Ob dann der Berechnungsauftrag zu einer Ressource oder einer anderen geroutet wird, ist für das Ergebnis und die Geschwindigkeit unerheblich.

Für Cloud-Storage-Dienste stellt sich die Situation schon anders dar. Zwar ist die Erweiterung der vorhandenen Speicherkapazität in der Regel einigermaßen unproblematisch, aber die Reduzierung kann nur durchgeführt werden, wenn die Daten nicht mehr benötigt werden. Im Regelfall muss vorher eine Sicherungskopie erstellt werden, was bei großen Datenmengen Stunden oder Tage dauern kann und entsprechende Bandbreitenkosten verursacht. Anders als bei Computing-Diensten sind die Daten eher ortsgebunden und nicht so flexibel zu handhaben.

Diese Problematik stellt sich natürlich auch für DBS in der Cloud, die mit größeren Mengen von Daten arbeiten. Dazu kommt aber nun auch das Problem der Skalierbarkeit des DBS als solches. Die Cloud allein bringt keine Lösung für das aus dem eigenen Rechenzentrum wohlbekannte Skalierungsproblem von traditionellen RDBS. Zwar existieren skalierbare DBS, die gewisse Abstriche im Vergleich zu den bekannten RDBS machen (vgl. z. B. Passage zur Eventual Consistency in Abschnitt 2.3.2). Übliche Cloud-Dienste für ein RDBS, wie der Amazon Relational Database Service (RDS), bieten z. B. eine vertikale Skalierbarkeit (scale up) in Bezug auf Prozessorleistung, Hauptspeicher und Plattenspeicher an. Eine wirklich befriedigende Lösung für das Problem steht allerdings noch aus, weswegen die tatsächliche Elastizität bei datenintensiven Cloud-Diensten nur eingeschränkt existiert.

2.4 Zusammenfassung der Grundlagen

Die generelle Idee der Kapselung von Funktionalität als Dienst ist im IT-Kontext, insbesondere im Rahmen einer SOA, schon länger bekannt. Im Suffix „as-a-Service“ werden genau diese Ideen wieder aufgegriffen und mit den neuen Konzepten des Cloud-Computing – vornehmlich Elastizität, Virtualisierung und Zugriff per Internet – zum Konzept des Cloud-Service kombiniert.

Es gibt verschiedene Servicemodelle für Cloud-Dienste und vier denkbare Arten des Cloud-Betriebs. Zusätzlich gibt es Service-Klassen, wie z. B. DaaS, die thematisch gleichartige Dienste zusammenfassen.

Wie im diesem Kapitel dargelegt, handelt es sich bei den technischen und wirtschaftlichen Grundlagen der Cloud-Dienste nur selten um grundlegend neue Konzepte; das Gesamtpaket ist jedoch durchaus neuartig. Cloud-Computing und insbesondere Database-as-a-Service kann für KMU sehr attraktiv sein, wenn die angebotenen Dienste zu den Rahmenbedingungen des geplanten Einsatzes passen. Welche Aspekte dabei genau beachtet werden müssen, beschreibt das folgende Kapitel.

3 Grundsatzentscheidung „Cloud oder nicht?“

Das Wichtigste in Kürze

- Cloud-Computing wird in **vier Dimensionen** betrachtet.
- **Wirtschaftlich** kann Cloud-Computing sehr attraktiv sein, muss es aber nicht, insbesondere bei individuellen Verträgen.
- **Technisch** birgt Cloud-Computing für den Anwender nur wenig wirklich neue Herausforderungen, fordert aber oft eine Anpassung bestehender Systeme.
- **Rechtlich** ist Cloud-Computing noch höchst problematisch und derzeit weitgehend ungeklärt.
- **Organisatorisch** erfordert Cloud-Computing stringente Abläufe, die gegebenenfalls im Unternehmen erst noch einzuführen sind.
- Die Entwicklung einer **Cloud-Strategie** auf Managementebene ist eine essentielle Voraussetzung für jedes Cloud-Projekt.

Nachdem in Kapitel 2 durch eine Klärung der Grundlagen von Cloud-Computing und Database-as-a-Service ein gemeinsames Verständnis der Thematik geschaffen worden ist, geht es in diesem Kapitel um die grundsätzliche Entscheidung, ob eine Lösung mit Cloud-Computing angestrebt werden sollte oder nicht. Dazu werden einige Vorzüge und Probleme von aktuellen Cloud-Angeboten analysiert. Zudem werden einige Handlungsempfehlungen gegeben, für den Fall, dass Cloud-Computing tatsächlich in Frage kommt. Zum Ende des Kapitels stellen wir zwei übliche Szenarien des Einsatzes von Cloud-Diensten vor und erläutern die resultierenden Anforderungen. Bedingt durch die Leitfrage des Forschungsprojekts fokussieren wir in diesem Kapitel – wo nötig – auf das Spezialgebiet Database-as-a-Service. Ein kurzer Katalog von Leitfragen, die eine direkte Anwendung der Erkenntnisse auf das jeweilige Szenario ermöglichen, rundet das Kapitel ab.

3.1 Cloud Computing in vier Dimensionen

Im Folgenden werden die wichtigsten Vor- und Nachteile bzw. Neuerungen des Cloud-Computings erörtert. Da das Feld unter anderem durch die Verschiedenheit der Angebote recht unübersichtlich ist, wird die Diskussion zur besseren Übersichtlichkeit entlang von vier Dimensionen strukturiert, die im Rahmen der Analysen zu diesem Leitfaden identifiziert wurden. Diese Struktur wird auch im weiteren Verlauf dieses Leitfadens beibehalten. Zur Sprache kommen

1. wirtschaftliche,
2. technische,
3. rechtliche und

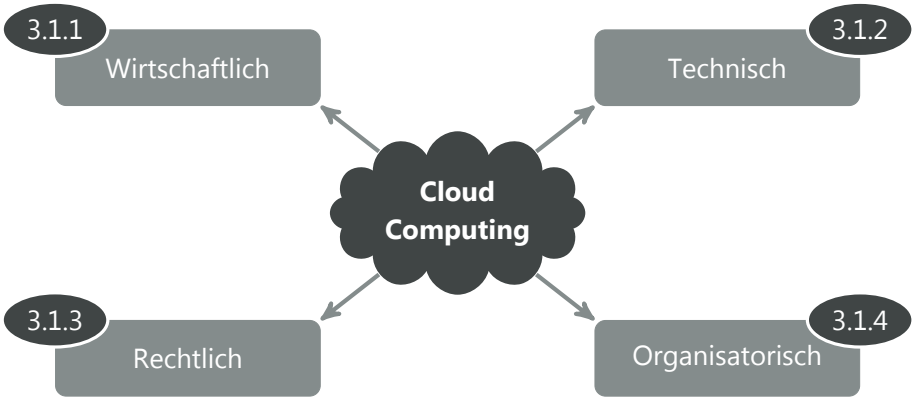

Abbildung 3.1: Die vier Dimensionen des Cloud Computings und gleichzeitig die Struktur des vorliegenden Kapitels mit der jeweiligen Abschnittsnummer.

4. organisatorische

Aspekte. Abbildung 3.1 stellt die Struktur des Kapitels inklusive der entsprechenden Abschnittsnummern grafisch dar.

3.1.1 Wirtschaftliche Dimension

Zweifellos sind die wirtschaftlichen Vorteile des Cloud-Computing die Hauptargumente, warum sich Unternehmen überhaupt mit dem Thema beschäftigen möchten. In diesem Abschnitt sollen daher die am häufigsten genannten Vorteile aufgelistet und hinterfragt werden, denn nicht immer sind die angepriesenen Vorzüge auch wirklich positiv zu bewerten. Üblicherweise werden sinngemäß folgende Punkte angesprochen (vgl. auch [32, S. 12]):

- Vorteile durch Bezahlung nur für die tatsächliche Nutzung
- Kostenvorteile des Anbieters, die an den Cloud-Nutzer weiter gegeben werden
- Kostenvorteile des Cloud-Anwenders, durch gesteigerte Flexibilität

Im Folgenden werden die Punkte jeweils detailliert erläutert. Zuvor sei allerdings noch auf einen Aspekt hingewiesen: Für einen Vergleich, ob sich Cloud-Computing im Vergleich zu einer Lösung im eigenen Haus lohnt, ist allerdings offensichtlich die erste Voraussetzung, dass die Kosten für eine solche Lösung im eigenen Unternehmen bekannt oder berechenbar sind. Sollte dies nicht möglich sein, so kann keine objektive Entscheidung für oder gegen Cloud-Computing getroffen werden.

Pay-per-Use – Nutzungsabhängige Bezahlung

Wie bereits in Abschnitt 2.1.3 angedeutet, werden die Cloud-Dienste in der Regel abhängig von der Nutzung abgerechnet; im Englischen spricht man von *Pay-per-Use*. Wird der Ansatz

in Reinform angewendet, so hat dies zur Konsequenz, dass die Kosten für die Cloud-Nutzung ganz direkt mit der tatsächlichen Ressourcennutzung korrelieren. Benötigt der Nutzer zeitweilig sehr viele Ressourcen, so bezahlt er für diese Zeit höhere Gebühren. Werden in einem Zeitraum jedoch keine Ressourcen benutzt, so fallen auch keine Kosten an. Oft findet man aber einen hybriden Ansatz bestehend aus einer Grundgebühr und einem nutzungsabhängigen Anteil. Die Grundgebühren sind aber in der Regel so niedrig, dass man trotzdem von einer nutzungsabhängigen Bezahlung sprechen kann.

Das Pay-per-Use-Prinzip hat im Allgemeinen zur Folge, dass effektiv nur ungefähr so viele Ressourcen bezahlt werden, wie es die Nachfrage erfordert. Somit bezahlt der Cloud-Nutzer, vereinfacht gesagt, die *durchschnittliche* Last. Im eigenen Rechenzentrum wird üblicherweise so geplant, dass auch die erwarteten Lastspitzen, z. B. zum Quartalsende, befriedigt werden können. Somit muss hier, wieder vereinfacht ausgedrückt, die *maximale* Last bezahlt werden, wenn der Dienst auf dedizierter Hardware läuft.

Gleichzeitig hat die nutzungsabhängige Bezahlung auch die Folge, dass sich das Investitionsrisiko größtenteils vom Nutzer zum Cloud-Anbieter verlagert. Der Anbieter übernimmt die Kosten für die benötigte Soft- und Hardware und trägt somit auch das Investitionsrisiko. Der Kunde bezahlt nur für die tatsächliche Nutzung des Dienstes. In der englischsprachigen Welt wird dieser Punkt häufig als Transformation von Capital Expenditure (CAPEX) in Operational Expenditure (OPEX), also im weitesten Sinne als Umwandlung von einmaligen in laufende Kosten, bezeichnet. Der Dienstanbieter wird natürlich das Investitionsrisiko bei der Preisgestaltung berücksichtigen. Jedoch wird das Risiko „auf viele Schultern“ verteilt, so dass jeder Kunde im Endeffekt nur einen geringen Bruchteil davon bezahlt.

Die nutzungsabhängige Bezahlung hat allerdings auch Auswirkungen bei der Berechnung der wirtschaftlichsten Alternative. Soll eine SaaS-Lösung mit einer Lösung verglichen werden, die den Kauf von Software-Lizenzen beinhaltet, so sollten die Kosten, wenn möglich, über den gesamten prognostizierten Nutzungszeitraum verglichen werden. In jedem Fall müssen aber Migrations- und Anpassungkosten einbezogen werden. Für die Lösung im eigenen Unternehmen fallen darüber hinaus meist noch Wartungsgebühren und Kosten für den Betrieb (Personal, Hardware, zusätzliche Software) an. Eventuell sollten auch zwischenzeitliche Upgradekosten einkalkuliert werden [16]. Insgesamt empfiehlt es sich, einen ganzheitlichen Ansatz, z. B. basierend auf der Total Cost of Ownership (TCO), zu wählen, um die gesamten Kosten der Alternativen zu vergleichen.

Bereits ohne aufwändige TCO-Berechnung können einige generelle Vor- und Nachteile der nutzungsabhängigen Bezahlung genannt werden. Offensichtlich lohnt sich ein Pay-per-Use-Modell, wenn die „Stückkosten“ in der Cloud günstiger sind als im eigenen Rechenzentrum. Kostet beispielsweise eine CPU-Stunde auf einer VM in Amazons EC2 weniger als eine CPU-Stunde im eigenen Unternehmen, so ist es auf jeden Fall günstiger, das Cloud-Angebot wahrzunehmen. Oft werden die Stückkosten in der Cloud jedoch geringfügig höher sein als die der eigenen Ressourcen. Selbst dann kann sich der Schritt in die Cloud rechnen, wenn nämlich der Preisaufschlag, im Englischen als *Utility-Premium* bezeichnet [38], kleiner ist als das Verhältnis von erwarteten Lastspitzen zu erwarteter Durschnittslast für den Dienst. Wenn z. B. in Spitzenzeiten doppelt so viele Ressourcen benötigt werden wie im durchschnittlichen Fall, so ist der Cloud-Dienst trotzdem günstiger, sobald die Stückkosten für die Cloud weniger als 200% der

Faustregel

internen Kosten betragen [38]. Diese Faustregel sollte jedoch nur ein erster Anhaltspunkt sein, um abzuschätzen, ob sich der Schritt in die Cloud rein monetär lohnen könnte oder nicht, da noch weitere Faktoren in die Berechnung hineinspielen.

Kostenvorteile durch Skaleneffekte beim Anbieter

Durch die hohe Spezialisierung des Anbieters und einen hohen Grad an Automation im Rechenzentrum wird es möglich, die Betriebskosten deutlich unter das Niveau zu senken, das ein gut organisiertes KMU erreichen könnte. Auf Beschaffungsseite entsteht ein großer Kostenvorteil durch die Skaleneffekte, die der Anbieter in Bezug auf die Investitionen in die Infrastruktur seiner Rechenzentren realisieren kann. Hochverfügbare Systeme und Maßnahmen für den Katastrophenfall können auf größerer Skala eingekauft und auf eine größere Anzahl von Nutzern verteilt werden. Auf diese Weise lassen sich für sehr große Rechenzentren – also solche in der Größenordnung von 50 000 Servern – Stückkosten realisieren, die nur 15-20% der Kosten betragen, die ein mittleres Rechenzentrum in der Größenordnung von 1 000 Servern realisieren könnte. Zudem können die Kosten für Brandschutz, Kühlung usw. auf viele Kunden umgelegt werden. Diese Skaleneffekte wird der Anbieter zumindest teilweise an seine Kunden weitergeben, um attraktive Preise anzubieten.

Auf technischer Seite kann der Anbieter durch Verfahren des Autonomic Computing [15] zusätzliche Einsparungen erreichen. Indem alle Aspekte der Verwaltung und der Konfiguration der Cloud-Infrastruktur weitestgehend automatisiert werden, lässt sich die Zahl der benötigten Mitarbeiter im Rechenzentrum und in der Verwaltung drastisch reduzieren. Auch aufseiten des Kundenunternehmens bedeutet die Auslagerung eine Entlastung beim IT-Personal, das sich nun um komplexere Aufgaben kümmern kann. Von der Theorie her bietet das Cloud-Computing also die Möglichkeit für eine Win-Win-Situation.

Kostenvorteile durch Ausnutzung der Elastizität

Der Einsatz von Cloud-Computing kann dem Unternehmen die Möglichkeit geben, bisher ungenutzte IT-Kapazitäten durch dynamische Zuweisung je nach aktuellem Bedarf Nutzen stiftend einzusetzen und die Investitionen in neue Hardware zu reduzieren. Diese Dynamik ermöglicht neue Geschäftsabläufe und kürzere Reaktionszeiten. So können z. B. neue Datenbanken einfach per Mausklick erzeugt werden, anstatt den oft langwierigen Weg über die traditionellen Prozesse zu nehmen. Im Endeffekt kann das Unternehmen so auch das Problem der Über- bzw. Unterversorgung deutlich reduzieren. Wird die Elastizität richtig ausgenutzt, werden die Ressourcen kostenmäßig nur noch etwa für den durchschnittlichen Fall vorgehalten. Unnötige Investitionen in eigene Hardware, um Lastspitzen befriedigen zu können, entfallen, ebenso Probleme, falls unvorhergesehene Lasten zu einer Ressourcenknappheit führen.

Die Elastizität bietet zudem Vorteile in Bezug auf die Bearbeitungsgeschwindigkeit einer Aufgabe. Ist beispielsweise ein Berechnungsproblem oder eine Massendatenverarbeitung gut parallelisierbar, so kann das Problem einfach auf eine große Zahl von Knoten verteilt werden. Das Pay-per-Use-Modell zusammen mit der Elastizität versprechen dann, dass ein Problem welches n Stunden auf einem Knoten benötigt, auch in einer Stunde durch n Knoten gelöst werden

kann – zu demselben Preis. Dieses Phänomen wird als *Cost-Associativity* bezeichnet [1]. Dadurch können Unternehmen große Batchjobs sehr viel schneller berechnen lassen als auf der eigenen Infrastruktur, so dass sich zeitliche Vorteile bei konstanten Kosten ergeben.

Diese zwei viel beworbenen Vorteile von Cloud-Computing werden in der Praxis aber nur dann zu realisieren sein, wenn eine stringente Cloud-Strategie verfolgt und umgesetzt wird. Außerdem eignet sich nicht jede Art von Problem gleichermaßen für die Anwendung der Cost-Associativity (vgl. Abschnitt 2.3.3). Für die ersten Gehversuche in der Cloud sollten die Ziele daher in dieser Hinsicht nicht zu hoch gesteckt werden, um keine unnötige Enttäuschung zu erleben.

3.1.2 Technische Dimension

Obgleich viele der beworbenen Vorteile von Cloud-Computing wirtschaftlicher Natur sind, gibt es trotzdem auch einige technische Vorteile, insbesondere die Elastizität und Leistungsfähigkeit der Cloud-Infrastruktur. Zudem gibt es einige neue technische Aspekte, die beachtet werden wollen, die zum einen mit der eingesetzten Virtualisierung zusammen hängen und die sich andererseits aus neuen Technologien wie NoSQL-DBS ergeben. Als häufigster technischer Aspekt wird jedoch die Sicherheit der Cloud-Lösung angezweifelt, weswegen diese zuerst kurz behandelt wird.

Sicherheit der Cloud

Cloud-Anbieter legen gezwungenermaßen sehr hohe Maßstäbe für die Sicherheit und Leistungsfähigkeit der eigenen Systeme an. Entsprechend stehen mehr Ressourcen und besser geschulte Mitarbeiter zur Verfügung, die sich ein KMU in der Regel nicht leisten kann. Zumindest bei den etablierten Anbietern kann daher von einem sehr hohen Sicherheitsstandard ausgegangen werden, der dem eines eigenen Rechenzentrums in nichts nachsteht. Insbesondere im Hinblick auf die Abwehr von Denial-of-Service-Angriffen, die durch die zunehmende Kommunikation über öffentliche Netze an Bedeutung gewinnen, sind etablierte Cloud-Anbieter üblicherweise sehr viel besser gerüstet als ein traditionelles Rechenzentrum.

Zwar müssen die Daten, die in der Cloud verarbeitet werden sollen, in der Regel über unsichere Netze an den Anbieter gesendet werden. Bei den allermeisten Anbietern lässt sich aber bereits durch einfache Maßnahmen, wie der Verwendung des SSL-Protokolls, ein akzeptables Maß an Sicherheit gewährleisten. Die pauschale Befürchtung, durch Cloud-Computing nähme die Sicherheit grundsätzlich ab, ist schlicht falsch. Bei kleineren Unternehmen mit weniger professionellem IT-Personal kann sogar leicht das Gegenteil der Fall sein. Kapitel 5 widmet sich im Detail den verschiedenen Aspekten der Sicherheit.

Elastizität und Leistungsfähigkeit der Infrastruktur

Die Elastizität von Cloud-Diensten gibt dem Kundenunternehmen die Möglichkeit, Ressourcen bei Bedarf dynamisch hinzuzufügen und wieder freizugeben. Mögliche Projektziele hängen somit nicht mehr davon ab, ob genügend Rechenleistung oder Speicherkapazität vorhanden ist.

Dieser Vorteil wird allerdings hauptsächlich für IaaS und mit Einschränkungen PaaS relevant. Dienste auf SaaS-Ebene bieten eher selten nennenswerte Chancen in dieser Hinsicht.

Für alle drei Servicemodelle gilt jedoch, dass die Cloud-Infrastruktur tendenziell mindestens so leistungsfähig ist, wie die Infrastruktur im eigenen Rechenzentrum. Besonders aufgrund ausbleibender Investitionen in Hardware, die viele KMU z. B. aufgrund der unklaren Kosten-Nutzen-Bilanz scheuen, wird in den Unternehmen oft ältere oder sogar veraltete Hardware eingesetzt. Diese Hardware kann Ausfälle oder starke Schwankungen in der Last nicht so gut abfangen, wie die hochverfügbare Infrastruktur im Rechenzentrum des Cloud-Anbieters. Tendenziell lässt sich also festhalten, dass sowohl die Leistungsfähigkeit der Infrastruktur als auch die Flexibilität im Hinblick auf den Ressourceneinsatz durch Cloud-Computing verbessert wird.

Virtualisierung

Als weiterer technischer Vorteil wird der Einsatz von Virtualisierungstechnologie in der Cloud angeführt. Zwar ist ein solcher Einsatz an sich erst einmal nur für den Anbieter von Nutzen und nicht so sehr für den Kunden. Es entstehen aber auch einige positive Nebeneffekte für den Cloud-Anwender. Während der Cloud-Anbieter die Virtualisierung eher deshalb einsetzt, um seine physische Infrastruktur ausreichend hoch auszulasten, kann der Kunde von der Virtualisierung profitieren, weil sie eine Abstraktionsschicht zwischen der Dienstimplementierung und der Kundenanwendung bildet. Im Falle von IaaS kann der Cloud-Nutzer so z. B. standardisierte, virtuelle Ressourcen beziehen ohne sich um die konkrete Realisierung zu kümmern. Der Anbieter kann die zugrunde liegende Hardware beliebig tauschen und sogar grundlegend ändern, solange die Abstraktionsschicht unberührt bleibt. Im Fall von PaaS und SaaS bleibt die zugrunde liegende Software-Schnittstelle unverändert, selbst wenn der Anbieter die Implementierung neu konzipiert. Der wirkliche Vorteil der Virtualisierung für den Kunden liegt also in der Standardisierung der Ressourcen. Im Endeffekt ist zu erwarten, dass die Standardisierung sogar über Anbieter hinweg stattfindet und z. B. eine standardisierte CPU-Stunde bei einem beliebigen Anbieter eingekauft werden kann. Dieser Zustand ist jedoch noch nicht absehbar, selbst wenn viele Cloud-Anbieter und -Nutzer ihn sich wünschen.[1]

NoSQL-Datenbanken

Besonders im Hinblick auf DaaS gibt es in der Cloud eine weitere interessante Entwicklung: Große Vorreiter der Cloud, vornehmlich Amazon und Google, sind von den traditionellen RDBS abgerückt hin zu den neu aufgekommenen *NoSQL-DBS*. Dabei handelt es sich nicht zwangsläufig um DBS, die überhaupt keine SQL-Anweisungen mehr verarbeiten können, sondern man interpretiert diesen Bezeichner als *Not only SQL*. Es gibt verschiedene Typen dieser NoSQL-DBS, wobei die bekanntesten die folgenden sind:

- dokumentenorientierte DBS, wie MongoDB oder CouchDB
- Key-Value-Stores, wie Memcached oder SimpleDB
- spaltenorientierte Speicher, wie BigTable oder HBase
- Graph-Datenbanken, wie AllegroGraph oder Neo4j

[1] Vgl. `http://opencloudmanifesto.org/`.

Allen NoSQL-DBS ist gemein, dass sie dem relationalen Modell den Rücken kehren, um horizontale Skalierbarkeit zu erreichen, die in der Cloud eine sehr viel größere Bedeutung erlangt als zuvor (vgl. hierzu Abschnitte 2.3.2 und 2.3.3). Je nachdem, welche Funktionalität in die Cloud ausgelagert werden soll, kann es sinnvoll sein, sich vom klassischen relationalen Modell zu lösen und sich auf die neuen Technologien einzulassen. Da diese speziell für die Cloud entwickelt wurden, können mit ihnen die Vorteile deutlich effektiver ausgenutzt werden.

Problematische Anbindung an andere Systeme

Die erfolgreichsten Cloud-Projekte, mit denen die Anbieter werben, sind normalerweise solche, die ausschließlich mit einem Dienst oder zumindest durch einen Anbieter realisiert wurden. Das ist leicht erklärlich, denn ein Hauptproblem, das nach wie vor ungelöst ist, besteht in der Kopplung der neuen Cloud-Dienste mit einander und insbesondere mit bestehenden Systemen. Zum einen ist der bereits thematisierte Transport der Daten zwischen den Systemen problematisch (vgl. Abschnitt 2.3.3). Zum anderen erschweren aber verschiedene weitere Hürden den Erfolg; die wichtigsten Hürden sind dabei:

- Die Anbieter offerieren häufig nur eine einzige, proprietäre Schnittstelle zu dem Cloud-Dienst. Oft basiert diese auf dem REST-Paradigma (oder ist zumindest daran angelehnt). Diese Wahl erschwert es, die neuen Dienste mit älteren Systemen zu koppeln, wenn diese noch nicht für die Kommunikation mit dieser Art von API ausgelegt sind.
- Der Cloud-Dienst bietet nur beschränkte Im- und Export-Möglichkeiten, so dass nicht alle benötigten Daten automatisch eingespielt oder ausgelesen werden können.
- Die bestehenden Systeme im Unternehmen bieten keine Schnittstellen für eine Kopplung mit anderen Diensten, sondern lediglich Batchfunktionen für Import bzw. Export.
- Die transaktionsorientierte Natur der bestehenden Systeme ist inkompatibel mit der neuen Idee der Eventual Consistency bzw. mit der Möglichkeit, dass ein anderes System, z. B. aufgrund von Netzwerkproblemen, nicht erreichbar ist.

Zur Ehrenrettung der bestehenden Systeme sollte aber auch gesagt werden, dass selbst die Kopplung zwischen zwei Cloud-Diensten aus denselben oder ähnlichen Gründen bei weitem nicht immer reibungslos funktioniert. Insgesamt bleibt daher festzuhalten, dass die geplante Anbindung an andere Systeme sehr genau geprüft werden muss, bevor der Schritt in die Cloud vollzogen wird.

3.1.3 Rechtliche Dimension

Aus juristischer Perspektive ist das Auslagern von Funktionalität in die Cloud ganz ähnlich zum klassischen IT-Outsourcing zu behandeln, da es sich beim Cloud-Computing ja im Wesentlichen um ein solches handelt. Jedoch verschärft sich die rechtliche Situation insofern, als dass die Transparenz der Cloud-Lösung deutlich niedriger ist als im klassischen IT-Outsourcing-Szenario. Während bei klassischen Outsourcing-Verträgen oft das genaue Rechenzentrum bezeichnet wird, in dem die Datenverarbeitung stattfindet, ist bei Standardverträgen zu Cloud-

Diensten noch nicht einmal festgelegt, in welchem Teil der Erde sich die Daten befinden werden. Daher müssen bei Cloud-Diensten einige Aspekte besonders beachtet werden.

Zudem ist zu bemerken, dass viele rechtlichen Aspekte noch nicht final geklärt sind. So ist z. B. das Problem einer Haftung für Vermögensschäden im Fall eines Fehlers durch den Anbieter noch offen. Denkbar wäre beispielsweise der Fall, dass die Berechnung von Finanzdaten fehlerhaft geschieht. Wer haftet und wie kann ein Fehler nachgewiesen werden, wenn der Cloud-Dienst falsche Ergebnisse liefert? Auch die Problematik der Reproduzierbarkeit bzw. Nachvollziehbarkeit von wichtigen Berechnungen, wie dem Jahresabschluss, ist noch unklar. Hier benötigt man oft die Möglichkeit, die Herkunft der Daten (*Data-Provenance*) oder den Berechnungsweg (*Data-Lineage*) nachzuweisen. An dieser Stelle soll daher nur eine Auswahl der wichtigsten Handlungsempfehlungen aus Sicht zahlreicher Praktiker vorgestellt werden [3].

- Die Rechtsabteilung und die für die Vertragsgestaltung zuständigen Mitarbeiter müssen frühzeitig miteinbezogen werden. Viele Standardverträge der Cloud-Anbieter werden den Anforderungen des eigenen Unternehmens nicht gerecht werden, so dass die entsprechenden Fachleute direkt auf problematische Klauseln oder Aspekte hinweisen und entsprechende Verbesserungen vorschlagen können. Auch grundsätzliche rechtliche Probleme mit dem Auslagern bestimmter Systeme können so rechtzeitig erkannt werden.

- Die Rechtsabteilung muss ebenfalls frühzeitig zusammen mit den betroffenen Fachabteilungen untersuchen, in welchem Ausmaß das Auslagern in die Cloud juristische Regularien und interne Vorgaben berührt. Zumindest die Gesetzgebung zum Datenschutz ist für die meisten Cloud-Projekten relevant. Damit einher gehen in der Regel auch Anforderungen an die Datensicherheit (vgl. Kapitel 5). Eventuell werden auch gesetzliche Vorgaben zur eingesetzten Infrastruktur oder zur Kontrolle über diese gemacht. In diesem Fall muss überprüft werden, ob es Cloud-Anbieter gibt, die diese Vorgaben erfüllen können.

- Da die Cloud für den Kunden bewusst undurchsichtig gestaltet wird, um die oben beschriebenen Vorteile der Abstraktion zu erlangen, sollten Maßnahmen zur teilweisen Aufhebung dieser Intransparenz vorgesehen werden. Hier könnte die aus klassischen IT-Outsourcing-Verträgen bekannte Überprüfungsklausel (*Right-to-Audit-Klausel*) helfen, die es dem Cloud-Nutzer ermöglicht, die Rechenzentren des Providers vor Ort zu überprüfen. Oft wird von dieser Möglichkeit zwar kein Gebrauch gemacht, aber sie kann helfen, eine Vertrauensbeziehung zwischen den Parteien aufzubauen. Besser noch als eine solche Klausel sind natürlich einschlägige Zertifikate externer Gutachter, die der Cloud-Anbieter vorweisen kann. Hier ist insbesondere die Zertifizierung nach ISO/IEC 27001 zu nennen.

- Wenn die Zertifizierung nach ISO/IEC 27001 noch nicht erfolgt ist, sollte zumindest der strategische Plan des Anbieters in Bezug auf diese Zertifizierung erfragt werden. Zusätzlich kann hilfsweise auch die Umsetzung von ISO/IEC 27002 demonstriert werden.

- Genauso wichtig wie die Analyse des tatsächlichen Cloud-Anbieters ist die Untersuchung der vorgelagerten Dienstleister desselben. Zum einen ist dies für die eigene Einschätzung

der Zuverlässigkeit sinnvoll. Zum anderen kann das aber auch durch gesetzliche Anforderungen erforderlich werden, wenn z. B. die Daten zur Verarbeitung noch an weitere Dienstleister übergeben werden.

- Im Vertragswerk sollte eine klare Vereinbarung über die jeweiligen Zuständigkeiten der Parteien getroffen werden, damit klar ist, welche Partei welche Aufgaben (z. B. Sicherung der Daten) wahrnehmen muss.

- Durch Rechts- und Fachabteilungen muss geklärt werden, wie der Nachweis über die Erfüllung der gesetzlichen Normen statt finden könnte. Es muss ein Prozess installiert werden, der die Sammlung von z. B. Log-Dateien oder Aktivitätsberichten formalisiert und mit dessen Hilfe ein juristisch ausreichend sicherer Nachweis über die Erfüllung der verschiedenen Anforderungen möglich ist. Viele dieser Informationen kann nur der Cloud-Provider liefern, was im Vorfeld geklärt werden muss.

Es bleibt zu bemerken, dass ein Cloud-Computing-Projekt aus rechtlicher Sicht keine Vorteile sondern eher zusätzliche Problemstellungen mit sich bringt. Insofern sollten die Vorteile aus technischer und wirtschaftlicher Sicht verglichen werden mit den zusätzlichen Problemen, die auf der juristischen Dimension aufkommen. Je nachdem, wie kooperativ der Cloud-Anbieter in dieser Hinsicht ist, kann sich diese Dimension derzeit leider als K.O.-Kriterium für das Cloud-Projekt erweisen. Insbesondere durch die sehr restriktive Datenschutzgesetzgebung in Deutschland kann es zu Problemen kommen, wenn der Cloud-Anbieter Daten in einem Land mit laxeren Vorgaben verarbeiten lässt.[2] Weitere Aspekte hierzu werden in Abschnitt 4.3 diskutiert. Das rechtliche Risiko nimmt allerdings stark ab, wenn bereits Präzedenzfälle existieren, in denen andere Unternehmen in vergleichbarer Situation ähnliche Lösungen realisiert haben. Dann ist – gesetzt den Fall, dass die Lösungen schon eine Weile existieren – davon auszugehen, dass das entsprechende Risiko stark reduziert ist.

3.1.4 Organisatorische Dimension

Aus organisatorischer Sicht ist die Cloud-Nutzung nahezu identisch mit einem klassischen IT-Outsourcing. Sind entsprechende Prozesse bereits im Unternehmen installiert, so muss für eine Verwaltung der Cloud-Dienste nur eine entsprechende Erweiterung stattfinden. Wichtiger als beim klassischen Modell ist in der Cloud allerdings, dass regelmäßig geprüft wird, ob es inzwischen einen günstigeren Anbieter gibt. Da sich der Markt noch stetig wandelt, kann es leicht sein, dass neue, besser passende Angebote auftauchen oder dass andere Anbieter identische Dienstleistungen zu deutlich niedrigeren Preisen anbieten. Für solche Fälle sollte ein strukturiertes Vorgehen vorgesehen werden, um die Möglichkeit eines Anbieterwechsels zu erörtern. Dazu bietet es sich an, die Dokumentation der ursprünglichen Anbieterwahl zu Rate zu ziehen, um die damals ausschlaggebenden Punkte der Reihe nach zu prüfen und so bereits einen Kriterienkatalog für den Vergleich verschiedener Produkte an der Hand zu haben.

[2] Eine grafische Übersicht über die verschiedenen Datenschutzniveaus bietet `http://forrester.com/cloudprivacyheatmap`.

Auch die technische Betreuung der Systeme ist aus Sicht des Systemadministrators so gut wie identisch zur Verwaltung der physischen Systeme im eigenen Rechenzentrum. Abgesehen davon, dass nun keine physische Box mehr im Serverraum steht, werden auch Cloud-Systeme mit denselben Fernwartungsprogrammen und Werkzeugen verwaltet wie lokale Systeme. Verwendet man z. B. virtuelle Maschineninstanzen in der Cloud, so werden diese genauso verwaltet wie virtuelle Maschinen im eigenen Haus. Im Fall eines relationalen Cloud-DBS hat der Administrator zwar weniger Eingriffsmöglichkeiten in die Konfiguration des Datenbank*management*systems per se (z. B. Nutzung des Hauptspeichers, Größen von Pufferspeichern), aber die Verwaltung innerhalb des RDBS bleibt wie gehabt (z. B. Benutzerrechteverwaltung, Anlegen von Datenbanken und Relationen) [18].

Die Verwaltungsfunktionen werden dabei je nach Art des bezogenen Dienstes entweder durch die virtualisierte Anwendung (IaaS, PaaS) oder durch eine Web-Oberfläche des Anbieters (SaaS, PaaS) durchgeführt. Zudem stellen Drittanbieter bereits Werkzeuge zur Überwachung der Clouds anderer Anbieter bereit, mit deren Hilfe Ausfälle oder Leistungseinbrüche erkannt werden können. Als kleine Auswahl dieser Anbieter – ohne Anspruch auf Vollständigkeit – seien folgende Dienste genannt (alle Angaben mit Stand August 2010):

- **CloudSleuth**[3] visualisiert die Zuverlässigkeit und Verfügbarkeit der populärsten IaaS- und PaaS-Anbieter, indem von zurzeit 50 Standorten in den USA und 75 internationalen Standorten auf die jeweiligen Dienste zugegriffen wird.

- **CloudHarmony**[4] führt Tests zur Leistungsfähigkeit durch, indem die Geschwindigkeit und Latenzzeit für ein- und ausgehenden Datenverkehr gemessen wird. Im Blog werden außerdem weitere Analysen publiziert, die sich unter anderem mit CPU-Leistung oder Datendurchsatz befassen.

- **Cloudstone**[5] ist eine Desktop-Anwendung zur Analyse von Cloud-Computing- und Web-2.0-Diensten. Dazu erzeugt Cloudstone künstliche Serverlast und berechnet entsprechende Kennzahlen. Das Projekt stellt zwar aktuell keine Ergebnisse zur Verfügung, mit der Anwendung können aber eigene Analysen durchgeführt werden.

- **Cloud CMP**[6] schickt nach eigenen Angaben „Clouds gegeneinander in den Ring“. Dabei werden die Leistungsfähigkeit von Rechenleistung, Speicher und Netzwerk verglichen. Als Resultat wird unter anderem ermittelt, was der Betrieb einer bestimmten Applikation bei einem bestimmten Cloud-Anbieter kosten würde.

- **CloudFail.net**[7] gibt Auskunft über Ausfälle und Störungen verschiedener Cloud-Anbieter. Dazu aggregiert der Dienst verschiedene RSS-Feeds, unter anderem von Amazon, Google und Rackpace. Auch Web-2.0-Dienste wie Twitter, die streng genommen keine Cloud-Dienste sind, sind berücksichtigt.

[3] http://www.cloudsleuth.net/
[4] http://www.cloudharmony.com/
[5] http://radlab.cs.berkeley.edu/wiki/Projects/Cloudstone
[6] http://cloudcmp.net/
[7] http://cloudfail.net/

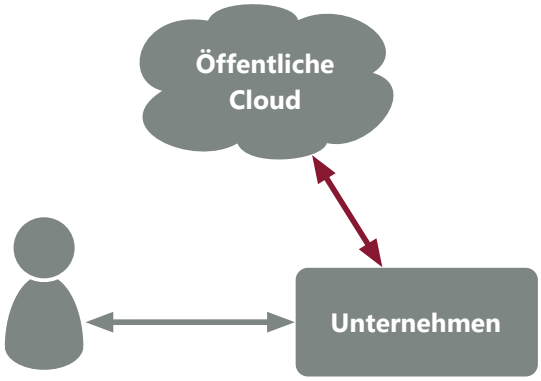

Abbildung 3.2: Schematische Darstellung des Szenarios KMU ↔ Cloud.

- **Cloutage.org**[8] hilft bei der Einschätzung der Sicherheit verschiedener Cloud-Dienste. Das Projekt möchte eine einheitliche Anlaufstelle für bekannte und veröffentlichte sicherheitsrelevante Vorfälle (Incidents) in der Cloud werden.

Diese oder vergleichbare Werkzeuge sollten bei der regelmäßigen Beurteilung der Cloud-Anbieter zur Hilfe gezogen werden.

3.2 Typische Szenarien für Cloud-Nutzung durch KMU

Aus den Diskussionen der *Cloud Use Case Group*, einer offenen Interessengemeinschaft aus Cloud-Anbietern und -Nutzern, sind verschiedene Szenarien für die Cloud-Nutzung entstanden, welche in einem regelmäßig aktualisierten Dokument [28] bereitgestellt werden. Diejenigen Szenarien, die für KMU am wahrscheinlichsten sind, werden im Folgenden zusammen mit den jeweiligen Implikationen kurz vorgestellt.

3.2.1 Szenario 1: KMU ↔ Cloud

In diesem Szenario nutzt ein KMU Cloud-Services in seinen internen Prozessen (vgl. Abbildung 3.2). Die Dienste werden also nur von den Mitarbeitern des Unternehmens einsetzt. Kunden kommen nicht mit der Cloud in Berührung. Dies ist zu Anfang vermutlich das häufigste Szenario für die Cloud-Nutzung [28], da sich die Unternehmen so erst einmal intern mit den neuen Cloud-Diensten vertraut machen können, bevor diese für die Kunden freigegeben werden. Ein Unternehmen kann in diesem Szenario beispielsweise Speicherplatz für die Datensicherung in der Cloud einsetzen, virtuelle Maschinen auf Cloud-Infrastruktur zur Erweiterung der Rechenkapazitäten und Befriedigung von Bedarfsspitzen bereitstellen oder Cloud-Anwendungen für bestimmte Unternehmensprozesse (z. B. E-Mail, Kalender, CRM, Kollaboration, usw.) einsetzen. Insbesondere können aber auch Cloud-Datenbanken im Rahmen der Datenverarbeitung

[8] http://cloutage.org/

im Unternehmen verwendet werden, um z. B. Daten mit Vertragspartnern oder sogar Regierungsstellen auszutauschen.

Die wichtigsten Anforderungen, die sich aus diesem Szenario ergeben, sind:

Identität und Identitätsverwaltung Der Cloud-Service muss den Benutzer authentifizieren. Ein Benutzer, der einem Unternehmen angehört, hat häufig schon eine Identität innerhalb dieses Unternehmens. Daher sollte diese Identität möglichst auch für den Zugriff auf die Cloud-Dienste verwendet werden, z. B. im Rahmen eines Single Sign On (SSO). Gegebenenfalls sind weitere Sicherheitsanforderungen z. B. zum Schutz der Privatsphäre des Benutzers zu beachten.

Offener Zugriff Die Nutzung des Cloud-Services sollte keine bestimmte Plattform oder Technologie benötigen, die den Zugriff auf den Cloud-Service einschränkt, denn dies würde dem Cloud-Gedanken entgegen wirken.

Ortsbezug Ein Grundprinzip des Cloud-Computings lautet zwar, dass die physische Realisierung des Dienstes vor dem Benutzer verborgen bleibt. In einigen Situationen kann es jedoch notwendig werden, den genauen Ort der physischen Ressourcen zu kennen. Wenn beispielsweise Daten Ländergrenzen überschreiten, können dadurch ungewollte juristische Konsequenzen entstehen. Es sollte deshalb für ein Unternehmen immer nachvollziehbar bleiben, in welchen Rechenzentren ihre Daten und Anwendungen geografisch aufzufinden sind. Der Cloud-Anbieter könnte hierzu beispielsweise eine API bereitstellen.

Verbrauchsmessung und Überwachung Für alle Cloud-Services ist dringed zu empfehlen, dass sie während ihrer Ausführung überwacht und bezüglich ihrer Ressourcenverwendung gemessen werden. Dadurch kann zum einen die Dienstnutzung abgerechnet werden. Zum anderen können Vertragsverletzungen und Sicherheitsprobleme oder Störungen im Betriebsablauf festgestellt werden. Die Messgrößen sollten im Vorfeld im Rahmen eines SLA vereinbart werden.

Service-Level-Agreements (SLAs) Unternehmen benötigen die Möglichkeit, SLAs kontinuierlich zu überwachen (siehe vorherigen Punkt). In einem SLA muss eindeutig festgehalten werden, was der Cloud-Anbieter liefern wird und wie dies gemessen wird. Dabei ist es wichtig, dass eine ausreichendes Abstraktionsniveau für die Messgrößen gewählt wird. Wünschenswert aus Nutzersicht sind tendenziell eher fachliche Größen („Transaktion“, „Vorgang“, „Datensatz“) und nicht so sehr technische („Gigabyte“, „CPU-Stunde“, „Stromverbrauch“), da sich so das Verhalten und die Kosten der Nutzung des Dienstes aus der betriebswirtschaftlichen Sicht ableiten lassen.

Sicherheit Wie bereits erwähnt, stellt die Sicherheit von Cloud-Services eine große Herausforderung dar. Anforderungen bezüglich der Sicherheit müssen die fünf Cloud-Charakteristika berücksichtigen. Die Sicherheitsaspekte werden im weiteren Verlauf, insbesondere in Abschnitt 5, detailliert betrachtet.

Interoperabilität und Portabilität Es sollte möglich sein, Anwendungen, Daten und virtuelle Maschinen zwischen den verschiedenen Systemen der Cloud-Anbieter zu portieren. Dazu bedarf es einer Menge an standardisierten Schnittstellen für den Zugriff auf die Services, wie beispielsweise Speicherdienste oder Middleware- bzw. Plattformdienste. Im Kontext von PaaS und IaaS sind auch Hilfsmittel relevant, die eine vom Anbieter unabhängige Bereitstellung der Applikation oder Infrastruktur ermöglichen (indem sie z. B. die verschiedenen APIs kompensieren). Dadurch werden Lock-in-Effekte vermieden und Cloud-Services verschiedener Anbieter verknüpfbar. Allerdings ist zu bemerken, dass heutige Systeme – insbesondere im Bereich DaaS – noch bei weitem nicht ausreichend standardisiert sind [14]. Im Gegenteil scheint der Fokus derzeit noch auf Diversifikation zu liegen.

Verteilung Eng mit der Interoperabilität und Portabilität verknüpft ist die Verteilung der Anwendungen und Daten. Unter Umständen müssen komplexe Systeme mit zahlreichen beteiligten Cloud-Diensten koordiniert werden. Diese Koordination kann durch Werkzeuge des Anbieters oder auch externe Dienste unterstützt werden (vgl. Abschnitt 3.1.4). Anforderungen bei der Verteilung können auch extern durch die juristischen Rahmenbedingungen vorgegeben sein.

Lebenszyklusverwaltung Unternehmen müssen auch bei der Nutzung von Cloud-Diensten die Möglichkeit haben, den Lebenszyklus ihrer Anwendungen, Daten oder Identitäten verwalten zu können. Dazu werden entsprechende Prozesse und Sicherheitsmechanismen gefordert, die dies unterstützen und nachvollziehbar umsetzen. Im Rahmen von DaaS spielen z. B. Aufbewahrungspflichten oder kontrollierte Löschverfahren für Daten eine Rolle.

Governance Anbieter von öffentlichen Clouds setzen die Einstiegsbarrieren absichtlich möglichst niedrig an, so dass es sehr einfach ist, sich ein Benutzerkonto zu eröffnen und die Dienste zu nutzen. Diese Einfachheit birgt jedoch Risiken, da Mitarbeiter des Unternehmens am geregelten IT-Prozess vorbei Cloud-Dienste beziehen können. So können sie sehr leicht z. B. sensible Daten „in die Cloud“ transferieren. Es ist daher wichtig, durch Governance verbindliche Regeln und Vorgehensweisen zu etablieren. Die Governance-Anforderungen sollten in einem Sicherheitskonzept berücksichtigt werden.

Industriespezifische Standards und Protokolle Werden Cloud-Dienste zur Bereitstellung von branchenspezifischer Funktionalität benutzt, so sind bestehende Industriestandards und Protokolle zu berücksichtigen. Diese branchenspezifischen Anforderungen sind sehr vielfältig und werden i. d. R. am besten vom Unternehmen selbst verstanden, so dass sie in diesem Leitfaden nicht weiter vertieft werden.

3.2.2 Szenario 2: KMU ↔ Cloud ↔ Endkunde

Eine Variante des ersten Szenarios ist die Verwendung von Cloud-Diensten durch ein Unternehmen mit dem Ziel, diese Dienste nicht nur für die unternehmensinternen Prozesse einzusetzen, sondern sie auch externen Akteuren wie beispielsweise Geschäftspartnern oder Endbenutzern

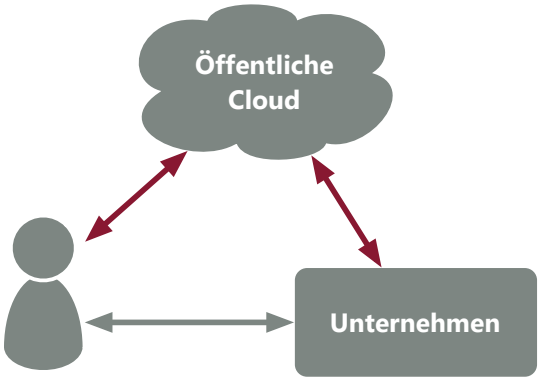

Abbildung 3.3: Schematische Darstellung des Szenarios KMU ↔ Cloud ↔ Endkunde.

zur Verfügung zu stellen (vgl. Abbildung 3.3). Ein typischer Fall für dieses Szenario ist die Auslagerung der Web- und Datenbankserver in die Cloud, so dass die Website des Unternehmens von der Elastizität der Cloud-Infrastruktur profitieren kann. Doch auch andere Konstellationen sind denkbar, wenn z. B. große Filme durch den Kunden direkt von Amazon S3 heruntergeladen werden sollen oder eine SaaS für die Durchführung einer Umfrage verwendet wird.

Durch die Beteiligung einer zusätzlichen, nicht vertrauenswürdigen Partei verkompliziert sich das Szenario leicht. Im Wesentlichen müssen die Mechanismen, die den Zugriff auf die Dienste und Ressourcen regeln etwas ausgefeilter sein, um eine feinere Abstimmung der Rechte zu erlauben. Auch kann der Zugriff auf die Dienste nicht einfach z. B. auf ein IP-Subnetz begrenzt werden, so dass eine etwas größere Angriffsfläche entsteht. Im Endeffekt treffen aber alle Überlegungen aus dem ersten Szenario unverändert zu und es kommen keine grundlegenden Problemstellungen hinzu. Lediglich ist zu beachten, dass ein Ausfall, ein Konfigurationsfehler oder eine falsche Bedienung des Cloud-Systems jetzt nicht nur interne Konsequenzen hat, sondern auch durch den Kunden wahrgenommen wird. Insofern ist dieses Szenario riskanter für den guten Ruf des Unternehmens, wenn noch keine ausreichende Cloud-Erfahrung vorhanden ist.

3.3 Entwicklung einer Cloud-Strategie und deren Umsetzung

Nachdem nun die verschiedenen Chancen und Risiken des Cloud-Computing geklärt wurden, stellt sich die Frage nach der Entscheidung für oder gegen die Cloud. Der erste und wichtigste Schritt dabei ist die Entwicklung einer *Cloud-Strategie* für das Unternehmen auf Managementebene. Die Strategie definiert, welche Geschäftsbereiche oder -prozesse „in die Cloud verlagert“ bzw. durch Cloud-Dienste unterstützt werden sollen. Ebenso wird definiert, für welche Bereiche oder Prozesse Cloud-Computing *nicht* einzusetzen ist. Das Management muss zudem im Vorfeld entscheiden, welche Risiken abzusichern sind und welche auf keinen Fall eingegangen werden dürfen. Erst nachdem auf Managementebene eine klare Strategie entwickelt wurde,

kann mit den weiteren Schritten in Richtung Cloud-Computing fortgefahren werden. Naturgemäß spielen bereits hierbei Sicherheitsaspekte eine entscheidende Rolle. Diese werden in Kapitel 5 aufgegriffen und erläutert.

Die Cloud-Strategie dient als Basis für das weitere Vorgehen. Für die Umsetzung der Strategie empfiehlt sich ein klar definiertes Vorgehen bestehend aus den fünf Phasen, die in Abbildung 3.4 auf Seite 40 dargestellt und erläutert werden.

Zudem muss für das weitere Vorgehen sichergestellt sein, dass einerseits die notwendigen Verantwortlichkeiten klar zugewiesen werden, dass andererseits aber auch alle betroffenen Parteien wie Management, Rechtsabteilung, Betriebsrat, Datenschutzbeauftragte, Sicherheitsbeauftragte und Fachabteilungen von Anfang an einbezogen werden. Es sollte explizit ein Sicherheitsbeauftragter für die Cloud-Systeme benannt werden, der sowohl während des Aufbaus als auch später während des Betriebs zuständig bleibt (vgl. [33]).

3.4 Zusammenfassung

In diesem Kapitel wurden die wichtigsten Neuerungen, die Cloud-Computing mit sich bringt, sowie die resultierenden Vor- und Nachteile einer Cloud-Lösung dargestellt. Tatsächlich ist es gerade bei kleineren Unternehmen aber häufig so, dass nicht die rationalen Abwägung der positiven und negativen Aspekte den Ausschlag gibt, sondern die Grundhaltung eines Entscheidungsträgers [16]. Kommt ein Unternehmen jedoch nach Abwägung der grundsätzlichen Vor- und Nachteil und nach Berücksichtigung aller Ausschlusskriterien zu dem Schluss, dass Cloud-Computing geeignet ist, so bietet das folgende Kapitel 4 Hilfestellung bei der Auswahl des Cloud-Anbieters. Vorher sollen aber die wichtigsten Aspekte der Grundsatzentscheidung in Form von zehn Leitfragen formuliert werden, die als erste Hilfestellung bei der Entscheidung für oder wider die Cloud genutzt werden können.

Abbildung 3.4: Vorgehen bei der Umsetzung der Cloud-Strategie.

Zehn Leitfragen zur Grundsatzentscheidung

1. Gibt es grundsätzliche Vorbehalte, das System auszulagern, bzw. wäre ein klassisches Outsourcing des Systems denkbar?
2. Was genau soll ausgelagert werden und durch welche Art von Cloud-Ressourcen soll die Auslagerung realisiert werden?
3. Handelt es sich bei der auszulagernden Funktionalität um eine, die das Kerngeschäft des Unternehmens direkt betrifft, oder um eine unterstützende, „nicht-vitale“?
4. Welche speziellen rechtlichen (und ggf. internen) Rahmenbedingungen müssen beim Auslagern des Systems eingehalten werden?
5. Benötigt die Anwendung eher einen intensiven Datenaustausch zwischen Cloud und Unternehmen oder funktioniert sie eher isoliert? In anderen Worten: Befinden sich Daten und Logik am selben Ort?
6. Wie ist die Last des Systems zu charakterisieren? Gibt es nennenswerte regelmäßige oder unvorhersehbare Schwankungen? Wie ist das Verhältnis von Lastspitzen zur durchschnittlichen Last?
7. Profitiert die Anwendung von „Elastizität“, d. h., ist sie (bevorzugt horizontal) skalierbar?
8. Soll ein bestehendes System ausgelagert und durch einen Cloud-Dienst ersetzt werden oder soll neue Funktionalität durch die Cloud bereitgestellt werden? Müsste im letzteren Fall für die Einführung im eigenen Unternehmen neue Hardware oder Software angeschafft werden?
9. Hat das System eine beschränkte Lebensdauer, z. B. durch ein klar definiertes Projektende?
10. Gibt es bereits Präzendenzfälle am Markt, in denen Unternehmen in vergleichbarer Situation ähnliche Lösungen realisiert haben?

4 Auswahl eines DaaS-Anbieters

Das Wichtigste in Kürze

- Bei der Auswahl des Anbieter müssen alle vier Dimensionen des Cloud-Computing betrachtet werden.
- **Wirtschaftlich** spielen die Reputation des Anbieters, sein Preismodell und die zu erwartenden Lock-in-Effekte die wichtigste Rolle.
- **Technisch** muss vor allem auf die Datensicherung, die Leistungsfähigkeit der Cloud und die Integration in bestehende Anwendungen geachtet werden.
- **Rechtlich** ist zu klären, ob der Anbieter alle relevanten Regularien erfüllt. Ebenfalls zu klären sind Ausstiegsszenarien und z. B. Preisänderungen während der Vertragslaufzeit.
- **Organisatorisch** ist ein strukturiertes Vorgehen zur Anbieterauswahl inklusive Dokumentation gefordert. Wichtige Aspekte dieser Dimension sind die Support-Leistungen und die Kommunikation mit dem Anbieter.

Inzwischen gibt es eine Vielzahl von Anbietern, die sich als Cloud-Anbieter positionieren möchten. Ebenso vielfältig wie die Anbieter sind leider auch die Angebote, da die Anbieter im sich entwickelnden Markt noch keine optimale Preis- und Produktstrategie gefunden haben und folglich an vielen Stellen noch experimentieren. Obwohl viele Services im Wesentlichen also dieselbe Funktionalität erbringen, gibt es de facto keine zwei, die sich gleichen. Die Anbieter locken die IT-Manager daher auch mit sehr kurzen Vertragslaufzeiten, so dass ein recht gefahrloses Ausprobieren der Dienste möglich ist. Allerdings sollten die IT-Verantwortlichen trotzdem ein diszipliniertes Vorgehen in Bezug auf die Evaluation und Auswahl des Cloud-Anbieters an den Tag legen, damit nicht plötzlich böse Überraschungen drohen.

Die Anbieter werben mit wohlklingenden Zahlen zu Stabilität und Verfügbarkeit ihrer Dienste oder locken mit der gebotenen „Elastizität“. Obschon diese Aspekte für die Auswahl des Cloud-Dienstes wichtig sind, sollte die Entscheidung für oder gegen einen Anbieter immer durch eine ganzheitliche Betrachtung begründet werden und besonders berücksichtigen, wie gut sich das Cloud-Angebot in die bestehende IT-Architektur einfügt. Weitere Punkte, die meist nicht ausdrücklich beworben werden, aber äußerst relevant für die Entscheidung sein sollten, sind die Support-Leistungen des Anbieters, das garantierte Serviceniveau, Sicherheitsaspekte sowie Datenschutz- und Compliance-Anforderungen.

Auch nachdem der Markt für Cloud-Services sich nun schon seit einiger Zeit entwickelt, gilt immer noch: Jeder Cloud-Dienst ist ein wenig anders. Jeder Dienst hat eine eigene Architektur für die Systeme, das Netzwerk, die Speicherhierarchie sowie andere Preismodelle, Support-Angebote und Sicherheitsmerkmale. Außerdem unterscheidet sich die Palette der Selbstbedienungsfunktionen sowie die Erfüllung von spezifischen juristischen Anforderungen. Gleichzeitig versuchen zahlreiche Unternehmen ihre Produkte unter dem Titel „Cloud Computing“ zu ver-

kaufen, obwohl es sich dabei um herkömmliche Produkte wie Hosting oder Managed Services handelt. Ein genauer Blick auf den vermeintlichen Cloud-Dienst und den Anbieter ist daher unvermeidlich.

Insgesamt lässt sich bereits jetzt festhalten, dass der Cloud-Computing-Markt – insbesondere der DaaS-Sektor – sich immer noch schnell wandelt. Unternehmen sollten daher einen Anbieter anhand der Übereinstimmung mit den *aktuellen* Bedürfnisse wählen, in regelmäßigen Abständen die Marktsituation erneut prüfen und wechselbereit bleiben. Es darf niemanden überraschen, wenn sich zwei Jahre nach der ersten Entscheidung für einen Anbieter herausstellt, dass dieser inzwischen nicht mehr die beste Übereinstimmung mit den Bedürfnissen des Unternehmens bietet. Im Verlauf dieses Kapitels wird daher genauer analysiert und bewertet, welche Aspekte bei der Wahl des Cloud-Anbieters relevant sein sollten. Die Struktur orientiert sich dabei an den vier Dimensionen, die im Kapitel 3 eingeführt wurden. Zum Ende des Kapitels werden die Inhalte in einigen grundsätzlichen Empfehlungen zusammengefasst und es wird wieder ein Bündel von Fragen bereitgestellt, die bei der Anbieterwahl hilfreich sind.

4.1 Wirtschaftliche Dimension

Der in der Praxis vorrangige Aspekt bei der Auswahl des Cloud-Anbieters ist vermutlich die wirtschaftliche Dimension. Im Folgenden wird beschrieben, inwiefern die Reputation des Anbieters sowie das angebotene Preismodell zu bewerten sind. Außerdem werden zwei Arten von Lock-in-Effekten dargestellt, die es nach Möglichkeit zu vermeiden gilt.

4.1.1 Reputation des Anbieters

Ein erster wichtiger Schritt bei der Auswahl des Cloud-Anbieters sollte eine Einschätzung der Größe und Bekanntheit des Anbieters sein. Die Branchengrößen wie Amazon, Google und Microsoft werden vermutlich auch auf längere Sicht Ihrer Cloud-Strategie treu bleiben. Bei kleineren Anbietern, Neulingen im Markt oder Firmen ohne klare Cloud-Strategie (z. B. Hewlett-Packard) kann man sich nicht so sicher sein [35]. Wenn es sich um ein großes bzw. wichtiges Projekt handelt, sollte folglich eher einem etablierten Hersteller der Vorzug gegeben werden.

Diese Bewertung ist eher subjektiv, aber nichtsdestotrotz hilfreich. Sie sollte ergänzt werden um den subjektiven Eindruck, wie transparent der Anbieter in seiner Informationspolitik ist:

- Werden detaillierte Informationen zu allen Fragen rund um die Servicenutzung bereitgestellt?
- Wird das Preismodell ausführlich erläutert? Wird auch auf nicht offensichtliche Kosten hingewiesen?
- Werden Informationen zu den Sicherheitsvorkehrungen und zum Stand der Technik in den Rechenzentren des Anbieters angeboten?

Auf Basis dieser subjektiven Eindrücke sollte ein erstes Bild von der Zuverlässigkeit der Anbieter entstehen.

Darüber hinaus sollte der Kunde aber versuchen, historische Kennzahlen zur Zuverlässigkeit des Dienstes für jeden Anbieter zu erlangen, am besten natürlich in den Dimensionen, die auch für die spätere Definition des SLA relevant sein könnten. Einige Anbieter geben solche Zahlen auf Anfrage heraus. Für andere gibt es teilweise Berichte in Blogs oder Online-Magazinen. Außerdem bietet es sich an, eine Recherche in einschlägigen Diskussionsforen und Online-Communitys durchzuführen. Dabei können sowohl einschlägige Web-Seiten[1], aber auch Dienste wie Twitter und Facebook hilfreich sein, in denen die Nutzer unmoderiert, aber auch ungenierter ihre Meinung äußern.

Zusätzliches Vertrauen in die Verlässlichkeit des Anbieters kann auch dadurch erlangt werden, dass geklärt wird, wie der Anbieter seine Mitarbeiter und Dienstleister aussucht. Dabei sollte beachtet werden, wie beispielsweise Mitarbeiter vor der Einstellung überprüft werden. Das ist insbesondere für das Personal interessant, das nachher mit sicherheitsrelevanten Systemen oder Daten in Berührung kommt. Dasselbe gilt für die gesamte „Supply Chain“ des Anbieters, also alle Subunternehmer oder beauftragten Dienstleister. Beispielsweise könnten Backups bei anderen Cloud-Anbietern gespeichert werden, die andere Standards an den Tag legen. Hier ist also wichtig zu erfahren, wie gewissenhaft der eigene Cloud-Anbieter seine Dienstleister vor der Auftragsvergabe aussucht.

Auf jeden Fall sollte eine Bewertung stattfinden, wie viel Schaden in dem Fall entsteht, dass die Nutzung eines Cloud-Dienstes aus unvorhergesehenen Gründen plötzlich beendet werden muss. Diese Bewertung gibt einen Hinweis darauf, wie genau der Cloud-Provider ausgesucht werden muss.

4.1.2 Preismodell

Wie schon eingangs erwähnt, sollte bei der Analyse des Preismodells genau auf versteckte Kosten geachtet werden. Die meisten Cloud-Anbieter erheben nämlich nicht nur Nutzungsentgelte für den Kern-Service, sondern auch für den Datentransfer in das und aus dem Rechenzentrum. Meistens erfolgt die Berechnung dabei anhand des transferierten Datenvolumen (z. B. pro GiB), wobei eingehender Datenverkehr oft günstiger ist als ausgehender.[2] Außerdem kann es auch sein, dass Support-Anfragen kostenpflichtig sind. Schließlich lassen sich viele Anbieter zusätzliche Dienstleistungen ebenfalls bezahlen. Es lohnt sich also, im Vorfeld genau zu recherchieren bzw. im Zweifelsfall genauere Informationen vom Anbieter anzufordern.

Ein wichtiger Aspekt des Preismodells ist die nutzungsabhängige Abrechnung (Pay-per-Use). Je nach Art der geplanten Verwendung der Cloud-Dienste lohnt sich der Schritt zum Cloud-Computing vielleicht erst, wenn (hauptsächlich) anhand der Nutzung abgerechnet wird. Das ist besonders dann interessant, wenn die Dienste zwischendurch überhaupt nicht verwendet werden und entsprechend keine Kosten anfallen sollten. Bei DaaS ist dies eher nicht der Fall, da zumindest der Speicherplatz für die Daten bezahlt werden muss. Es könnte jedoch vorkommen, dass die Daten nur zu ganz bestimmten Terminen benötigt werden und es daher günstiger ist,

[1] Z. B.: `http://cloutage.org/` oder `http://www.cloud-hosting-providers.com/`

[2] Derzeit berechnet Amazon beispielsweise eingehenden Datenverkehr für die Elastic Compute Cloud (EC2) überhaupt nicht, während ausgehender mit bis zu etwa 0,15 € pro GB zu Buche schlägt (Stand Oktober 2010).

die Datenbank für die Ruheperioden komplett zu löschen. Dies muss jedoch immer im Einzelfall entschieden werden. Hohe Grundgebühren widersprechen eigentlich dem Cloud-Gedanken, können aber bei intensiver Nutzung eventuell zu günstigeren Tarifen beim Anbieter verhelfen. Zu bedenken ist hierbei auch, dass im Rahmen der in Kapitel 3 beschriebenen Cost-Associativity, die Möglichkeit besteht, Zeit gegen höhere Ressourcennutzung abzuwägen. Im Rahmen einer rein nutzungsabhängigen Abrechnung ergeben sich daraus oft attraktive Zeitersparnisse.

Eng verwandt mit der nutzungsabhängigen Abrechnung ist auch die Frage, wie die Nutzung gemessen wird. Hier haben die Kunden bei großen Anbietern wie Amazon im Rahmen kleinerer Projekte vermutlich keine Wahlmöglichkeit. Bei kleineren Anbietern oder bei Aushandlung eines individuellen SLA sollte jedoch darauf geachtet werden, möglichst betriebswirtschaftlich motivierte Messgrößen zu verwenden. Das erleichtert die Prognose der Gebühren erheblich, da meistens die Zahl der erwarteten Transaktionen besser zu schätzen ist, als deren Dauer und genaue Beschaffenheit.

Obwohl viele Anbieter auf ihren Webseiten nur die Bezahlung per Kreditkarte oder PayPal angeben, bieten sie auf Anfrage meistens auch andere Modalitäten an, wie z. B. Zahlung gegen Rechnung [18]. Es lohnt sich also auch hier immer, genauer nachzufragen, falls die gewünschte Zahlungsart laut Webseiten nicht vorgesehen ist.

Zur Verwaltung der Cloud-Dienste stellen die Anbieter i. d. R. ein Webportal bereit, über das die Kunden den Dienst in Eigenregie verwalten können. Die bereitgestellte Funktionalität kann jedoch stark variieren. Als Minimum sollte das Portal eine Überwachung der Ressourcennutzung (Monitoring) inklusive einer Historie, eine Übersicht über die entstandenen Kosten und eine Schnittstelle zum Kundendienst („Trouble Tickets“ oder „Service Requests“) anbieten. Gerade in Bezug auf die Darstellung und Analyse der entstandenen Kosten gibt es große Unterschiede bei den Anbietern [18]. Einige Daten erscheinen vielleicht nur mit großer Zeitverzögerung oder werden anders aufgeschlüsselt, so dass ein Vergleich mit der vorliegenden Rechnung schwierig wird. Wenn die entstandenen Gebühren intern auf verschiedene Verursacher umgelegt werden sollen, so bietet es sich an, darauf zu achten, dass die Cloud-Ressourcen mit Metadaten (z. B. Tags) versehen werden können. Außerdem sind in solchen Fällen maschinenlesbare Rechnungen sowie Aufschlüsselungen der Servicenutzung inklusive Metadaten von Vorteil, um diese automatisiert zuordnen zu können.

Soll mehr als nur ein einzelner Dienst bezogen werden, kann es günstige Kombinationen geben. Amazon berechnet z. B. keinen Datenverkehr innerhalb der eigenen Cloud, so dass Transfers zwischen S3 und EC2 kostenlos sind. Auch lohnt es sich bei größeren Projekten, die möglicherweise eine breite Masse an Kunden ansprechen, auf zusätzliche Leistungen des Cloud-Anbieters wie spezielle SSL-Endpunkte für SSL-Offloading, Applikationsbeschleuniger oder ein Content Delivery Network (CDN) zu achten.

Abschließend sei bemerkt, dass es sich bei allen Anbieter lohnt, nach Rabatten zu fragen. Häufig kann man durch Vorauszahlung oder Vereinbarung einer Mindestnutzung bereits günstigere Preise erzielen. Besonders dann, wenn es sich um ein größeres Projekt handelt, sollte auf jeden Fall ein individuelles Angebot angefragt werden.

4.1.3 Lock-in-Effekte über die Daten

Der wohl wichtigste Aspekt für ein Unternehmen in Bezug die Auslagerung seiner Daten ist die Frage, ob das Unternehmen alleiniger und vollwertiger Eigentümer der Daten ist und bleibt. Das muss sowohl in Bezug auf die in das System explizit eingetragenen Daten gelten, als auch in Bezug auf die automatisch erstellten Daten und Metadaten. Insbesondere letzterer Aspekt wird leicht übersehen. Dies ist auch keineswegs selbstverständlich, da SaaS-Anbieter nicht immer vollständigen Zugriff auf alle Daten erlauben, die im Rahmen der Nutzung der Software im System angefallen sind. Auch ist es manchmal schwierig, die Daten in einem verwendbaren Format zu erhalten (vgl. Kasten „Erfahrung aus der Praxis“).

Erfahrung aus der Praxis:
Während der Vorbereitung dieses Leitfadens berichtete uns ein KMU davon, dass ein SaaS-Anbieter die Daten, die im Rahmen der Servicenutzung angefallen waren, nach Beendigung des Vertragsverhältnisses nicht herausgeben wollte. Das Argument lautete, dass die internen Datenstrukturen ein Geschäftsgeheimnis darstellten. Das KMU musste in diesem Fall genaue Angaben machen, welche Attribute und Datensätze vom Anbieter exportiert werden sollten – ein langwieriger Prozess. Im Endeffekt war es für das KMU quasi unmöglich zu entscheiden, ob alle relevanten Daten extrahiert worden waren oder nicht.

Als Kunde sollte also eine klare Absprache mit dem Anbieter getroffen werden, dass dieser entweder regelmäßig oder auf Anfrage eine *vollständige* Kopie der Daten in für den Kunden verwendbarer Form zur Verfügung stellt. Eine „verwendbare Form“ kann dabei je nach Anwendungsfall eine Kopie der Datenbank in Form eines SQL-Dump oder einer Access-Datenbank sein. Eventuell ist auch ein Excel-Dokument oder ein CSV-Export in eine Textdatei angemessen. Als letzte Möglichkeit wäre auch ein PDF-Dokument denkbar. Im besten Fall bietet die Weboberfläche die Möglichkeit, einen solchen Export ohne Interaktion mit dem Anbieter durchzuführen.

Wie einfach die Daten auch aus dem jeweiligen Dienst exportiert werden können, so muss doch immer ein gewisser Lock-in-Effekt einkalkuliert werden. Auch im Fall eines vollständigen SQL-Dump müssen die Daten vor der Verwendung in anderen Systemen im Normalfall noch recht aufwändig konvertiert und aufbereitet werden. Die von Cloud-Anbietern suggerierten extrem kurzfristigen Ein- und Ausstiegsmöglichkeiten sind daher mit entsprechender Vorsicht zu genießen.

4.1.4 Lock-in-Effekte über die Prozesse

Neben dem Lock-in-Effekt über die Daten, kann es auch leicht zu einem solchen Effekt über die Geschäftsprozesse kommen. Wie bereits in Abschnitt 2.2 angesprochen erfordert die Integration eines Cloud-Dienstes immer auch eine gewisse Anpassung der eigenen Geschäftsprozesse. Je nachdem, wie weit diese Anpassungen gehen, kann auch durch sie eine Lock-in-Situation entstehen.

Die nötigen Anpassungen der Prozesse lassen sich zum großen Teil über die funktionalen Anforderungen an die Software abschätzen. Bietet der Cloud-Dienst bereits in seiner Basisausführung alle benötigten Funktionen, so ist der Anpassungsaufwand tendenziell niedrig. Unter Umständen können fehlende oder unpassende Funktionen durch Anpassung der Anwendung (Customizing) nachgerüstet werden. Gerade in Bezug auf die Funktionen, die nicht in die Kernkompetenz der Software fallen, ist dies aber häufig nicht möglich. Hier muss Abhilfe dann

entweder durch Anpassung der internen Abläufe oder durch zusätzliche Bereitstellung lokaler Hilfsprogramme geschaffen werden. Es ist für die Anpassung sehr hilfreich, wenn der Cloud-Dienst vielfältige Schnittstellen zur Verfügung stellt (vgl. Abschnitt 4.2.3).

Die Kompatibilität des Cloud-Anbieters zu bestehenden Geschäftsprozessen darf nicht unterschätzt werden. Im Zweifelsfall ist eine Anpassung der Software oder gar die Änderung der internen Prozesse deutlich aufwändiger und teurer als die Wahl eines teureren Cloud-Anbieters, der sich aber besser in die bestehenden Abläufe einfügt.

4.2 Technische Dimension

Abgesehen von den wirtschaftlichen Aspekten, spielen auch die technischen Fragestellungen eine wichtige Rolle bei der Auswahl des Anbieters. Insbesondere die Fragen nach der Sicherung der Daten, der Zuverlässigkeit und der Leistungsfähigkeit der Cloud sind hierbei relevant. Es darf jedoch nicht vergessen werden, ebenfalls zu prüfen, ob sich die Dienste eines konkreten Anbieters gut in die bestehende Systemlandschaft einfügen. Dieser Aspekt wird daher ebenfalls thematisiert. Fragen zur technischen Sicherheit der Angebote werden detailliert in Kapitel 5 behandelt und daher hier weitgehend ausgeblendet.

4.2.1 Sicherung und Wiederherstellung von Daten

Eine essentielle Voraussetzung für den Schritt in die Cloud ist häufig, dass die Daten beim Cloud-Anbieter mindestens genauso gut vor Datenverlust geschützt werden, wie im eigenen Rechenzentrum. Alle großen Cloud-Anbieter implementieren eine vorbildliche Backupstrategie, aber es lohnt sich immer, genauer nachzufragen. Es gibt zahlreiche Aspekte, die im Rahmen dieser Fragen zu klären sind. Als erstes ist zu klären, wie oft und zu welchen Zeitpunkten vollständige und inkrementelle Sicherungskopien der Daten durchgeführt werden. Außerdem ist interessant, ob die Daten auf Festplatten oder Bändern gesichert werden und wo die Daten aufbewahrt werden. Der Aufbewahrungsort ist zum einen interessant, um zu beurteilen, wie sicher die Daten aufbewahrt werden und wie schnell sie wieder hergestellt werden können. Zum anderen können dadurch aber auch rechtliche oder sicherheitstechnische Probleme auftreten. Nutzt das Unternehmen bereits einen Dienstleister, der die Archivierung der Backups übernimmt, so sollte der Cloud-Anbieter die Backups auch zu diesem Dienstleister schicken können. In jedem Fall muss die gesamte Prozess der Datensicherung mit den Compliance-Anforderungen und den branchenspezifischen rechtlichen Rahmenbedingungen abgeglichen werden.

Je nach Anwendung kann auch die Wiederherstellungsprozedur sehr wichtig werden. Es kann z. B. erforderlich werden, die Daten auf einen bestimmten Stand „zurückzusetzen“. Das erfordert regelmäßige *Snapshots* durch den Anbieter. Für kritische Daten kann auch die Möglichkeit einer *Forward-Recovery* wichtig sein. Zudem ist die Frage, wie und unter welchen Umständen der Kunde die Daten wiederherstellen kann. Kann eine Wiederherstellung beispielsweise auch im Fall logischer[3] Fehler durchgeführt werden? Sollen die Daten wiederhergestellt werden, so

[3] Das Auftreten *logischer Fehler* bedeutet, dass die Datenbasis fachlich falsche Daten enthält. Beispielsweise könnte ein Programmierfehler dazu führen, dass widersprüchliche Informationen zu Konten-

sollte außerdem klar definiert werden, wie lange dies dauern darf. Handelt es sich um eine SaaS-Anwendung, so kann es gut sein, dass der Anbieter keine nach Mandanten getrennten Backups aufbewahrt, weil die internen Datenstrukturen dies nicht leicht erlauben. Das hat zur Konsequenz, dass eine Wiederherstellung lange dauert und vielleicht nur sehr eingeschränkt möglich ist. Im optimalen Fall kann der Anwender die Wiederherstellung über eine Weboberfläche völlig automatisiert anstoßen.

4.2.2 Leistungsfähigkeit der Cloud

Auch wenn die Versprechen des Cloud-Anbieters gut klingen und der angebotene Service insgesamt gut zu passen scheint, sollte immer noch eine Reihe von Tests durchgeführt werden. Schon mit einfachen Mitteln, z. B. einem Verbindungstest („Ping“-Test) lässt sich die durchschnittliche Latenz der Verbindung zu verschiedenen Tageszeiten testen. Bereits durch Tests der Provider-Infrastruktur im kleinen Maßstab lassen sich belastbare Aussagen treffen. Soll ein größeres Projekt in der Cloud gestartet werden, so sollte auch die Skala der Tests größer ausfallen, damit mögliche Ressourcenengpässe auf Anbieterseite frühzeitig erkannt werden.

Verfügbarkeit

Der Verfügbarkeit des Cloud-Dienstes kommt dabei eine besondere Rolle zu. Kann ein Unternehmen etwas längere Laufzeit bei Anfragen oft noch tolerieren, so ist die Nichterreichbarkeit eines Dienstes – insbesondere einer Database-as-a-Service – oft hoch problematisch. Typischerweise wird heutzutage eine Verfügbarkeit von 99,95% garantiert [18], vergleichbar mit den SLAs, die traditionelle Hosting-Anbieter für hochverfügbare dedizierte Server bieten. Für die meisten Einsatzzwecke werden diese Garantien anfangs ausreichen. Sollte jedoch eine höhere Verfügbarkeit benötigt werden, so muss dies mit dem Cloud-Anbieter genau abgesprochen werden. Aktuelle Angebote sind von der Infrastruktur nicht dafür ausgelegt, mehr als 99,95%ige Verfügbarkeit zu bieten. Bei diesen Überlegungen ist immer zu beachten, dass die Verfügbarkeit üblicherweise ohne Berücksichtigung der angekündigten Systemabschaltungen und Wartungsfenster berechnet wird. Je nachdem, wie viel Zeit der Anbieter hierfür einplant, kann sich die tatsächliche Verfügbarkeit deutlich nach unten verschieben.

Sinnvollerweise sollte auch die Netzanbindung des Anbieters durch das SLA zugesichert werden. Teilweise kann es auch sinnvoll sein, die Leistung des internen Netzwerks im Rechenzentrum des Cloud-Anbieters vertraglich zu vereinbaren. Hierbei legt man oft Grenzwerte für Verfügbarkeit, Latenzzeit, Paketverlust und Jitter fest. Gleichermaßen ist es oft notwendig, die Internetanbindung des eigenen Unternehmens durch ein entsprechendes SLA mit dem eigenen Internet Service Provider (ISP) abzusichern.

bewegungen und dem Saldo gespeichert werden. Rein technisch ist die Datenbank nach wie vor in Ordnung; sie weist keine *physischen Fehler* auf, die z. B. durch einen defekten Sektor auf der Festplatte verursacht werden. Im Gegensatz zu physischen Fehlern kann nur der Kunde (und nicht der Anbieter) die logischen Fehler erkennen.

Leistungsfähigkeit der Cloud-Infrastruktur

Neben der Verfügbarkeit spielt natürlich auch die Leistungsfähigkeit der Infrastruktur des Cloud-Anbieters eine entscheidende Rolle. Der Dienst soll schließlich nicht nur erreichbar sein, sondern auch reibungslos funktionieren, damit z. B. von der Elastizität der Cloud profitiert werden kann. Um sicherzustellen, dass die Infrastruktur des Anbieters den Anforderungen gewachsen ist, kann das Anwenderunternehmen im Fall eines DaaS-Dienstes z. B. Testdaten hin und her zu kopieren sowie Dummy-Abfragen auszuführen. Beim Kopieren sollte sowohl die Geschwindigkeit zwischen eigenem Intranet und der Cloud als auch die Geschwindigkeit innerhalb der Cloud gemessen werden, falls mehrere Dienste beim Cloud-Anbieter bezogen werden. Bei der Durchführung von Dummy-Abfragen sollte besonderes Augenmerk auf die Funktionen zur automatischen Skalierung des Ressourcenangebots gelegt werden, denn das ist normalerweise ein Hauptargument für die Nutzung einer DaaS.

Die Reaktionszeit auf den geänderten Ressourcenbedarf ist je nach Anbieter unterschiedlich. Normalerweise sollte die Bereitstellung neuer bzw. Freigabe nicht mehr benötigter Ressourcen weitgehend automatisch erfolgen. Je nach Service-Typ muss entweder der Benutzer den geänderten Bedarf über eine Weboberfläche (oder eine API) mitteilen oder – wie für eine DaaS üblich sein sollte – die Erkennung und Anpassung erfolgt vollautomatisch. Einige Cloud-Anbieter sprechen auch Garantien für diese Reaktionszeit im SLA aus [18].

Verbindung zur Cloud

Obwohl Cloud-Anbieter ihre Dienste per Internet anbieten, gibt es bei einigen auch die Möglichkeit, eine dedizierte, private Verbindung zur Cloud aufzubauen. Eine Möglichkeit besteht darin, ein Virtual Private Network (VPN) über das Internet zum Anbieter aufzubauen, so dass sämtlicher Verkehr zum Dienst automatisch gesichert wird. Bei anderen Anbietern ist es sogar möglich, eine dedizierte Netzwerkverbindung zu erhalten, so dass ein Multiprotocol Label Switching (MPLS) VPN aufgebaut werden kann (was allerdings mittel- bis langfristige Verträge mit dem Telekommunikationsanbieter nach sich zieht). Gerade im Bereich der größeren Firmenkunden könnte diese Option interessant sein, zumal einige Anbieter sie nicht extra berechnen. [18]

Vorgehen für die Performance-Analyse

Die beschriebenen Tests können und sollten zum einen durch die eigenen IT-Abteilung durchgeführt werden – so werden auch die eigenen Systeme als Faktor einbezogen. Eine Studie der Harvard-Universität [10] zeigt auf, wie man prinzipiell vorgehen kann. Zusätzlich sollten aber auch die in Abschnitt 3.1.4 auf Seite 34 beschriebenen Werkzeuge und Informationsportale verwendet werden.

Bei der Evaluation sollten nicht nur die aktuellen Garantien betrachtet werden, sondern auch die Vergangenheit: Hat der Anbieter es in den letzten Monaten und Jahren geschafft, seine Versprechen einzuhalten? Hierzu kann es hilfreich sein, in Diskussionsforen zu recherchieren, um Kundenstimmen zu hören, die von Problemen oder guten Erfahrungen mit dem Anbieter berichten. Interessant ist in diesem Zusammenhang auch, ob die SLAs mit angemessenen Strafen

versehen sind und ob der Anbieter die Strafen auch bezahlt. Welche Strafe angemessen ist, muss allerdings immer im Einzelfall entschieden werden. Für hochverfügbare Cloud-DBS ist ein 10%iger Rabatt auf die Nutzungsgebühr unangemessen, da der drohende Schaden durch einen Ausfall des Systems oft viel schwerer wiegt. Für zeitlich unkritische Berechnungen hingegen kann diese Regelung völlig in Ordnung sein.

Bei der gesamten Analyse ist zu bedenken, dass viele Cloud-Anbieter rapide wachsen. Das kann sich negativ auf die Stabilität und Verfügbarkeit der Infrastruktur auswirken. Die Qualität der Architektur und des Personals wirken sich ebenso direkt darauf aus, ebenso wie klar definierte Change- und Release-Management-Prozesse. In der Realität können daher die versprochenen und erbrachten Werte für Verfügbarkeit und Stabilität auseinander klaffen. Eine gründliche Analyse ist unabdingbar. [18]

Bei aller Analyse der harten Fakten sollte jedoch nie vergessen werden, dass der Dienst auch von den Nutzern im Unternehmen akzeptiert werden muss. Daher sollte als weitere nichtfunktionale Anforderung auch die Benutzungsfreundlichkeit in Betracht gezogen werden.

4.2.3 Integration in bestehende Systeme

Sollen Cloud-Dienste und bestehende Systeme eng zusammenarbeiten, so zeigt sich schnell, dass eine Integration von Cloud-Diensten und Nicht-Cloud-Systemen oft sehr problematisch ist. Die Erfahrung zeigt, dass Cloud-Dienste untereinander oft einigermaßen einfach zu koppeln sind, vor allem, wenn sie von demselben Hersteller angeboten werden. Sollen Cloud-Dienste jedoch in bestehende, vielleicht sogar „(wild) gewachsene“ Systeme integriert werden, so treten verstärkt Integrationsprobleme auf und in deren Folge die Lock-in-Effekte, die in den Abschnitten 4.1.3 und 4.1.4 bereits betrachtet wurden.

Eine technische Gegenmaßnahme stellen offene Schnittstellen dar. Daher sollte bei der Wahl des Cloud-Dienstes darauf geachtet werden, dass ausreichend mächtige APIs zur Verfügung stehen. Dies ist insbesondere für DaaS-Angebote essentiell, weil eine ihrer Hauptaufgaben im Lesen und Schreiben von Daten besteht. Durch geeignete Schnittstellen können die Daten flexibel und in passenden Formaten im- oder exportiert werden, so dass eine Integration keine allzu große Anpassung bestehender Systeme erfordert. Im Rahmen des *Open Cloud Manifesto*[4] organisieren sich zahlreiche kleinere Cloud-Anbieter und -Nutzer, die gemeinsame, offene Schnittstellen für Cloud-Dienste befürworten bzw. entwickeln wollen. Die Branchengrößen wie Amazon und Google fehlen allerdings – ebenso wie praxisrelevante Ergebnisse.

Abgesehen vom reinen Datenaustausch und der Konvertierung zwischen verschiedenen Datenformaten oder -strukturen können aber auch durch das nunmehr entfernte DBS Probleme entstehen. Während die Verbindung zum DBS im eigenen Rechenzentrum nur marginale Latenzzeiten und hohe Transferraten bietet, bedingt ein Cloud-DBS prinzipiell eine höhere Latenz und niedrigere Bandbreite. Gleichzeitig steigt durch die Vielzahl von beteiligten Parteien das Risiko, dass die Verbindung zwischen Unternehmen und Cloud nicht mehr hergestellt werden kann. Diese Faktoren müssen bei der Integration des neuen Dienstes berücksichtigt werden. Sollten bestehende Anwendungen Annahmen zur Verfügbarkeit, Antwortzeit oder Übertragungsgeschwindigkeit treffen, so müssen diese eventuell aufwändig umgearbeitet werden.

[4] http://www.opencloudmanifesto.org/

Als Alternative bieten einige Cloud-Provider die Möglichkeit, eigene dedizierte Hardware in das Cloud-Rechenzentrum zu stellen. Der Anbieter kümmert sich dann um die Verwaltung und Wartung der Server und bietet eine Verbindungsqualität zwischen den dedizierten Systemen und den Cloud-Diensten, die der eines lokalen Intranet in nichts nachsteht. Diese „Hybridisierung“ der Firmen-IT wird in Zukunft zunehmen (vgl. [18]).

4.3 Rechtliche Dimension

Eine ganz entscheidende Fragestellung bei der Entscheidung für oder gegen einen Cloud-Anbieter können die rechtlichen Aspekte sein. Im Rahmen der Grundsatzentscheidung aus Kapitel 3 sollte bereits eine grundsätzlich juristische Prüfung stattgefunden haben, ob die zur Debatte stehende Anwendung generell ausgelagert werden darf. Ist diese Frage geklärt, so ist die Auswahl des geeigneten Cloud-Anbieters glücklicherweise deutlich einfacher.

4.3.1 Erfüllung der gesetzlichen Anforderungen

Als Ergebnis der grundsätzlichen Analyse existiert im Unternehmen bereits eine Liste aller relevanten gesetzlichen Vorschriften für die spezielle Branche und das konkrete Szenario. Im günstigsten Fall hat der Anbieter die Konformität mit den entsprechenden Normen bereits geprüft und kann diese auf Anfrage bestätigen. Zumindest die Zusage über die Konformität mit dem Bundesdatenschutzgesetz (BDSG) sollte für alle DaaS-Anbieter eine Selbstverständlichkeit sein. Im ungünstigen Fall ist die Prüfung jedoch noch nicht passiert und entweder der Anbieter oder das Anwenderunternehmen müsste sie noch durchführen. Sollte der Anbieter nicht aus eigenen Stücken zu der Konformitätsprüfung bereit sein, so sollte das Anwenderunternehmen von dem Cloud-Dienst Abstand nehmen. Die rechtlichen Probleme in diesem juristischen Neuland sind nur schwer absehbar.

Als Anhaltspunkt für die Konformität mit den relevanten Normen können Zertifizierungen nach ISO/IEC 27001 oder SAS 70 sein. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet außerdem weitere Zertifizierungen an. Diese Standards sind jedoch alle nur behelfsmäßig auf die Situation im Cloud-Computing angewendet worden. Insbesondere bei der SAS 70-Zertifizierung muss daher genau der Volltext der Zertifzierungsurkunde studiert werden, da der Standard keine Vorgaben über den Umfang der Zertifizierung macht. Einen wirklichen „Cloud-Sicherheitsstandard“ gibt es noch nicht.

Im Rahmen der Frage, ob ein Angebot konform zum BDSG ist, bietet der Ort der Datenverarbeitung einen guten Anhaltspunkt. Kann der Cloud-Anbieter schriftlich bestätigen, dass die Daten nur innerhalb der EU verarbeitet und gespeichert werden, so ist bereits eine wichtige Vorgabe des Datenschutzrechts erfüllt. Diesem Aspekt tragen heute bereits viele Cloud-Anbieter Rechnung. Amazon bietet z. B. geografische Einschränkungsmöglichkeiten für die Services an, um die Datenverarbeitung auf „Europe“ zu begrenzen. Von allen Anbietern, die keine Beschränkung der Datenverarbeitung auf die EU anbieten, sollte zurzeit noch abgesehen werden. Selbst Zertifikate wie der „US Safe Harbor“, der eigentlich US-Unternehmen als konform zur EU-Datenschutzrichtlinie ausweisen soll, sind nicht praxistauglich. Eine Studie zur Praxistauglichkeit des Safe-Harbor-Siegels zeigt auf, dass Ende des Jahres 2008 nur 54 von den 1 597

Tabelle 4.1: Einschätzung der Relevanz von Zertifikaten und Qualitätssiegeln im Cloud-Computing

Zertifikat/Siegel	Aussagekraft	Bemerkung
ISO/IEC 27001	mittel bis hoch	Empfehlung des BSI
SAS 70	niedrig bis mittel	Umfang der Prüfung entscheidend
US Safe Harbor	ohne Aussagekraft	Keine Prüfung, vgl. [5]
PrivacyMark	niedrig	Beschränkung auf Japan

Unternehmen, die zu dem Zeitpunkt als „US Safe Harbor“ gelistet waren, die grundlegenden Anforderungen des Safe-Harbor-Siegels umsetzten [5]. Daher sind die juristischen Konsequenzen einer Zusammenarbeit mit solchen Anbietern nicht absehbar. Tabelle 4.1 gibt einen kurzen Überblick über die bekanntesten Zertifikate und ihre Aussagekraft in Bezug auf die zertifizierten Cloud-Anbieter. Eine grafische Übersicht über die verschiedenen Stufen der Gesetzgebung zum Datenschutz findet sich unter `http://www.forrester.com/cloudprivacyheatmap`.

Über den sorgfältigen Umgang mit den personenbezogenen Daten hinaus fordert das BDSG allerdings auch geregelte Löschverfahren für personenbezogene Daten. Zu beachten ist hierbei, dass höchstwahrscheinlich auch archivierte und replizierte Datensätze betroffen sind. In dieser Hinsicht stellen sich einige wichtige, teilweise bis dato unbeantwortete Fragen (vgl. [19, S. 150 f.]):

- Wie löscht der Cloud-Anbieter die personenbezogenen Daten tatsächlich? Wie werden replizierte und archivierte Daten gelöscht? Kann ein Datum überhaupt je gänzlich gelöscht werden, sobald es in die Cloud gespielt wurde?
- Hat der Anbieter die Daten tatsächlich physikalisch gelöscht („zerstört“) oder nur per Software als gelöscht markiert („in den Papierkorb verschoben“)? Reicht eine Löschung im Dateisystem oder müssen die Daten auch gänzlich aus den physikalischen Speichermedien getilgt werden? Ist ein weit verzweigtes Netz aus replizierten Daten eine „besondere Art der Speicherung“ im Sinne des §35 Abs. 3 Nr. 3 des BDSG, was zur Folge hätte, dass die Daten nur gesperrt, nicht aber gelöscht werden müssen?
- Der Anbieter darf die Daten nicht zu früh löschen, aber andererseits auch nicht über den Zeitpunkt der geforderten Löschung hinaus aufbewahren. Wie kann also der richtige Zeitpunkt der Löschung sichergestellt und nachgewiesen werden?

Nach aktuellem Wissensstand bietet derzeit keiner der großen Cloud-Provider eine vollständige Löschung von personenbezogenen Daten an.[5]

4.3.2 Ausstiegsszenarien

Im Rahmen der Verträge mit dem Cloud-Anbieter sollten auch die Szenarien klar definiert werden, in denen das Anwenderunternehmen bzw. der Anbieter das Vertragsverhältnis beenden

[5] Stand: September 2010.

kann. Das übliche Szenario ist dabei, dass der Cloud-Nutzer die Anwendung nicht mehr länger nutzen möchte. Für diesen Fall sollte der Zugriff auf den gesamten Datenbestand ebenso sichergestellt werden wie die Kooperation des bisherigen Anbieters bei der Migration.

Um eine gewisse Sicherheit gegenüber der plötzlichen Einstellung des Dienstes oder der unverhofften Kündigung zu haben, kann das Anwenderunternehmen gewisse Vorsichtsmaßnahmen treffen. Im optimalen Fall sichert der Anbieter dem Cloud-Nutzer die Möglichkeit zu, zur Not auf ein lokales System (unter eigener Kontrolle) umzuschalten. Dazu wird die Cloud-Anwendung lokal beim Anwender installiert. Im Notfall darf das Unternehmen auf die lokale Version umschalten. Zu klären sind die genauen Konditionen und die Dauer für eine solche Umschaltung.

Da größere Anbieter sich i. d. R. nicht auf so einen Handel einlassen und die Kosten für die Bereithaltung eines solches Backup-Systems meistens die Vorteile der Cloud-Nutzung aufwiegen, besteht außerdem die Möglichkeit, den Programm-Code des Systems bei einem Notar oder Treuhänder zu hinterlegen (engl. *Escrow*). Im Fall, dass der Anbieter seinen vertraglichen Verpflichtungen zur Weiterentwicklung und Wartung der Software nicht mehr nachkommen kann, hat das Anwenderunternehmen zumindest die theoretische Möglichkeit, dies selbst durchzuführen.

Schließlich sollte auch der Fall berücksichtigt werden, dass der Anbieter den Betrieb des Systems nicht mehr gewährleisten kann.

4.3.3 Weitere Aspekte

Ein weiterer Aspekt, der bei der Wahl des Anbieters bzw. der Vertragsgestaltung berücksichtigt werden sollte sind mögliche nachträgliche Änderungen am Produkt, insbesondere Preisänderungen. Im Vertragswerk sollte festgelegt werden, welche Möglichkeiten zur Preisänderung sich der Cloud-Anbieter vorbehält. Oft werden die Preise nicht festgeschrieben, sondern können vom Anbieter recht frei angepasst werden. Ein Sonderkündigungsrecht bei Änderung der Preise ist oft nur Makulatur, weil der Aufwand des Anbieterwechsels im Hinblick auf die oben beschriebenen Lock-in-Effekte zu hoch ist. Im Vorfeld muss daher geklärt werden, welche Preisänderungen möglich sind. Ist es nicht möglich oder zu unattraktiv fixe Gebühren zu vereinbaren, so sollte zumindest eine Berechnung erfolgen, in welchem Preiskorridor der Dienst attraktiv bleibt. Mithilfe der geschätzten Wahrscheinlichkeit für die entsprechende Preissteigerung kann dann eine Entscheidung erfolgen, ob das Angebot trotzdem attraktiv ist.

Im Hinblick auf alle individuellen Verträge mit dem Cloud-Anbieter muss bemerkt werden, dass jede Abweichung vom Standardprodukt und den Standardverträge für den Anbieter zu gesteigerter Komplexität und damit in der Regel auch zu höheren Preisen führt. Besonders im Hinblick auf die mehrfach erwähnten individuellen SLAs ist abzuwägen, ob die oft deutlich höheren Kosten dem zusätzlichen Nutzen angemessen sind. Zwar sind solche individuellen Anpassungen aus Sicht des Cloud-Anwenders oft notwendig, aber aus Anbietersicht nicht immer einfach realisierbar. Ob Cloud-Computing wirklich zu einer Kostenreduktion führt, hängt deshalb maßgeblich davon ab, mit welchen Risiken man seine Geschäftsprozesse aussetzen kann und will.

4.3.4 Handlungsempfehlungen zur rechtlichen Dimension

Abschließend bleibt festzuhalten: *Selbstverständlich ist jeder Vertrag juristisch gründlich zu prüfen.* Besonderes Augenmerk muss dabei der Compliance, Datensicherheit, den Ausstiegsszenarien und Möglichkeiten zur Preisänderung gelten [16]. Aus der aktuellen juristischen Situation sind außerdem drei empfehlenswerte Vorgehensweisen für den Schritt „in die Cloud“ abzuleiten:

1. Im besten Fall garantiert der Anbieter die Konformität zu den bestehenden gesetzlichen Regelungen, so dass das juristische Risiko größtenteils auf diesen abgewälzt werden kann.

2. Weit verbreitete Vorgehensweisen und Dienste wie z. B. das CRM-Outsourcing zu Salesforce können de facto als unbedenklich angesehen werden, da eine breite Masse an Präzedenzfällen existiert.

3. Im Zweifelsfall, besonders beim Betreten von „Neuland“ in der Cloud, sollte lieber Abstand davon genommen werden, sensible oder personenbezogene Daten an einen Cloud-Anbieter zu übergeben.

4.4 Organisatorische Dimension

Auch aus organisatorischer Sicht ist das Cloud-Computing ähnlich zu behandeln wie klassisches IT-Outsourcing. Die wichtige Frage im Hintergrund ist, wie viel Kontrolle das Anwenderunternehmen über den Cloud-Anbieter ausüben kann. Dazu gehört auch die Frage, wie die tatsächliche Umsetzung der versprochenen Maßnahmen und Leistungen vor Ort überprüft werden können. Konkret äußern sich diese Aspekte unter anderem in der Zusammenarbeit mit dem Anbieter sowohl im Falle üblicher Probleme bei der Servicenutzung sowie im „Notfall“, wenn etwas wirklich schief läuft. Zuvor soll jedoch kurz erläutert werden, wie ein systematisches Vorgehen zur Anbieterwahl aussehen könnte.

4.4.1 Vorgehen zur und Dokumentation der Anbieterwahl

Wie in Kapitel 3.1.4 angedeutet, ist es sinnvoll, die Auswahl des Cloud-Anbieters strukturiert anzugehen. Dafür bietet es sich an, einen Kriterien- bzw. Anforderungskatalog aufzustellen, der die Anforderungen des eigenen Unternehmens an einen hypothetischen, optimalen Cloud-Anbieter aufzeigt. Als zweiter Schritt kann dann ein Vergleich der tatsächlich verfügbaren Angebote mit den Anforderungen durchgeführt werden. Das Ergebnis wird häufig ein kleiner Kreis der „am wenigsten schlecht passenden“ Cloud-Anbieter sein, aus welcher der geeignetste ausgewählt werden kann. Welche Kriterien in dem Katalog auftauchen, ist sehr stark abhängig vom jeweiligen Anwendungsfall und kann hier nicht allgemein beantwortet werden. Viele Anregungen werden sich jedoch aus diesem Leitfaden sowie aus dem Katalog von Mindestanforderungen für Cloud-Anbieter des BSI [4] ergeben.

Ein bedeutsamer Teilaspekt der Anbieterwahl ist die nachvollziehbare Dokumentation derselben. Im Bereich der Cloud-Angebote muss auf mittlere Sicht damit gerechnet werden, dass

sich der Markt recht dynamisch ändern wird. Daher ist eine regelmäßige Prüfung nötig, ob der aktuelle Anbieter noch immer der am besten geeignetste ist. Eventuell gibt es inzwischen besser passende Angebote oder identische Produkte zu günstigeren Preisen. Anhand der früheren Kriterien und Anforderungen kann die neue Marktlage relativ schnell und strukturiert analysiert werden. Zudem erschließen sich eventuell Entwicklungen im Zeitverlauf, die für oder gegen einen Provider sprechen, wenn dieser seine Produktpalette beispielsweise deutliche langsamer weiterentwickelt als der Rest des Marktes.

4.4.2 Support-Leistungen des Anbieters

Ein sehr wichtiger Aspekt bei der Zusammenarbeit mit dem Cloud-Anbieter ist die Frage, wie die Mitarbeiter des Anwenderunternehmens mit der Kundenbetreuung in Kontakt treten können und welche Reaktionszeiten zugesagt werden. Dabei können drei Aspekte der Kundenbetreuung unterschieden werden [18]:

- **Reaktion auf Kundenanfragen** Die Kundenbetreuung wird kontaktiert, weil ein Problem aufgetreten ist. Hierbei ist es wichtig, dass der Anbieter zu offener Kommunikation und zügiger Problemlösung bereit ist. Dies ist der klassische Fall für Kundenbetreuung.

- **Anbieter-initiierter Support** Der Anbieter weist bereits im Vorfeld auf drohende Probleme (z. B. Ressourcenengpässe, nötige Wartungsarbeiten) hin bzw. alarmiert den Nutzer sobald ein Fehler auftritt. Der Provider bietet dabei entweder eine Lösung oder zumindest Hilfestellung bei der selbständigen Lösung an. Im Rahmen von Verträgen, in denen der Anbieter viele bis alle Aspekte der Infrastruktur verwaltet (also jegliche Cloud-Computing-Verträge), sollte dieser Aspekt berücksichtigt werden.

- **Projekt-Unterstützung** Der Cloud-Anbieter unterstützt den Kunden bei komplexen Projekten wie z. B. beim Versionswechsel, bei Migrationen oder bei dem Produktivschalten neuer Systeme. Diese Art von Support muss in aller Regel zusätzlich eingekauft werden.

In Bezug auf die Kontaktaufnahme mit dem Cloud-Anbieter ist zu klären, welche Kanäle dafür vorgesehen sind. Während viele Anbieter nur die Kommunikation per Web-Formular erlauben, erhalten die Nutzer bei anderen spezielle E-Mail-Adressen für ihre Anfragen. Eventuell bietet der Provider auch eine telefonische Unterstützung. In jedem Fall ist es wichtig zu wissen, ob es sich um einen Rund-um-die-Uhr-Support („24/7“) handelt, oder ob nur bestimmte Geschäftszeiten vorgesehen sind. Im Rahmen des durch den Anbieter initiierten Supports ist es wichtig, die Ansprechpartner zu klären, um sicherzustellen, dass Meldungen zu anstehenden Wartungsarbeiten oder Systemabschaltungen auch bei den richtigen Mitarbeitern in der Unternehmung ankommen. Eventuell werden entsprechende Nachrichten aber auch nur über einen Newsfeed (z. B. mit Really Simple Syndication, RSS) veröffentlicht, der regelmäßig gelesen werden muss.

Die Kundenbetreuung hat bei jedem Anbieter eine etwas andere Zielgruppe, die bei der Entscheidung für oder gegen einen Anbieter mit berücksichtigt werden sollte. Typische Zielgruppen für den Support sind z. B.:

- Anwendungsentwickler, die sich nicht mit dem laufenden Betrieb der Systeme auskennen

- Systemintegratoren oder Drittanbieter, die im Auftrag eines Kunden dessen Systeme in die Cloud bringen, aber selbst nur wenig Wissen über den Betrieb dieser Systeme mitbringen

- Systemadministratoren, die sich noch nicht tiefgehender mit der Cloud auseinander gesetzt haben und daher grundlegende Fragen haben, die aber auch detaillierte technische Probleme klären möchten

- Systemadministratoren, die bereits viel Erfahrung mit Cloud-Computing gesammelt haben und Unterstützung bei komplexen Cloud-Projekten benötigen

- Nutzer aus Fachabteilungen, die Cloud-Dienste (besonders SaaS) nutzen, um sich nicht um die technischen Details kümmern zu müssen, und daher wenig technisches Wissen mitbringen

Je nachdem wie die Zielgruppe im Anwenderunternehmen eingeschätzt wird, sollte ein passender Provider ausgewählt werden. Neben „Verständigungsproblemen“ stellt die richtige Wahl auch sicher, dass die bestehenden Support-Prozesse besser mit den Prozessen des Cloud-Anbieters in Einklang gebracht werden können. Dabei spielt natürlich auch das Support-Personal auf Provider-Seite eine Rolle. Hier ist wichtig, dass es sich um ausreichend geschulte und fähige Mitarbeiter handelt. Wendet sich beispielsweise immer die technisch versierte IT-Abteilung an den Support, welche das Problem vielleicht sogar schon identifiziert hat, so sollte sichergestellt sein, dass die Mitarbeiter nicht lange in Warteschleifen bei technisch nicht ausreichend geschulten Kundenbetreuern aufgehalten werden.

Beispiel aus der Praxis:
Ein sehr positives Beispiel in Bezug auf den Support durch einen SaaS-Anbieter haben wir während der Vorbereitungen dieses Leitfadens erfahren. Ein KMU wollte seine internen Kreativprozesse durch eine SaaS-Lösung unterstützen. Während der Nutzung im Haus traten einige Defizite des Dienstes zu Tage. Nach einer klärenden E-Mail-Kommunikation mit dem Anbieter fand dieser die vorgeschlagenen Erweiterungen sehr sinnvoll. Bereits wenige Tage später konnte das Unternehmen die „Beta-Version“ der neuen Funktionen nutzen – wie natürlich auch alle anderen Nutzer des Dienstes.

Einige Cloud-Anbieter geben auch für die Kundenbetreuung Dienstgütegarantien im SLA ab. Sie garantieren dann die mittlere Antwortzeit (Mean-Time-to-respond) oder die durchschnittliche Reparaturdauer (Mean-Time-to-repair) im Problemfall. Außerdem können verschiedene Dringlichkeitsstufen vorgesehen sein (z. B. „Systemausfall“ ggü. „Feature Request“). Schließlich können auch die Schritte zur Eskalation formalisiert werden [18].

Grundsätzlich gilt jedoch häufig: je größer die Unternehmung, desto mühsamer ist die Support-Anfrage, falls man die normale Hotline benutzt. Um im Bedarfsfall größeren Ärger zu vermeiden, sollte die Kundenbetreuung daher bereits im Vorfeld geprüft und als Kriterium in die Anbieterauswahl einbezogen werden.

4.4.3 Kommunikation mit dem Anbieter im Problemfall

Ein sehr wichtiger und leider oft viel zu spät beachteter Aspekt ist die Kommunikation mit dem Cloud-Anbieter im Problemfall. Als erstes ist zu beachten, dass eine Situation nicht notwendigerweise für beide Parteien einen „Problemfall“ darstellt. Es muss also im Fehlerfall zuerst identifiziert werden, in wessen Verantwortungsbereich das Problem fällt. Bereits dabei hilft es jedoch ungemein, wenn die Kommunikationskanäle zum Cloud-Anbieter wie oben beschrieben im Vorfeld festgelegt wurden und die Kooperation der Support-Mannschaft gesichert ist. Selbst wenn das Problem durch das Anwenderunternehmen verschuldet wurde, kann der Anbieter durch die bessere Kenntnis der zugrunde liegenden Systeme und den physischen Zugriff auf die Hardware oft effektivere Lösungen realisieren. Besonders für den Notfall empfiehlt es sich, in regelmäßigen Abständen die Aktualität der Daten zu prüfen, um z. B. nicht erst in einer dringenden Situation zu erfahren, dass der entsprechende Ansprechpartner inzwischen in einem anderen Unternehmen arbeitet.

Neben der reinen Kommunikation sollten auch die Aktionen für den Notfall abgestimmt werden. Existieren im eigenen Unternehmen bereits Maßnahmen zum betrieblichen Kontinuitätsmanagement (engl. Business Continuity), so können diese mit den entsprechenden Maßnahmen auf Anbieterseite koordiniert werden. Ansonsten ist es empfehlenswert, zusammen mit dem Anbieter einen Ablaufplan für den Notfall auszuarbeiten. Ein seriöser Cloud-Anbieter sollte bereits einen passenden, generischen Plan als Grundlage anbieten können.

4.5 Zusammenfassung

Cloud-Computing wird auch in den nächsten Jahren noch keine „Stangenware“ werden. Die Anbieter führen kontinuierlich neue Funktionalitäten ein und experimentieren mit neuen Technologien und Geschäftsmodellen. Derzeit entwickelt sich der Markt noch zügig und die Anbieter integrieren neu entstehende Technologien schnell in ihre Dienste. Gleichzeitig werden existierende Schwachstellen ausgebessert.

In der aktuellen Situation sollten Unternehmen daher denjenigen Anbieter wählen, der momentan am besten auf die Problemstellung und die Situation in der eigenen Unternehmung passt. Allerdings muss besonders im Bereich des Cloud-Computing eine regelmäßige Prüfung durchgeführt werden, ob diese Übereinstimmung immer noch gegeben ist und ob es nicht inzwischen deutlich bessere Alternativen gibt. Dazu ist es nötig, sich möglichst wenig an den Provider anzupassen (siehe Abschnitte 4.1.3 und 4.1.4 zu den Lock-in-Effekten). Die Migrationskosten beim Anbieterwechsel sollten nicht unterschätzt werden. Um einen zuverlässigen Anbieter auszuwählen bietet sich eine ausführliche Internet-Recherche in Foren, Blogs und Web-2.0-Diensten wie Twitter an, die deutlich besser Auskunft geben können als traditionelle Auswahlverfahren.

Abschließend bleibt zu bemerken, dass bei der Anbieterwahl mindestens drei ähnliche Anbieter anhand eines strukturierten Anforderungskatalogs untersucht und getestet werden sollten, bevor intern eine Entscheidung getroffen wird. Zu beachten ist auch, dass nicht immer alle wichtigen Informationen auf den Webseiten der Anbieter dargestellt sind. Für größere Projekte sollte daher immer telefonisch oder schriftlich nach weiteren Informationen gefragt werden.

Im Hinblick auf den Vergleich der Kosten sollte – wie schon bei der Grundsatzentscheidung für eine Cloud-Lösung – immer eine ganzheitliche Sicht verwendet werden, z. B. nach dem Ansatz der Total Cost of Ownership (TCO). Nur so werden auch die unterschiedlichen Mitarbeiteranforderungen, Einarbeitungszeiten, Gebühren und Maßnahmen zur Risikominimierung erfasst. Cloud-Angebote dürfen nicht nur – wie von den Anbietern häufig propagiert – mit den reinen Hardwarekosten verglichen werden.

Als Hilfestellung bei der Auswahl des Cloud-Anbieters sind auf der folgenden Seite die wichtigsten Aspekte der Wahl des Anbieters in Form von zehn Leitfragen aufgelistet. Natürlich handelt es sich auch bei dieser Liste nur um ein Instrument für eine erste Auswahl, die durch eine intensivere Analyse der Anbieter verfeinert werden muss.

10 Fragen

Zehn Leitfragen zur Wahl des Anbieters

1. Wie etabliert, groß und zuverlässig ist der Cloud-Anbieter nach eigener Meinung und nach Meinung seiner (un-)zufriedenen Kunden? Kann der Cloud-Anbieter dies durch relevante Zertifizierungen z. B. nach SAS 70 oder ISO/IEC 27001 belegen?
2. Wie viel Kontrolle kann das Unternehmen über den Cloud-Anbieter ausüben? Wie können die tatsächliche Umsetzung der versprochenen Maßnahmen und Leistungen vor Ort überprüft werden?
3. Ist und bleibt das Anwenderunternehmen alleiniger Eigentümer seiner Daten? Stellt ihm der Cloud-Anbieter (auf Anfrage oder regelmäßig) eine *vollständige* Kopie Ihrer Daten in für Sie verwendbarer Form zur Verfügung?
4. Wo und in welchen Rechenzentren werden die Daten durch den Anbieter verarbeitet? Bieten alle Rechenzentren dasselbe Serviceniveau?
5. In welchem Ausmaß muss das Anwenderunternehmen seine Prozesse und Systeme anpassen, um sinnvoll mit dem Anbieter zusammenarbeiten zu können?
6. Erfüllt der Cloud-Service alle notwendigen gesetzlichen Vorschriften für die spezielle Branche? Wird insbesondere das BDSG vollständig umgesetzt?
7. Wie umfangreich, flexibel und praxistauglich sind die Möglichkeiten, individuelle SLAs zu vereinbaren?
8. Wie umfangreich ist die durch den Anbieter implementierte Backupstrategie und wie flexibel können Daten wiederhergestellt werden?
9. Sind die Support-Leistungen des Anbieters für die Bedürfnisse des Cloud-Nutzers angemessen, z. B. in Bezug auf Art der Kommunikation, Erreichbarkeit, Ausbildung des Support-Personals?
10. Wie überprüft der Anbieter seine Mitarbeiter bzw. Dienstleister vor der Einstellung bzw. Auftragsvergabe?

5 Sicherheitaspekte von DaaS-Angeboten

Das Wichtigste in Kürze

- Sicherheit in der Cloud ist ein zentrales Thema. Einige einfache Maßnahmen verhelfen bereits zu einer soliden Grundlage.
- Im Vorfeld müssen die eigenen Anforderungen an die Sicherheit genau geklärt werden.
- Es überwiegen die **organisatorischen** Probleme. Unter anderem müssen die Mitarbeiter sensibilisiert und geschult werden sowie bestehende und neue Sicherheitskonzepte integriert werden.
- Auf **technischer** Seite müssen sowohl die Infrastruktur als auch die Daten geschützt werden. Ansätze für ersteres sind bekannt. Der Aspekt der Datensicherheit ist zwar teilweise auch bekannt, stellt aber größere Hürden in den Weg, da viele Anbieter nur ein durchschnittliches, aber kein hohes Schutzniveau erbringen.
- Insgesamt ist die Sicherheit von Cloud-Diensten nicht notwendigerweise schlechter als von Lösungen im eigenen Haus.

Im Rahmen der aktuellen Entwicklung im Bereich des Cloud-Computings gibt es noch immer eine große Unklarheit, wie Sicherheit auf den verschiedenen Ebenen in der IT-Landschaft erreicht werden kann. Die unklare Situation verleitet viele IT-Verantwortliche zu der Aussage, dass die Sicherheit in der Cloud für sie als das größte Problem erscheint (vgl. [19, S. 31]). Eine aktuelle Umfrage unter KMU mit dem Schwerpunkt auf dem Münsterland[1] zeigt ebenfalls, dass die Entscheider um die Sicherheit besorgt sind: die Vertraulichkeit der eigenen Daten gegenüber Dritten ist die wichtigste Voraussetzung für die Cloud-Nutzung. Interessanterweise zeigen die Antworten ein ausgeprägtes Misstrauen gegenüber den Cloud-Anbietern, denn an zweiter Stelle wird auch die Vertraulichkeit der Daten gegenüber dem Provider gefordert – noch deutlich vor einschlägigen Zertifikaten, z. B. nach ISO/IEC 27001. Tatsächlich gibt es hinsichtlich der Datenvertraulichkeit noch einige ungeklärte Aspekte, wie dieser Abschnitt zeigen wird. Das Hauptproblem liegt aber eigentlich nicht in der Sicherheit, sondern in den Steuerungs- und Kontrollmöglichkeiten, die der Cloud-Nutzer über den Cloud-Anbieter haben möchte. Nach dem aktuellen Stand der Technik ließen sich viele Cloud-Szenarien prinzipiell sicher realisieren. Der eigentlich problematische Punkt ist, wie das Anwenderunternehmen bestimmte Richtlinien vorgeben und ihre Einhaltung durch den Cloud-Anbieter sicherstellen kann (vgl. [7]).

[1] Eine ausführliche Ausarbeitung der Studie durch die DBIS Group ist zurzeit in Vorbereitung. Bei Interesse wenden Sie sich bitte an die Autoren dieses Leitfadens. Die Kontaktdaten finden Sie auch unter `http://dbis-group.uni-muenster.de/`.

Dieses Kapitel soll daher zum einen für die verschiedenen zu beachtenden Aspekte sensibilisieren und – wo möglich – erste Schritte oder Handlungsempfehlungen nahe legen. In der Kürze dieses Leitfadens ist es jedoch unmöglich, die Erstellung eines vollständigen Sicherheitskonzepts umfassend zu beschreiben. Hierzu sei auf die einschlägige Literatur verwiesen, wie z. B. [8, 19, 32], die Dokumentation im Internet, z. B. [3], oder die umfangreiche Dokumentation zum IT-Grundschutz, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht[2] [22, 23, 24, 25, 27].

5.1 Vorgehen für die Bewertung der Risiken in der Cloud

Häufig wird als Vorteil von Cloud-Computing genannt, dass „das Risiko“ einfach auf den Cloud-Anbieter abgewälzt werden könne. Dies ist jedoch ein Trugschluss. Obwohl sich gewisse Risiken, wie z. B. das Investitionsrisiko, teilweise sich auf den Anbieter übertragen lassen, „verpufft“ Risiko nicht einfach in der Cloud (vgl. [7]). Es wird auch niemals vollständig an den Cloud-Anbieter abgegeben werden, da eine Beeinträchtigung des Anbieters in den meisten Fällen Konsequenzen für seinen Kundenstamm hat. Es ist daher für eine ordentliche Bewertung der Cloud-Strategie essentiell, eine ganzheitliche Übersicht zu gewinnen und eine wohlüberlegte Menge von Verantwortung in die Cloud auszulagern, aber auch Überprüfungsmöglichkeiten und die eigene Verantwortung zu klären. Viele Vertrauens- und Risikoaspekte des Cloud-Computing sind noch weitgehend unerforscht und können daher gefährlich werden [7]. Nur eine gründliche Analyse im Vorfeld kann ein vernünftige Entscheidungsgrundlage für den Schritt zum Cloud-Computing liefern.

Im Hinblick auf die Sicherheit von Cloud-Angeboten heißt dies, dass zuerst festgelegt werden muss, welche Anforderungen an die Sicherheit von der wirtschaftlichen Seite her gestellt werden, bevor irgendeine sinnvolle Entscheidung getroffen werden kann, ob der jeweilige Cloud-Anbieter „ausreichend sicher“ ist (vgl. [18]). Erst auf Basis der individuellen Anforderungen kann ein Cloud-Anbieter evaluiert werden. Wie bereits in Abschnitt 3.3 erläutert, ist dabei die Entwicklung einer klaren Cloud-Strategie und eine stringente Umsetzung derselben sehr wichtig. Ein explizit benannter Sicherheitsbeauftragter sollte von Anfang an über die Umsetzung des Sicherheitskonzepts für die Cloud-Computing-Lösung wachen. Nur so lässt sich eine wirklich sichere Umsetzung gewährleisten. Dieser Bericht leistet dabei insofern Unterstützung, als dass die wichtigsten Themenbereiche diskutiert werden, die im Rahmen einer solchen Umsetzung behandelt werden müssen. Eine allgemeingültige Handlungsempfehlung kann jedoch nicht ausgesprochen werden.

5.1.1 Analyse der eigenen Anforderungen

Durch die Einbindung von Cloud-Diensten werden die IT-Systeme im Unternehmen immer komplexer. Verteilte Systeme bestehen aus einer Vielzahl von Komponenten und Teilsystemen auf unterschiedlichen Schichten. Ein systematisches Vorgehen muss dabei Schicht für Schicht die relevanten Sicherheitsaspekte untersuchen. Hilfestellung bei einer vollständigen

[2] https://www.bsi.bund.de/gshb

Analyse gibt eine Taxonomie wie die des Fraunhofer SIT [32] und die Bausteine aus den IT-Grundschutzkatalogen [27]. Im Folgenden werden die wichtigsten Aspekte der jeweiligen Schichten kurz angerissen, um einen ersten Eindruck von den notwendigen Schritten zu erhalten.

Zusätzlich ist auch die Vorgehensweise nach den *IT-Grundschutz-Standards* des BSI zu empfehlen [22, 23, 24, 25]. In diesen Standards, früher als „IT-Grundschutz-Handbuch“ bekannt, veröffentlicht das BSI empfohlene Vorgehensweisen zu Erstellung eines vollständigen Sicherheitskonzepts. Zusätzlich zur Beschreibung des Vorgehen bietet das BSI auch die sogenannten *Grundschutz-Kataloge* an, in denen mögliche Gefährdungen und Gegenmaßnahmen aufgeführt sind. Die Dokumentation zum IT-Grundschutz ist zwar noch nicht explizit an die neuen Gegebenheiten des Cloud-Computings angepasst. Jedoch lässt sich ein auf dieser Basis erstelltes Sicherheitskonzept für das Unternehmen auch um die Cloud-Dienste erweitern und bietet daher eine gute Ausgangsposition. Alle Dokumente zum IT-Grundschutz finden sich auf `https://www.bsi.bund.de/gshb`.

Schutzziele

Um die eigenen Anforderungen an die Sicherheit zu verstehen, müssen zuerst die grundlegenden Schutzziele verstanden werden. An dieser Stelle werden sie nur sehr kurz aufgelistet. Für eine genauere Beschreibung sei auf die einschlägige Literatur, z. B. [8, 32], verwiesen. Die drei zentralen Schutzziele für jegliche Informationssysteme sind:

1. **Vertraulichkeit:** das System ermöglicht keine unautorisierte Informationsgewinnung [8, S. 8]

2. **Integrität:** die Daten im System können nicht unbemerkt und unautorisiert manipuliert werden [8, S. 7]

3. **Verfügbarkeit:** berechtigte Nutzer können nicht durch unautorisierte Aktionen externer Akteure in ihrer Nutzung des Systems beeinträchtigt werden (in Anlehnung an [8, S. 10] und [32, S. 23])

Diese Schutzziele müssen auf jeden Fall berücksichtigt werden, da dies auch durch den Gesetzgeber, z. B. in §10 Abs. 2 DSG NRW, gefordert wird. Auch aus praktischen Erwägungen heraus müssen diese drei Ziele adressiert werden, weil sonst ein sinnvoller Einsatz des Systems im Unternehmenskontext nicht gewährleistet werden kann.

Im Rahmen von Cloud-Computing liegt es nahe, zwei weitere, abgeleitete Schutzziele zu beachten:

4. **Authentizität:** die Identität des Kommunikationspartners bzw. Akteurs (sei es ein System oder ein Subjekt) kann eindeutig bestimmt werden

5. **Verbindlichkeit** (engl. Non-repudiation)**:** Aktionen im System lassen sich eindeutig Subjekten zuordnen und die Ausführung einer Aktion durch ein Subjekt kann auch im Nachhinein nicht abgestritten werden

Diese beiden Schutzziele sind besonders wichtig in Umgebungen, in denen mehrere Akteure beteiligt sind. Dies trifft also auf fast jedes IT-System im Unternehmenseinsatz zu, insbesondere auch auf Cloud-Anwendungen.

Je nach Anwendungsfall können eventuell auch noch weitere Schutzziele aufgenommen werden:

6. **Schutz der Privatsphäre:** das System bietet durch Anonymisierung oder Pseudonymisierung einen Schutz vor der Zuordnung schützenswerter Daten zu einer Person

7. **Transparenz:** die Verarbeitung der Daten im System erfolgt gut dokumentiert und einfach nachvollziehbar

Speziell für das Szenario von Database-as-a-Service müssen spezielle Facetten der genannten Schutzziele berücksichtigt werden. Zusätzlich muss jedoch auch ein weiteres spezifisches Schutzziel miteinbezogen werden:

8. **Inferenzkontrolle:** das System muss sicherstellen, dass durch das Zusammenführen für sich genommen nicht schützenswerter Einzelinformationen keine weiteren Informationen abgeleitet werden können, die dem betreffenden Subjekt eigentlich nicht zugänglich sein dürften (vgl. [8, S. 9])

Dieses Problem tritt besonders in Datenbanken auf. In diesen kann sich beispielsweise durch geschicktes Formulieren von Abfragen auf pseudonymisierten Daten die Ergebnismengen unter Umständen so stark einschränken lassen, dass eine Zuordnung zu einer Person möglich wird. Für eine ausführlichere Beschreibung siehe [6].

5.1.2 Analyse der Anbieter

Um die Schutzziele zu gewährleisten müssen einerseits im Anwenderunternehmen entsprechende Maßnahmen getroffen werden. Andererseits ist aber im Rahmen von Cloud-Computing besonders auch der Cloud-Anbieter in der Pflicht. Um eine Erfüllung der Schutzziele sicherzustellen, muss daher der Anbieter gründlich untersucht werden. Es gibt drei prinzipielle Möglichkeiten, diese Analyse des Anbieters durchzuführen:

1. Analyse der Situation vor Ort durch einen Besuch beim Provider

2. Analyse der vorhandenen Dokumentation und Antworten auf entsprechende Anfragen

3. Vertrauen in die Untersuchung durch neutrale Dritte

Während bei der Analyse der eigenen Systeme mit der vollen Kooperation durch das jeweilige Fachpersonal zu rechnen ist, muss das bei der Analyse der Cloud-Anbieter nicht so sein. Gerade bei größeren Anbietern ist es dem einzelnen Kunden nicht möglich, detaillierte Einblicke in die Systeme des Anbieters zu erhalten. In diesem Fall entfällt die erste Möglichkeit und die Analyse muss sich auf vorhandene Dokumente, Aussagen des Anbieters und durch Dritte attestierte Tatsachen stützen.

Für den dritten Fall hat der Anbieter die entsprechenden Zertifikate oder Zeugnisse hoffentlich bereits vorliegen. Relevante Urkunden sind beispielsweise Zertifikate nach ISO/IEC 27001 und SAS 70. Auf jeden Fall müssen die zertifizierten Aspekte gründlich analysiert werden, wie bereits in Abschnitt 4.3.1 beschrieben. Wenn es spezielle Compliance-Anforderungen gibt, so sollte im Vorfeld eine schriftliche Erklärung des Providers eingeholt werden, dass entsprechende Kontrollen (Audits) durchgeführt werden dürfen.

Inhaltlich sollte die Analyse natürlich einerseits prüfen, ob die im eigenen Unternehmen identifizierten Anforderungen an den Cloud-Dienstleister erfüllt werden. Zusätzlich bietet es sich jedoch auch an, weitere Aspekte in die Untersuchung mit aufzunehmen, um ein umfassenderes Bild von der Seriosität des Cloud-Anbieters zu erhalten. Insbesondere sollte überprüft werden, welche Prozesse und Technologien der Anbieter selbst etabliert hat, um mögliche Angriffsvektoren und Schwachstellen zu identifizieren und zu adressieren. Wichtig ist auch zu erfahren, welche Prozesse beim Anbieter gewährleisten, dass alle Sicherheitsmechanismen korrekt funktionieren, und welche Maßnahmen für den Fehlerfall vorgesehen sind. Dazu gehört auch eine Reaktion auf mögliche Angriffe auf die Cloud-Dienste oder -Infrastruktur.

5.2 Das kleine Einmaleins

Durch die Umsetzung von drei einfachen Punkten kann oft schon ein vernünftiger Anfang für die Cloud-Sicherheit gemacht werden (vgl. [32]):

1. **Unterstützende Dienste des Cloud-Anbieters verwenden:** Die meisten Anbieter offerieren bereits einige grundlegenden Sicherheitsfunktionen wie z. B. Firewalls sowie andere grundlegende Zusatzdienste aus den Bereichen Integration, Bereitstellung, Verteilung und Sicherheit. Diese Funktionen sollten auf jeden Fall genutzt werden, da die Anbieter in der Regel ein sehr gutes Verständnis für die schutzbedürftigen Schwachstellen der eigenen Services haben. In einem hybriden Ansatz kann der Dienst eventuell um eigene dedizierte Hardware ergänzt werden. Wenn der Cloud-Anbieter seine IT-Landschaft vernünftig verwaltet, kann mithilfe dieser Dienste ohne großen Aufwand ein recht ordentliches Sicherheitsniveau erreicht werden. Ein guter Cloud-Anbieter steht auch im Rahmen der vereinbarten Support-Leistungen bei der sicheren Einbindung seiner Services beratend zur Seite.

2. **Schutz der Netzinfrastruktur:** Die Cloud-Dienste werden üblicherweise über das Internet bezogen. Daher sollte darauf geachtet werden, dass alle Verbindungen zum Anbieter verschlüsselt sind. Oft reicht eine Verwendung von SSL bzw. TLS („HTTPS“) anstelle der unsicheren Verbindung per HTTP. Etwas ausgefeiltere Szenarien können VPNs ausnutzen, Firewalls verschiedener Ebenen und redundante Kommunikationskanäle umfassen. Auf jeden Fall ist die Netzinfrastruktur hinsichtlich der Sicherheit und Zuverlässigkeit als besonders schutzbedürftig einzustufen.

3. **Kein Verzicht auf Sicherheitskonzepte aus ökonomischen Überlegungen heraus:** Wann immer Sicherheitsmechanismen diskutiert werden, sollten fachliche Argumente

Tabelle 5.1: Übersicht über die Verteilung der Verantwortlichkeit zwischen Cloud-Anbieter und -Nutzer auf den drei Service-Ebenen.

Ebene	Provider	Nutzer	Bsp. für Maßnahmen
SaaS	Sicherer *Betrieb* der Anwendung	Sichere *Konfiguration* der Anwendung	Sinnvolle Vergabe von Rechten, sichere Passwörter
PaaS	Sicherer Betrieb der Plattform	Sichere Konzeption, Programmierung und Konfiguration der Anwendung	Sicheres Konzept für die Applikationslogik, Überprüfung von Stored Procedures
IaaS	Sicherer Betrieb der Hardware, des Host-Betriebssystems und der Virtualisierungsschicht	Sicherer Betrieb und Konfiguration der virtualisierten Software	Härtung der Software, Sichere Konfiguration des DBMS

zu einer Entscheidung für oder gegen bestimmte Maßnahmen führen. Es ist nicht ratsam, auf Basis rein ökonomischer Überlegungen auf bestimmte Aspekte des Sicherheitskonzepts zu verzichten, wenn diese durch fachliche Argumente, z. B. etablierte Sicherheitsrichtlinien im Unternehmen, motiviert werden. Auch wenn dieser Hinweis trivial klingen mag, so werden in der Praxis vielfältige Argumente zum Verstoß gegen diesen Grundsatz verführen. Die gesetzlichen Anforderungen zum Datenschutz erfordern beispielsweise in der Praxis fast zwingend den Einsatz von kryptographische Verfahren. Diese sind jedoch in den Standardprodukten vieler Cloud-Anbieter nicht vorgesehen, so dass der sichere Einsatz dieser Angebote erschwert und damit teurer wird (vgl. [33]).

5.3 Organisatorische Aspekte

Bei der Sicherheit im Cloud-Computing geht es nicht so sehr um neue *technische* Aspekte, sondern um *organisatorische* Aspekte wie die Absprache und Verteilung von Verantwortung zwischen Cloud-Anbieter und Cloud-Nutzer. Es müssen trennscharfe Grenzen, sogenannte *Trust Boundaries*, gezogen werden, die festlegen, welche Aufgaben vom Provider erbracht werden und an welchen Stellen das Anwenderunternehmen Hand anlegen muss. Tabelle 5.1 gibt eine Übersicht über die generelle Aufteilung der Verantwortlichkeiten auf den verschiedenen Service-Ebenen und nennt beispielhaft einige typische Maßnahmen, die der Cloud-Nutzer selbst durchführen muss. Abgesehen von der Klärung der Verantwortlichkeiten, die je nach Anwendungsfall sehr unterschiedlich ausfallen können, gibt es viele generelle organisatorische Aspekte, von denen im Folgenden die wichtigsten kurz angerissen werden.

5.3.1 Sensibilisierung der Mitarbeiter für das Thema

Eine Vielzahl von Sicherheitsproblemen ist heute direkt oder indirekt auf die Mitarbeiter des eigenen Unternehmens zurückzuführen. Die Mehrheit der bekannt gewordenen Sicherheits-GAUs ist von eigenen Mitarbeitern oder Dienstleistern verursacht worden, welche die Schad-

software über ihre Laptops oder USB-Sticks ins Intranet des Unternehmens eingeschleust hatten. Das derartige Umgehen der Firewalls ist eine offene Hintertür, die alle Schutzmaßnahmen am Haupteingang unsinnig erscheinen lässt. Die Ursache solcher Sicherheitslücken ist dabei im leichtsinnigen Verhalten der IT-Nutzer zu finden und kann durch Technik nur begrenzt kontrolliert werden. Stattdessen ist es erforderlich, die Mitarbeiter für die Themen der IT-Sicherheit zu sensibilisieren.

Derartige Programme laufen neudeutsch unter dem Titel *Security Awareness* und werden bislang hauptsächlich bei großen Unternehmen aufgesetzt. Die Programme kommen offenbar hauptsächlich zustande, wenn es im Unternehmen einen Sicherheitsverantwortlichen gibt – zum Beispiel einen Chief Information Security Officer (CISO) –, der sie vorantreibt. Empfehlenswert ist es außerdem, die Programme in einen größeren Rahmen, ein Informationssicherheits-Managementsystem (ISMS), einzubetten.

Bewusstsein für IT-Sicherheit

Die Programme sollen Mitarbeiter aus IT- und Nicht-IT-Abteilungen gleichermaßen für Themen wie Sicherheitsrichtlinien, Bedrohungen und wirksame Gegenmaßnahmen aufklären (vgl. auch Abschnitt 5.4.1). Wie noch aus der Schulzeit bekannt, sind interaktive Maßnahmen dabei erfolgreicher als „Frontalunterricht“. Wird der Inhalt zudem durch für die Mitarbeiter persönlich interessante Aspekte, wie Sicherheit für den heimischen PC, aufgepeppt, ist die Teilnahme erfahrungsgemäß höher. Es muss aber nicht immer eine aufwändige Schulung sein: Auch weniger umfangreiche Maßnahmen wie Newsletter, Poster und kleine „Werbegeschenke“ können eine Erhöhung des Sicherheitsbewusstseins unterstützen. Selbstverständlich sollte hierbei eine Klassifikation der Mitarbeiter erfolgen, um solche, die mit sensibleren Daten hantieren, gründlicher zu schulen, als weniger risikobehaftete Mitarbeiter.

Die Messung des Erfolgs sowie der Akzeptanz der Kampagnen ist erfahrungsgemäß alles andere als trivial. Ein Erfolg wird sich auch nicht nach der ersten Veranstaltung einstellen, sondern erst im Laufe mehrerer Monate oder sogar Jahre. Nichtsdestotrotz ist die Sensibilisierung der Mitarbeiter für die IT-Sicherheit ein zentraler Faktor für eine sichere Gesamtlösung.

5.3.2 Integration in ein bestehendes Sicherheitskonzept

Wie sich in Abschnitt 5.4 zeigen wird, ergeben sich durch das Cloud-Computing nicht zwangsläufig grundlegend neue Problemstellungen in Bezug auf das Sicherheitskonzept. Existiert im Unternehmen bereits ein gut ausgearbeitetes Sicherheitskonzept, so ist es daher oft relativ unproblematisch, dieses um „Cloud-Aspekte“ zu erweitern. Wichtig ist eine tatsächliche Integration in das bestehende Konzept, inklusive einer Versicherung, dass die entsprechenden Maßnahmen auch angewandt und durchgesetzt werden. Unter Umständen müssen bestehende Systeme für die Integration von Cloud-Diensten angepasst werden. Auch diese Änderungen sind im Sicherheitskonzept zu berücksichtigen, um z. B. weiterhin eine zentrale Verwaltung der IT-Systeme zu gewährleisten. [32]

Außerdem müssen die Verantwortlichkeiten geklärt werden, damit im Fall eines dringenden Handlungsbedarfs nicht erst ein Pokern zwischen den Abteilungen anfängt, welche von ihnen nun Ressourcen und Mitarbeiter aufwenden muss, um die Probleme zu beheben. Je nach Cloud-Dienst, der zur Debatte steht, muss diese Frage nämlich gar nicht eindeutig sein. Sollte der Dienst dem Chief Operating Officer zugeordnet werden oder eher dem Chief Information

Officer? Oder ist es sogar eher eine Aufgabe für die entsprechende Fachabteilung?

5.3.3 Herstellen einer Vertrauensbeziehung zwischen Cloud-Konsument und Cloud-Anbieter

Während beim klassischen IT-Outsourcing eine recht konkrete Zusammenarbeit mit dem Personal des externen Dienstleisters üblich ist, kann es im Kontext des Cloud-Computing sogar soweit kommen, dass überhaupt keine menschliche Interaktion mehr nötig ist. Durch den hohen Automatisierungsgrad der Systeme (vgl. Abschnitt 2.1.3) kann das Anwenderunternehmen vollständig in Selbstbedienung die nötige Konfiguration vornehmen. Erst bei schwierigeren Problemstellungen oder im Fehlerfall kommt es dann noch zu einer Kommunikation mit dem Anbieter. Aus diesem Grund sollte ein Unternehmen vor der Nutzung der Cloud-Dienste ein Treffen mit dem Anbieter vereinbaren, um vor Ort ein Bild von den Rechenzentren, den Mitarbeitern, der Sicherheit und den Prozessen des Anbieters zu bekommen. Durch die konkreten Kontakte zu Mitarbeitern entsteht auch eine gewisse Vertrauensbasis, die vieles erleichtern kann. Bei dem Besuch sollten zudem Ansprechpartner vereinbart werden, die bei Fragen oder Problemen kontaktiert werden können [32]. Auf diese Weise wird die Akzeptanz für die Cloud-Lösung auch bei den eigenen Mitarbeitern steigen.

5.3.4 Verwaltung von kryptographischen Schlüsseln

Ein weiterer kritischer Punkt für die Umsetzung sicherer Cloud-Dienste ist die Verwaltung der kryptographischen Schlüssel, auf Englisch *Key Management* [19, S. 69]. Je nachdem, wie hoch die Anforderungen an die Datenvertraulichkeit sind, kann ein ausgefeiltes Schlüsselmanagement aufseiten des Anbieters erforderlich sein. Da dies jedoch organisatorisch und technisch schnell komplex wird, scheuen sich die meisten Anbieter, eine entsprechende Lösung anzubieten. Falls die Sicherheitsanalyse jedoch ergibt, dass ein ausgefeiltes Schlüsselmanagement erforderlich ist, so sollte geprüft werden, dass der Anbieter die einschlägigen *Best Practices* umsetzt (vgl. [4]):

- Die Administratoren des Cloud-Anbieters sollten keinen Zugriff auf die Schlüssel haben.
- Verschlüsselungsschlüssel sollten niemals in Klartext offen gelegt werden.
- Zugang zu Schlüsselverwaltungsfunktionen sollten eine separate Authentisierung erfordern. Es empfiehlt sich zusätzlich die Anwendung des Vier-Augen-Prinzips.
- Im Speicher zwischengespeicherte Schlüssel müssen vor unbefugtem Zugriff geschützt sein.
- Die Schlüssel müssen auf sichere Art und Weise archiviert werden.
- Die Replizierung der Schlüsseln muss auf sichere Art und Weise erfolgen.

Insgesamt gilt, dass der Umgang mit den Schlüsseln sehr penibel reguliert und überwacht werden sollte. Auf der technischen Seite sind dann selbstverständlich noch weitere Aspekte zu prüfen, z. B. ob alle relevanten Daten auch ausreichend sicher und mit verschiedenen Schlüsseln verschlüsselt werden.

5.3.5 Einsatz von Service-Level-Agreements (SLAs)

Ein elementarer Aspekt bei der Nutzung von Cloud-Services ist die Vereinbarung geeigneter Service-Level-Agreements (SLAs), in denen alle Rechte und Pflichten der beteiligten Akteure festgeschrieben werden müssen. Die von den Cloud-Anbietern vorgefertigten SLAs sind allerdings häufig unzureichend, so dass sie kritisch überprüft werden sollten. Bei Bedarf müssen individuelle Vereinbarungen ausgehandelt werden, wobei die Rechtsabteilung des Unternehmens und insbesondere auch die für die Sicherheit verantwortlichen Mitarbeiter frühzeitig in die Vertragsgestaltung einbezogen werden sollten. Auf diese Weise kann eine Praxistauglichkeit und Durchsetzbarkeit der SLAs sicher gestellt werden [32, 3].

Zusätzlich sollten die Anforderungen der Sicherheitsverantwortlichen in Bezug auf Metriken und Standards in die SLAs einfließen, um das eigene Sicherheitsmanagement, aber auch die Erfüllung aller regulatorischen Anforderungen zu ermöglichen. Besondere Aufmerksamkeit erfordert die Dokumentation und Nachvollziehbarkeit (Überprüfbarkeit) der Umsetzung seitens des Anbieters [3]. Die Erfüllung der SLAs sollte möglichst automatisiert prüfbar sein, um sowohl Anbieter als auch Nutzer unnötigen Aufwand zu ersparen.

Bei aller Freiheit, die manche Anbieter bei der Gestaltung der SLAs einräumen mögen, sollte trotzdem klar sein, dass jede Abweichung von dem Standard-SLA des Anbieters zusätzliche Kosten nach sich zieht. Die monetären Vorteile des Cloud-Computings können sich auf diese Weise schnell relativieren. Andererseits bieten manche Cloud-Anbieter auch gar keine Möglichkeit an, neben den Standardverträgen weitere individuelle Vereinbarungen zu treffen. Derzeit muss dieser Aspekt also leider für den Einzelfall geprüft werden.

5.3.6 Überprüfung und Einhaltung des Sicherheitskonzepts

Eine Überprüfung, ob das Sicherheitskonzept sowohl im eigenen Unternehmen als auch durch den Cloud-Anbieter eingehalten wird, ist alles andere als trivial. Wegen der Vielzahl von Einflussfaktoren kommt hier nur ein koordiniertes Vorgehen durch eine zuständige Stelle in Frage. Im Hinblick auf vertraglich festgelegte Messgrößen empfiehlt es sich, diese möglichst automatisiert zu überwachen und nur bei Über- oder Unterschreitung bestimmter Meldegrenzen aktiv zu werden. Wer diese Überwachung vornimmt muss eindeutig zugewiesen sein. In der Regel übernimmt dies der Chief Information Security Officer (CISO) des Unternehmens – so es ihn gibt. In der ITIL finden sich bewährte Vorgehensweisen zur Installation eines ISMS im Unternehmen. Ähnliche Kontrollen beschreibt auch ISO/IEC 27001.

Sollten diese Standards für das eigene Unternehmen als zu viel des Guten gesehen werden, so sind trotzdem strukturierte Prozesse für das Sicherheitsmanagement Pflicht. Die Empfehlung lautet, einen Teil des durch Cloud-Computing gesparten Gelds in zusätzliche Sicherheitsprüfungen des Cloud-Anbieters und des Cloud-Dienstes zu investieren. In diesem Zusammenhang ist es

wichtig, die Messgrößen und (internen) Standards, die zur Messung der Effektivität des Sicherheitsmanagements benutzt werden sollen, bereits vor dem Auslagern der Systeme in die Cloud zu definieren. Als absolutes Minimum sollten aktuelle Messgrößen und die erforderlichen Änderungen verstanden und dokumentiert werden, da der Cloud-Anbieter höchstwahrscheinlich andere, möglicherweise inkompatible Maßstäbe anlegen wird [3].

Die Installation entsprechender Prozesse ist – falls sie noch nicht vorhanden sind – sehr aufwändig und zeitintensiv und darüber hinaus nicht Thema dieses Leitfadens. Das Cloud-Computing bringt keine neuen Themen, wohl aber eine Verschiebung der Schwerpunkte mit sich. Bewährte Vorgehensweisen sollten weiterhin funktionieren, wobei die detaillierten Hinweise und Maßnahmen in [3] die neue Akzentuierung in der Cloud erläutern. Zusammenfassend lässt sich die Cloud-Sicherheit ungefähr so wie die Supply-Chain-Sicherheit auffassen: In beiden Fällen müssen auch die vorgelagerten Glieder der Supply Chain, im Falle des Cloud-Computings die Dienstleister des eigentlichen Cloud-Anbieters, so weit wie möglich durchleuchtet werden.

5.3.7 Einbindung des Anbieters

Wie bereits in den Abschnitten 4.4.2 und 4.4.3 erläutert, ist die Klärung der Kommunikation mit dem Anbieter wichtig. Im Hinblick auf die Sicherheit der Systeme wird diese Wichtigkeit noch einmal verstärkt, da Sicherheitsprobleme und eventuelle Angriffe auf die Cloud offen und zeitnah mit dem Kunden besprochen werden sollten. Zusätzlich sollte geprüft werden, ob der Anbieter in ein Computer Emergency Response Team (CERT), manchmal auch treffender als Computer Security Incident Response Team (CSIRT) bezeichnet, und in das nationale IT-Krisenmanagement eingebunden ist [4].

5.4 Technische Aspekte

Nach Umsetzung der erforderlichen organisatorischen Maßnahmen aus dem vorangegangenen Abschnitt 5.3 sind selbstverständlich auch technische Aspekte der Sicherheit zu beachten. Die wichtigsten Themenbereiche werden im Folgenden vorgestellt. Zuerst steht dabei die Sicherheit der Cloud-Infrastruktur sowie der eigenen Infrastruktur im Unternehmen im Fokus. Anschließend wird das oft als zentral empfundene Thema der Datensicherheit und -vertraulichkeit beschrieben.

5.4.1 Sicherheit der Infrastruktur

Je nachdem wie die bisherige Systemlandschaft im Unternehmen aussieht, muss sich durch die Einführung von Cloud-Computing nicht unbedingt viel in Bezug auf die Sicherheitskonzepte ändern. Im Rahmen einer eigenen nichtöffentlichen Cloud (Private Cloud) gibt es z. B. keine wirklich neuen Aspekte. Hier kann das bewährte Vorgehen für die „traditionelle“ IT-Landschaft angewendet werden. Werden bereits externe Websites oder Datenbanken von Partnerunternehmen über das Internet genutzt, so muss sich ebenfalls nicht zwangsläufig allzu viel an der Bedrohungslage ändern, wenn nun auch noch eine öffentliche Cloud ins Spiel kommt. Da die

Situation durch die Nutzung von Cloud-Computing jedoch insgesamt komplexer wird, ist eine gründliche Analyse in jedem Fall zu empfehlen.

Netzwerkebene

Ein wichtiger Aspekt auf der Netzwerkebene ist, dass Außenstehende nun unter Umständen leichter Störungen von internen Prozessen verursachen können, indem sie die Cloud-Dienste, insbesondere eine DaaS, bzw. die Verbindung mit diesen angreifen. Letzteres ist im Zweifelsfall sogar einfacher, da grundlegende Routing-Protokolle und das Domain Name System (DNS) relativ schlecht gesichert und daher anfällig für Angriffe sind.[3] Im Gegensatz zu einer internen Datenbanklösung ist hier also die Verbindung über ein WAN einer größeren Gefahr ausgesetzt als vorher die LAN-Verbindung. Insbesondere größere Anbieter wie Amazon sind jedoch durch diverse technische Maßnahmen gegen solche Angriffe geschützt, so dass eine Gefahr eher von einem gezielten Angriff gegen das eigene Unternehmen ausgeht. Wie hoch das Risiko dafür ist, muss jedes Unternehmen selbst bewerten.

Allerdings muss nicht einmal ein gezielter Angriff Schuld an Verbindungsproblemen sein. Auch beispielsweise ein bei Bauarbeiten durchtrenntes Glasfaserkabel, eine Fehlkonfiguration eines Router im Internet oder Probleme mit der Infrastruktur des eigenen ISP können eine Störung verursachen. Je nachdem, wie wichtig die Verfügbarkeit der DaaS ist, führt dann oft kein Weg an einer redundanten Internetanbindung über mehrere, unabhängige Provider vorbei.

Abgesehen von der Anbindung an die Cloud ist auch zu beachten, dass die klassische Vorgehensweise zur Isolation von Netzwerkzonen und Anwendungsschichten nicht mehr greift. Während es im traditionellen Szenario möglich ist, beispielsweise Entwicklungs- und Produktionsserver in logisch getrennte Zonen und physisch getrennte Server innerhalb des LAN zu organisieren, steht in der Cloud normalerweise nur die Einordnung in „Domains“ zur Verfügung. Diese Einordnung ist aber rein organisatorisch, da die Systeme eventuell sogar auf demselben physischen Server laufen – die Entscheidung liegt allein beim Cloud-Anbieter. Einige Anbieter offerieren die Möglichkeit einer „Virtual Private Cloud“, also eines logisch abgetrennten Teils einer öffentlichen Cloud, die zur privaten Verwendung eingerichtet wird. Dieses Vorgehen bietet – je nach konkreter Ausgestaltung – einige der Vorteile, die aus dem eigenen Rechenzentrum bekannt sind, und kann insbesondere für DaaS-Lösungen, die in der Regel nicht direkt aus dem Internet angesprochen werden sollen, eine sehr sinnvolle Schutzvorkehrung sein.

Zwar ist die Netzwerksicherheit ein Aspekt, dem durch Cloud-Computing ein sehr großer Stellenwert zukommt. Realistisch betrachtet ändert sich durch die Einführung von Cloud-Computing für die meisten Unternehmen aber wahrscheinlich nicht viel. In vielen KMU existieren bereits Schnittstellen zu Partnerunternehmen oder sogar ganze Extranets, die einige Systeme des Unternehmens im Internet exponieren. In solchen Fällen müssen die neuen Risiken durch Cloud-Computing zwar genau analysiert werden, um sie passend zu adressieren. Oft sind aber keine grundlegend neuen Vorgehensweisen erforderlich, sondern etablierte Prozesse und Maßnahmen müssen lediglich erweitert werden (vgl. [19, S. 35–46]).

[3] Stichworte für die weitere Recherche hierzu sind z. B. „Border Gateway Protocol (BGP) prefix hijacking“, „DNS cache poisoning“ oder „DNS forgery“.

Host-Ebene

Ähnlich wie auf der Netzwerkebene ergeben sich auch auf der Host-Ebene durch Cloud-Computing keine grundlegenden neuen Sicherheitsaspekte. Zwar muss auch hier eine gründlichere Analyse durchgeführt werden, da der Host nun in der Regel aus dem gesamten Internet erreichbar ist, aber die prinzipielle Natur der Analyse bleibt wie gehabt.

Großes Augenmerk sollte bei der Analyse auf die Virtualisierungsschicht des Anbieters gerichtet sein. Im Rahmen eines Geheimhaltungsvertrags (Non-disclosure Agreement, NDA) sollte der Anbieter die Details zur gewählten Virtualisierungslösung offenlegen. In der Regel wird ein Hypervisor an der Virtualisierung beteiligt sein. In diesem Fall ist besonders auf die Sicherheitsmechanismen zu achten, die dafür sorgen, dass der Hypervisor nicht kompromittiert wird. Sollte der Hypervisor erfolgreich angegriffen werden, erhält der Angreifer Zugriff auf beliebige Daten des physischen Host. Verschiedene Beiträge auf einschlägigen Sicherheitskonferenzen beschäftigen sich mit möglichen (teilweise erfolgreichen) Angriffen auf aktuelle Virtualisierungssoftware (vgl. [19]).

In Bezug auf die Host-Sicherheit muss man als SaaS- und PaaS-Nutzer dem Anbieter vertrauen, dass er seine Aufgaben entsprechend der getroffenen Vereinbarungen ordentlich erfüllt. Diese Übertragung der Verantwortung ist aber gewollt, weil sie genau einen Vorteil des Cloud-Computing darstellt. Im Falle von IaaS-Angeboten muss der Dienstnutzer sich um zahlreiche Aspekte selbst kümmern. Speziell für DaaS-Angebote auf IaaS-Niveau erfordert dies, das Datenbankmanagementsystem (DBMS) genauso abzusichern, wie man es für einen physischen Datenbank-Host im Internet auch getan hätte.

Applikationsebene

Auf Applikationsebene muss die Cloud-Datenbank im Endeffekt genauso abgesichert werden, wie eine traditionelle Datenbank im Internet. Bei der Konfiguration geht man nach gewohntem Muster vor und schaltet jegliche ungenutzte Funktionalität ab bzw. schränkt die Rechte der Nutzer entsprechend ein. Falls möglich sollte der Zugriff auf das DBS nur von vorgegebenen IP-Adressen aus dem Firmennetz zugelassen werden. Auch sollten den Benutzerkonten immer nur die für den Zweck nötigen Rechte eingeräumt werden, z. B. keine Löschvorgänge für Programme, die nur Daten erzeugen, etc.

Abgesehen von diesen hinreichend bekannten Standardmaßnahmen trägt der Benutzer mit zunehmender Cloud-Nutzung auch immer mehr die Verantwortung seinen Webbrowser und Arbeitsplatz-PC abzusichern. Es gilt der neue Grundsatz: „Der Browser ist das Betriebssystem“. Daher müssen aktuelle Sicherheitsupdates sowohl für das Betriebssystem als auch für den Browser zeitnah eingespielt werden. Zusätzlich ist die Installation von Anti-Virus- und Anti-Malware-Software notwendig. Diese muss zudem mehrmals täglich aktualisiert werden, um ausreichenden Schutz zu bieten. Die Vorsichtsmaßnahmen sind insbesondere deshalb wichtig, weil der Zugriff auf die Cloud-Dienste häufig nur über ein Passwort oder – etwas besser – einen privaten Schlüssel gesichert ist. Angreifer versuchen inzwischen gezielt solche Daten auszuspähen, weswegen sie besonders sorgfältig gehandhabt werden müssen. Ein etabliertes IT-Sicherheitsmanagement vorausgesetzt, sind diese Aspekte jedoch bereits für Unternehmen Routine.

Denial-of-Service

Neben dem Ausspähen von Zugangsdaten bieten in die Cloud ausgelagerte Dienste auch mehr Angriffsfläche für gezielte Denial-of-Service-(DoS-)Angriffe auf Applikationsebene. Diese Angriffe können z. B. darin bestehen, dass eine enorme Anzahl von Anfragen an den Dienst gestellt wird. Diese Anfragen lassen sich in der Regel nur sehr schwierig von legitimen Anfragen unterscheiden und daher auch kaum filtern. Abgesehen von der Beeinträchtigung des Cloud-Dienstes, ist die neuartige Bedrohung darin zu sehen, dass diese Angriffe bares Geld kosten. Da der Anbieter die Ressourcennutzung abrechnet, bedeuten viele Anfragen auch hohe Kosten. Teilweise zielen die Angriffe inzwischen sogar auf genau diese Verursachung von Kosten ab, weswegen man bei dieser Art von Angriff auch von Economic-Denial-of-Sustainability (EDoS) spricht.

Mandantenfähigkeit als Sicherheitsaspekt

Als letzter, wichtiger Aspekt ist besonders für SaaS- und DaaS-Dienste zu klären, wie die Trennung der Daten verschiedener Mandanten vom Provider vorgenommen wird. Das Vorgehen ist wichtig, um zu erkennen, welche potentiellen Sicherheitsrisiken von einer gemeinsamen Speicherung der Daten verschiedener Kunden ausgehen. Prinzipiell eröffnen sich dem Anbieter viele Möglichkeiten, die Daten zu trennen. Oft werden einfach dieselben Tabellen verwendet, wobei die Datensätze dann über ein zusätzliches Feld „Kunden-ID“ dem jeweiligen Mandanten zugeordnet werden. Eventuell werden auch getrennte Tabellen oder sogar Datenbanken verwendet. Im besten Fall werden die Daten pro Kunde mit einem individuellen Schlüssel verschlüsselt abgespeichert, was jedoch in der Praxis wegen der komplexen Schlüsselverwaltung von den Cloud-Anbietern üblicherweise gescheut wird (vgl. Abschnitt 5.3.4). In jedem Fall ist es jedoch wichtig zu wissen, welche Maßnahmen eingesetzt werden, um die Sicherheit des Diensts insgesamt beurteilen zu können. Zwar wird der Anbieter versuchen, hierüber mit einem Verweis auf das Geschäftsgeheimnis Stillschweigen zu bewahren. Im Rahmen eines Geheimhaltungsvertrags könnte sich der Informationsaustausch aber eventuell realisieren lassen. Alternativ könnte eine externe Begutachtung ein entsprechendes Testat erbringen.

5.4.2 Sicherheit und Schutz der Daten

Als zentrales Problem des Cloud-Computing wird meistens die Sicherheit der eigenen Daten in der Cloud angeführt. Die Sorge ist nicht ganz unberechtigt, da ja auch zahlreiche gesetzliche Vorgaben zum Schutz der Daten erfüllt werden müssen (vgl. Abschnitt 3.1.3). Zur Erfüllung dieser Vorgaben müssen kryptographische Methoden eingesetzt werden, die allerdings häufig den Einsatz von standardisierten Applikationen erschweren. Einige Anbieter machen daher Abstriche bei der Sicherheit oder versuchen durch eigene Lösungen Abhilfe zu schaffen. Im Folgenden soll erörtert werden, an welchen Stellen das Anwenderunternehmen genau nachhaken muss.

Im Vorfeld zu klären ist, wer eigentlich bestimmte sensible Daten einsehen darf und wer nicht. Diese zentrale Problemstellung wird leider häufig übersehen, ist aber essentiell wichtig, um die Sicherheit der gesamten Lösung bewerten zu können. Es muss sowohl auf der Seite des Cloud-Anbieters als auch auf der Seite des Cloud-Nutzers klar definiert werden, welche Personen bestimmte, sensible Daten einsehen dürfen und welche Maßnahmen verhindern, dass Unbefugte Zugriff auf die Daten erlangen.

Ansätze zur Wahrung der Datenvertraulichkeit

Das für Unternehmen wohl wichtigste Schutzziel ist die Vertraulichkeit der Daten. Dabei ist zu beachten, dass die Datenvertraulichkeit zwei Teilaspekte aufweist:

1. Zugriffskontrolle (Access Control)

2. Schutz der eigentlichen Daten

Durch die Zugriffskontrolle stellt das System sicher, dass nur authentifizierte und autorisierte Benutzer auf die Daten zugreifen dürfen. Diese Kontrolle besteht bei den Cloud-Anbietern derzeit üblicherweise aus einem schwachen Authentisierungsverfahren („Benutzername + Passwort“) kombiniert mit einem dichotomen Autorisierungsverfahren (Anmeldung als „Administrator“ oder „Benutzer“). Für Unternehmen kann diese Zugriffskontrolle schnell unzulänglich sein, insbesondere wenn keine weiteren Rollen- und Rechteverwaltung vorgesehen ist.

Darüber hinaus müssen die Daten vor Zugriffen geschützt werden, die das System nicht per Zugriffskontrolle absichern kann. Die Datenvertraulichkeit soll dabei auch gegeben sein, wenn z. B. direkt auf das physische Speichermedium zugegriffen wird. Alle praxistauglichen Ansätze zur Datenvertraulichkeit involvieren heutzutage kryptographische Verfahren zur Verschlüsselung der Daten [19, S. 66 f.]. Die Verschlüsselung erfolgt mithilfe symmetrischer Verfahren – z. B. dem Advanced Encryption Standard (AES) – und sollte am besten direkt vom Provider unterstützt werden, um ordentliche Datenraten zu erzielen. Die meisten Anbieter übertragen jedoch diese Aufgabe gerne an den Kunden. Dadurch fallen aber gerade im DaaS-Bereich viele Vorteile wie serverseitige Auswertung von Abfragen weg, weil der Server nur noch verschlüsselte Daten sieht. In der Praxis gibt es also bei den meisten Angeboten nur zwei Möglichkeiten:

- den Cloud-Dienst ohne Verschlüsselung der Daten im Rechenzentrum des Providers nutzen,[4] was ein Sicherheitsrisiko darstellen und daher inakzeptabel sein kann, oder

- die Daten vor dem Senden an den Cloud-Dienst verschlüsseln, was jedoch den Cloud-Dienst oft zu einer überteuerten Backup-Lösung degenerieren lässt.

Zwar existieren einige Ansätze aus der Wissenschaft, die verschlüsselte Indexstrukturen oder partielle Unterstützung von Abfragen auf verschlüsselten Daten realisieren könnten.[5] Es sind sogar erste Schritte in Richtung einer vollständig homomorphen Verschlüsselung erfolgt, die erlauben würde, dass der Cloud-Anbieter ausschließlich mit verschlüsselten Daten arbeitete [11]. In der Praxis ist jedoch die einzige realisierbare Möglichkeit, dass der Cloud-Anbieter die Daten zumindest verschlüsselt auf der Festplatte ablegt – und selbst diese Möglichkeit besteht bei vielen Cloud-Anbietern noch nicht. Als Konsequenz müssen daher strikte Vereinbarungen über die Verarbeitung und Speicherung der Daten mit dem Dienstanbieter getroffen werden, um zumindest Transparenz über die tatsächliche Lage zu erhalten.

[4] Der Transportweg zum Rechenzentrum kann dabei natürlich trotzdem z. B. per SSL/TLS abgesichert werden.

[5] Vgl. [17] für eine Übersicht.

Sicherheit der Daten des Anbieters

Zusätzlich zur Sicherheit der eigenen Daten sollte auch darauf geachtet werden, welche Daten der Cloud-Anbieter sammelt und wie diese geschützt sind. Insbesondere in Bezug auf die in der Cloud gespeicherten Daten über den eigenen Kundenstamm ist es interessant zu wissen, welche Metadaten der Anbieter sammelt, wie er diese schützt und in welcher Form der Dienstnutzer diese Daten einsehen kann.

Abgesehen von den Daten, die Nutzer explizit mit dem Cloud-Dienst verarbeiten, fallen auch noch reichlich zusätzliche sicherheitsrelevante Daten an, z. B. diverse Log-Dateien oder Statistiken. Einerseits benötigt der Cloud-Anbieter diese Informationen, um die Funktionsfähigkeit seiner verschiedenen System, wie Firewall, Intrusion Prevention System (IPS) oder eigener Applikationen zu überwachen. Auch im Hinblick auf Zertifizierungen, digitale Forensik oder Analyse von Störungen (Incidents) werden diese Daten benötigt. Andererseits lassen sich auf Basis dieser Metadaten bereits zahlreiche Schlussfolgerungen über die Geschäftstätigkeit der Dienstnutzer ableiten. Reine Verbindungsdaten reichen beispielsweise aus, um Beziehungen innerhalb von sozialen Netzen zu charakterisieren. Auf Basis der Routing-Protokolle lassen sich so z. B. Großkunden identifizieren. Daher muss sichergestellt werden, dass auch für diese Daten die relevanten Schutzziele erreicht werden.

Weitere potentielle Probleme der Datenvertraulichkeit

Abgesehen von gezielten Angriffen oder Datenpannen kann die Datenvertraulichkeit auch durch zwei weitere, häufig nicht bedachte Ursachen verletzt werden (vgl. [33]):

- **Insolvenz des Providers:** Die Insolvenz eines Providers bedeutet nicht, dass alle Rechenzentren, die für den Cloud-Dienst genutzt wurden, ebenfalls insolvent sind. Rechenzentren werden außerdem im Falle einer Insolvenz höchstwahrscheinlich weiterverkauft. In beiden Fällen ist nicht klar, was mit den sensiblen Daten, die wahrscheinlich noch im Rechenzentrum vorhanden sind, passiert und wie diese Daten vor unberechtigtem Zugriff geschützt werden können.

- **Beschlagnahmung von Hardware:** Eine Beschlagnahmung von Hardware kann in allen Ländern erfolgen in denen der Anbieter Cloud-Ressourcen betreibt. Die Beschlagnahmung kann aus diversen Gründen erfolgen, für die der Dienstnutzer keine Verantwortung trägt. Sehr wohl können sich aber Daten des Cloud-Nutzers oder Metadaten über die Cloud-Nutzung (z. B. Logs) auf den beschlagnahmten Servern befinden. Diese Daten können unerwünschte Schlussfolgerungen über die Geschäftstätigkeit des Cloud-Nutzers ermöglichen (s. o.).

Ansätze zur Wahrung der Datenintegrität

Zwar ist die Gewährleistung von Vertraulichkeit für die Daten genug, um die sensiblen Daten vor unberechtigtem Mitlesen zu schützen. Ein weiterer wichtiger Aspekt, insbesondere für eine DaaS, ist jedoch, sicherzustellen, dass die Daten nicht verändert oder manipuliert wurden. Während für die Wahrung der Vertraulichkeit eine Verschlüsselung ausreicht, erfordert die Wahrung

der Datenintegrität kryptographische Hash-Funktionen, z. B. in Form eines Message Authentication Code (MAC). Die richtige Anwendung dieser MACs ist jedoch nicht trivial und sollte daher mit dem Cloud-Anbieter abgeklärt werden. Zumindest erfährt das Kundenunternehmen auf diese Weise, wie gut sich der Anbieter mit diesen sicherheitsrelevanten Fragestellungen bereits auseinander gesetzt hat. Im besten Fall hat der Anbieter bereits eine Lösung im Angebot, was jedoch – ähnlich wie bei der Verschlüsselung – derzeit nicht die Regel ist.

Eine weitere Frage, die sich in diesem Zusammenhang stellt, ist die Überprüfbarkeit der Datenintegrität bei großen Datenbanken. Wenn die DaaS-Lösung intensiv genutzt wird, will der Kunde natürlich nicht immer die gesamte Datenbank herunterladen, bloß um die Integrität der Daten zu prüfen. Zum einen erzeugt dies unnötige Kosten, zum anderen dauert es lange. Daher muss geklärt werden, wie eine Integritätsprüfung „in der Cloud“ durchgeführt werden kann. Hier gibt es ebenfalls Ansätze in der Wissenschaft unter dem Stichwort „Proof of Retrievability“ [30, 2, 37], die jedoch nach unserem Kenntnisstand von keinem Cloud-Anbieter angeboten werden. Daher bleibt in der Praxis nur die Möglichkeit, dem Anbieter in dieser Hinsicht zu vertrauen und gegebenenfalls anhand von Prüfsummen die Integrität der Daten zumindest plausibel zu machen.

5.5 Zusammenfassung

Wie in diesem Kapitel dargelegt, bringt das Cloud-Computing keine grundlegend neuen Sicherheitsprobleme, sondern verändert lediglich den Schwerpunkt bzw. verschärft einige bekannte Aspekte. Durch sorgfältige Planung und Analyse können die sicherheitsrelevanten Bereiche identifiziert und kontrolliert werden. In Verbindung mit der Lektüre der ausführlichen Erläuterungen, stellen die zehn Leitfragen auf der folgenden Seite ein Werkzeug zur ersten Einschätzung der Sicherheit einer konkreten Cloud-Lösung dar. Selbstverständlich sollte vor dem tatsächlichen Schritt „in die Cloud“ eine sehr viel gründlichere Analyse durchgeführt werden, die auf den vorgestellten Verfahren und Standards beruht. Das BSI stellt mit [4] einen etwas detaillierteren Leitfaden hierzu bereit. Das Vorgehen nach IT-Grundschutz bietet eine noch feinere Granularitätsstufe [23].

Zehn Leitfragen zur Sicherheit der Cloud-Lösung

1. Wird die Sicherheit der Cloud-Computing-Lösung in einem *ganzheitlichen* Sicherheitskonzept beurteilt, werden bestehende Sicherheitskonzepte angemessen berücksichtigt und die neue Cloud-Computing-Lösung in diese eingearbeitet?
2. Hat der Provider eine ausführliche Analyse der Sicherheitsaspekte des Cloud-Dienstes durchgeführt, bei der mögliche Angriffsvektoren und Schwachstellen analysiert und bewertet sowie durch angemessene Technologien und Prozesse adressiert wurden?
3. Durch welche Zertifikate, Testate oder externe Überprüfungen kann der Cloud-Anbieter den sicheren Betrieb seiner Services glaubhaft machen und wie kann das Anwenderunternehmen dies überprüfen?
4. Wie wird die korrekte Funktion aller Sicherheitsmechanismen gewährleistet und wie wird im Fehlerfall vorgegangen?
5. Sind auch die sicherheitsrelevanten Aspekte der Servicenutzung durch ein SLA abgedeckt?
6. Wurde die gesamte Wertschöpfungskette inklusive der Dienstleister des Cloud-Anbieters analysiert?
7. Wie werden die Kommunikationskanäle (Netzinfrastruktur) zur Cloud im Sicherheitskonzept berücksichtigt und geschützt?
8. Bieten alle Rechenzentren, in denen der Provider die Daten des Unternehmens verarbeitet, dasselbe Sicherheitsniveau, auch z. B. im Hinblick auf die politische Lage und rechtliche Situation im jeweiligen Land?
9. Ist klar definiert, wer bestimmte sensible Daten einsehen darf, und welche Kontrollmechanismen bzw. technischen Maßnahmen kann der Anbieter vorweisen, um zu garantieren, dass diese Daten vor dem Zugriff durch unberechtigte Dritte geschützt sind, solange sie in seinem Wirkungsbereich gespeichert sind?
10. Wie erkennt der Cloud-Anbieter, dass ein Dienst angegriffen wird, und auf welche Art und Weise werden die Mitarbeiter des Cloud-Nutzers darüber informiert?

6 Zusammenfassung

Im Rahmen dieses Leitfadens wurde ein erster Eindruck von den Einsatzmöglichkeiten von Cloud-Computing gegeben. Es wurden vor allem auch die zu erwartenden Maßnahmen beschrieben, die mit der Einführung von Cloud-Computing im Unternehmen einhergehen. Festzuhalten bleibt, dass Cloud-Computing keine technische Revolution, aber eine neuartige Kombination aus vielen bekannten und einigen neuen Ansätzen ist. Die Definition des Begriffs hat sich einigermaßen stabilisiert und man unterscheidet drei verschiedene Servicemodelle: Infrastructure-as-a-Service, Platform-as-a-Service sowie Software-as-a-Service. Database-as-a-Service (DaaS), der Fokus dieses Leitfadens, bezeichnet eine Klasse von Cloud-Diensten, die Funktionalitäten eines DBS in der Cloud bereitstellen. DaaS kann dabei basierend auf einem der drei Servicemodelle angeboten werden. Die meisten Aspekte aus diesem Leitfaden lassen sich direkt auf andere Arten von Diensten übertragen und sind nicht spezifisch für DaaS. Es gibt zudem vier verschiedene Arten des Cloud-Betriebs: die öffentliche und die nichtöffentliche Cloud sowie die Community-Cloud und die hybride Cloud. Trotz der vielen neuen Begriffe ist Cloud-Computing nicht allzu verschieden vom klassischen IT-Outsourcing. Allerdings verschiebt sich die Gewichtung der zu beachtenden Aspekte.

Keine Revolution

Wirtschaftlich kann Cloud-Computing je nach Anwendungsfall sehr attraktiv sein – muss es aber auch nicht. Insbesondere für Cloud-Dienste, die von der „Stangenware“ abweichen, fordern die Anbieter hohe Gebühren, so dass die Vorteile schnell schwinden. Technisch bringt Cloud-Computing für den Anwender nur wenig wirklich neue Herausforderungen, fordert aber oft eine Anpassung bestehender Systeme. Organisatorisch erfordert es stringente Abläufe, die gegebenenfalls im Unternehmen erst noch einzuführen sind. Das Hauptproblem ist jedoch die rechtliche Unsicherheit, die der Tatsache geschuldet ist, dass die meisten Aspekte des Cloud-Computing juristisch noch ungeklärt sind. In jedem Fall muss auf Managementebene eine Cloud-Strategie entwickelt werden. Sie ist eine essentielle Voraussetzung für jedes Cloud-Projekt.

Rechtliche Unsicherheit

Bei der Auswahl des Anbieters müssen alle vier Dimensionen des Cloud-Computing betrachtet werden. Besondere Aufmerksamkeit sollte den erwarteten Lock-in-Effekten, der Integration in bestehende Systeme und der Erfüllung rechtlicher Rahmenbedingungen gewidmet werden. Auch die Support-Leistungen und die Kommunikation mit dem Anbieter sind wichtige Aspekte. Auf jeden Fall ist ein strukturiertes Vorgehen zur Anbieterauswahl inklusive Dokumentation gefordert.

Die Sicherheit in der Cloud ist für alle Unternehmen ein zentrales Thema und muss explizit in der Cloud-Strategie behandelt werden. Einige einfache Maßnahmen, sozusagen das „Kleine Einmaleins der Cloud-Sicherheit“, verhelfen bereits zu einer soliden Grundlage. Selbstverständlich müssen die eigenen Anforderungen an die Sicherheit im Vorfeld genau geklärt werden. Aus technischer Sicht müssen sowohl die Infrastruktur als auch die Daten geschützt werden. Ansät-

Sicherheit in der Cloud

ze für ersteres sind bekannt, der Aspekt der Datensicherheit stellt größere Hürden in den Weg, da viele Anbieter nur ein durchschnittliches, aber kein hohes Schutzniveau erbringen. Trotz ungeklärter technischer Fragestellungen überwiegen die organisatorischen Probleme. Unter anderem müssen die Mitarbeiter sensibilisiert und geschult werden sowie bestehende und neue Sicherheitskonzepte integriert werden. Insgesamt ist die Sicherheit von Cloud-Diensten nicht notwendigerweise schlechter als von Lösungen im eigenen Haus.

Beim Cloud-Computing verhält es sich folglich nicht anders als bei anderen Fragestellungen der IT: der Einsatz kann sehr sinnvoll sein, aber dies ist abhängig vom konkreten Szenario. Auch ein sicherer und zuverlässiger Betrieb ist möglich. Je höher allerdings die Anforderungen an den Dienstleister werden, desto unattraktiver wird eine Cloud-Lösung. Als Faustregel lässt sich daher festhalten, dass Cloud-Computing vor allem für standardisierte Produkte attraktiv ist. Trotzdem sollte sich jedes Unternehmen mit dem Thema auseinander setzen und eine individuelle Cloud-Strategie erarbeiten – selbst wenn das Ergebnis die Festlegung ist, dass Cloud-Computing vermieden wird.

Literaturverzeichnis

[1] Armbrust, Michael ; Fox, Armando ; Griffith, Rean ; Joseph, Anthony D. ; Katz, Randy H. ; Konwinski, Andrew ; Lee, Gunho ; Patterson, David A. ; Rabkin, Ariel ; Stoica, Ion ; Zaharia, Matei: Above the Clouds: A Berkeley View of Cloud Computing / EECS Department, University of California, Berkeley. 2009 (UCB/EECS-2009-28). – Forschungsbericht

[2] Bowers, Kevin D. ; Juels, Ari ; Oprea, Alina: Proofs of retrievability: theory and implementation. In: *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*. New York, NY, USA : ACM, 2009. – ISBN 978–1–60558–784–4, S. 43–54

[3] Brunette, Glenn ; Mogull, Rich: Security Guidance for Critical Areas of Focus in Cloud Computing / Cloud Security Alliance. Version: December 2009. http://www.cloudsecurityalliance.org/csaguide.pdf. 2009. – White Paper

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter*. Entwurf zur Diskussion. http://tinyurl.com/35kfeua. Version: September 2010

[5] Connolly, Chris: The US Safe Harbor – Fact or Fiction? / Galexia Pty Ltd. 2008. – Research Article

[6] Denning, Dorothy E.: *Cryptography and data security*. Addison-Wesley, 1982 (ACM Classic Books Series)

[7] Discini, Sonny ; Needle, David ; McGarvey, Robert ; Maguire, James: Understanding the Security Challenges of Cloud Computing / internet.com. 2010. – White Paper

[8] Eckert, Claudia: *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. 6. Auflage. München : Oldenbourg, 2009

[9] Erl, Thomas: *Service-Oriented Architecture – Concepts, Technology and Design*. Prentice Hall PTR, 2005 (Prentice Hall Service Oriented Computing Series)

[10] Garfinkel, Simson L.: An Evaluation of Amazon's Grid Computing Services: EC2, S3 and SQS / Center for Research on Computation and Society, Harvard University, Cambridge, MA. 2007 (TR-08-07). – Technical Report

[11] Gentry, Craig: *A fully homomorphic encryption scheme*, Stanford University, Diss., 2009. http://crypto.stanford.edu/craig

[12] Gilbert, Seth ; Lynch, Nancy: Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. In: *ACM SIGACT News*, 2002

[13] Grossman, Robert L.: The Case for Cloud Computing. In: *IT Professional* 11 (2009), Nr. 2, S. 23–27. http://dx.doi.org/10.1109/MITP.2009.40. – DOI 10.1109/MITP.2009.40. – ISSN 1520–9202

[14] Haselmann, Till ; Thies, Gunnar ; Vossen, Gottfried: Looking into a REST-based API for Database-as-a-Service Systems. In: *Proc. 12th IEEE Conference on Commerce and Enterprise Computing (CEC 2010)* (to appear) (2010)

[15] Kephart, Jeffrey O. ; Chess, David M.: The Vision of Autonomic Computing. In: *IEEE Computer* 36 (2003), Nr. 1, S. 41–50

[16] Kittlaus, Hans-Bernd ; Schreiber, Dirk: SaaS – wie können KMU profitieren? In: *Wirtschafsinformatik & Management* (2010), Nr. 02, S. 36–42

[17] Lansing, Jens: *Aktueller Stand und zukünftige Entwicklungsmöglichkeiten von Database-as-a-Service-Angeboten*, Lehrstuhl für Informatik, Institut für Wirtschaftsinformatik, Westfälische Wilhelms-Universität Münster, Diplomarbeit, Dezember 2008

[18] Leong, Lydia: How to Select a Cloud Computing Infrastructure Provider / Gartner Group. 2009 (G00166565). – White Paper

[19] Mather, Tim ; Kumaraswamy, Subra ; Latif, Shahed: *Cloud Security and Privacy*. O'Reilly Media, 2009. – ISBN 9780596802769

[20] National Institute of Standards and Technology (NIST): *NIST Cloud Computing Project*. http://csrc.nist.gov/groups/SNS/cloud-computing/. Version: May 2010, Abruf: 2010-08-09. – online

[21] Neuman, B. C.: Scale in Distributed Systems. In: *Readings in Distributed Computing Systems*, IEEE Computer Society Press, 1994, S. 463–489

[22] o. V.: *BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)*. Version 1.5. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008 (IT-Grundschutz)

[23] o. V.: *BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise*. Version 2.0. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008 (IT-Grundschutz)

[24] o. V.: *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz*. Version 2.5. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008 (IT-Grundschutz)

[25] o. V.: *BSI-Standard 100-4: Notfallmanagement*. Version 1.0. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008 (IT-Grundschutz)

[26] o. V.: How VMware Virtualization Right-sizes IT Infrastructure to Reduce Power Consumption / VMware, Inc. Version: 2008. http://www.vmware.com/files/pdf/WhitePaper_ReducePowerConsumption.pdf. 2008. – White Paper

[27] o. V.: *IT-Grundschutz-Kataloge*. 11. EL. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009

[28] o. V.: Cloud Computing Use Case White Paper V4 / Cloud Computing Use Cases Group. Version: Juli 2010. http://cloudusecases.org/. 2010. – White Paper

[29] Pritchett, Dan: BASE: An Acid Alternative. In: *ACM Queue* 6 (2008), Nr. 3, 48–55. http://dx.doi.org/10.1145/1394127.1394128. – DOI 10.1145/1394127.1394128. – ISSN 1542–7730

[30] Shacham, Hovav ; Waters, Brent: Compact Proofs of Retrievability. Version: 2008. http://dx.doi.org/10.1007/978-3-540-89255-7_7. In: Pieprzyk, Josef (Hrsg.): *Advances in Cryptology - ASIACRYPT 2008* Bd. 5350. Springer Berlin/Heidelberg, 2008. – DOI 10.1007/978–3–540–89255–7_7, S. 90–107

[31] Stonebraker, Michael ; Madden, Samuel ; Abadi, Daniel J. ; Harizopoulos, Stavros ; Hachem, Nabil ; Helland, Pat: The End of an Architectural Era (It's Time for a Complete Rewrite). In: Koch, Christoph (Hrsg.) ; Gehrke, Johannes (Hrsg.) ; Garofalakis, Minos N. (Hrsg.) ; Srivastava, Divesh (Hrsg.) ; Aberer, Karl (Hrsg.) ; Deshpande, Anand (Hrsg.) ; Florescu, Daniela (Hrsg.) ; Chan, Chee Y. (Hrsg.) ; Ganti, Venkatesh (Hrsg.) ; Kanne, Carl-Christian (Hrsg.) ; Klas, Wolfgang (Hrsg.) ; Neuhold, Erich J. (Hrsg.): *VLDB*, ACM, September 2007. – ISBN 978–1–59593–649–3, S. 1150–1160

[32] Streitberger, Werner ; Ruppel, Angelika: *Cloud Computing Sicherheit - Schutzziele. Taxonomie. Marktübersicht*. Parkring 4, Garching b. München : Fraunhofer-Institut für sichere Informationstechnologie, September 2009

[33] Störtkuhl, Thomas ; Wagner, Hans: Cloud Computing und die IT-Security. In: *IT-Grundschutz* (2010), Februar, Nr. 2, S. 7–9

[34] Vaquero, Luis M. ; Rodero-Merino, Luis ; Caceres, Juan ; Lindner, Maik: A Break in the Clouds: Towards a Cloud Definition. In: *Computer Communication Review* 39 (2009), Nr. 1, S. 50–55

[35] Velten, Carlo ; Janata, Steve: Cloud Vendor Benchmark – Cloud Computing Anbieter im Vergleich / Experton Group. 2010. – White Paper

[36] Vossen, Gottfried: *Datenmodelle, Datenbanksprachen und Datenbankmanagement-Systeme*. 5. überarbeitete und erweiterte Auflage. München, Wien : R. Oldenbourg Verlag, 2008

[37] Wang, Cong ; Wang, Qian ; Ren, Kui ; Lou, Wenjing: Ensuring data storage security in Cloud Computing. In: *Proc. 17th International Workshop on Quality of Service (IWQoS)*. Charleston, SC, July 2009, S. 1–9

[38] Weinman, Joe: *Mathematical Proof of the Inevitability of Cloud Computing*. http://cloudonomics.wordpress.com/2009/11/30/mathematical-proof-of-the-inevitability-of-cloud-computing/. Version: November 2009, Abruf: 2010-08-09. – online

[39] Wikipedia (DE): *Virtualisierung (Informatik)*. http://de.wikipedia.org/w/index.php?title=Virtualisierung_(Informatik)&oldid=79167522. Version: September 2010, Abruf: 2010-09-30. – online

[40] Wikipedia (EN): *Utility Computing*. http://en.wikipedia.org/w/index.php?title=Utility_computing&oldid=387678616. Version: September 2010, Abruf: 2010-09-30. – online

Förderkreis der Angewandten Informatik
an der Westfälischen Wilhelms-Universität Münster e.V.

Einsteinstraße 62
D-48149 Münster
Tel.: +49 251 83 33797
Fax : +49 251 83 33755

ISSN 1868-0801