



Bundesministerium  
für Wirtschaft  
und Technologie

WIRTSCHAFT.  
WACHSTUM.  
WOHLSTAND.

Nationaler **IT** Gipfel  
Essen 2012

# Chancen für den Mittelstand durch Cloud Computing – ein Wegweiser

AG2 Fachinitiative Cloud Computing

## Impressum

### Herausgeber

Bundesministerium für Wirtschaft  
und Technologie (BMWi)  
Öffentlichkeitsarbeit  
11019 Berlin  
www.bmwi.de

### Redaktion

Fachinitiative „Cloud Computing“  
der AG2 „Digitale Infrastrukturen  
für innovative Anwendungen“

### Stand

November 2012

### Gestaltung und Produktion

PRpetuum GmbH, München

### Bildnachweis

tashka2000 – Fotolia.com (Titel)

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des Bundesministeriums für Wirtschaft und Technologie. Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Nicht zulässig ist die Verteilung auf Wahlveranstaltungen und an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben von Informationen oder Werbemitteln.



Das Bundesministerium für Wirtschaft und Technologie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

# Inhalt

1. Einleitung .....	2
2. Was sind Cloud-Computing-Lösungen überhaupt? .....	3
3. Chancen durch Cloud Computing .....	4
3.1 Potenziale für kleine und mittelständische Unternehmen .....	4
3.2 Gesellschaftliche Vorteile .....	4
4. Die wesentlichen Anforderungen an die Cloud-Nutzung .....	5
4.1 Rechtskonformität der Geschäftstätigkeit .....	5
4.2 Datenschutz .....	5
4.3 Informationssicherheit .....	6
4.4 Portabilität .....	7
4.5 Interoperabilität .....	8
5. Zertifizierung und Standardisierung .....	9
5.1 Zertifizierung .....	9
5.2 Standardisierung .....	9
6. Orientierungshilfe zur Auswahl eines Cloud-Anbieters – wesentliche Leitfragen .....	11
6.1 Rechtskonformität .....	11
6.2 Datenschutz .....	11
6.3 Informationssicherheit .....	11
6.4 Portabilität .....	11
6.5 Interoperabilität .....	11
Anhang .....	12

# 1. Einleitung

Heute nutzt bereits ein Viertel aller Unternehmen in Westeuropa – Tendenz steigend – Cloud-Dienste<sup>1</sup>. Damit ist Europa nach den USA der Markt mit der höchsten Marktdurchdringung von Cloud-Services<sup>2</sup>. Setzen noch vor wenigen Jahren fast ausschließlich Großunternehmen aus der produzierenden Industrie und der Dienstleistungsbranche entsprechende Cloud-Lösungen ein, sind es heute immer mehr klein- und mittelständische Unternehmen, die den hohen Nutzen von Cloud-basierten Lösungen erkennen.

Für Unternehmen, die in der Cloud bereitgestellte IT-Services nutzen, anstatt diese selbst aufzubauen und zu betreiben, entstehen viele Vorteile:

- Die Startinvestitionen für den Kauf von Hardware (Server, Speicher etc.) und Software-Lizenzen entfallen (nahezu) komplett, ebenso wie die Kosten für den Aufbau und die Durchführung des eigenen Betriebs der IT-Services. Stattdessen ist in der Regel nur ein „verbrauchsabhängiges“ Nutzungsentgelt zu zahlen (z. B. nach Anzahl der User, die einen IT-Service aus der Cloud nutzen).
- Es entfallen Kosten für Erweiterungen von Hardware, Lizenzen und Personal im selbstorganisierten Betrieb. Nur wenn der Nutzungsbedarf steigt, steigen auch die operativen Kosten für die aus der Cloud bezogenen IT-Services.
- Investitionsmittel werden durch den Einsatz von IT-Services aus der Cloud freigesetzt und der Managementaufwand wird reduziert. Unternehmen können sich dadurch besser auf ihr Kerngeschäft konzentrieren.
- Der Zugriff auf IT-Services in der Cloud erfolgt über das Internet. Die Services sind über unterschiedliche Plattformen und über mobile Endgeräte verfügbar und sind von überall her abruf- und nutzbar.

- Wichtige Synergiepotenziale, insbesondere mit Blick auf notwendige Investitionen in Sicherheitsinfrastrukturen der Rechenzentren, können über Unternehmensgrenzen hinweg genutzt werden, ohne die Integrität der eigenen Daten zu gefährden.

Um die beschriebenen Potenziale von Cloud-Services voll ausschöpfen zu können, bedarf es des Vertrauens und der Akzeptanz hinsichtlich der Technologie. Dies gilt insbesondere für kleine und mittelständische Unternehmen. Die Fachinitiative Cloud Computing der Arbeitsgruppe 2 des Nationalen IT-Gipfels hat deshalb den vorliegenden Wegweiser „Chancen für den Mittelstand durch Cloud Computing“ entwickelt.

Die wesentlichen Anforderungen an Cloud Computing, wie Rechtskonformität, Datenschutz, Informationssicherheit, Portabilität und Interoperabilität, werden analysiert. In Kapitel fünf wird kurz auf die Rolle von Zertifizierung und Standardisierung im Cloud Computing eingegangen. Der Wegweiser endet mit einigen wichtigen Leitfragen, bezogen auf die fünf in Kapitel 4 genannten Anforderungen. Die Leitfragen sind keineswegs erschöpfend und sollen als Orientierung und Impulsgeber beim Einstieg in die Cloud dienen.

1 [http://www.bitkom.org/de/presse/8477\\_71446.aspx](http://www.bitkom.org/de/presse/8477_71446.aspx) (letzter Zugriff: 04.09.2012)

2 <http://www.gartner.com/it/page.jsp?id=1389313> (letzter Zugriff: 04.09.2012)

## 2. Was sind Cloud-Computing-Lösungen überhaupt?

Eine Cloud-Computing-Lösung wird nachfolgend als die Menge derjenigen IT-Services definiert, die ein Cloud-Anbieter einem Cloud-Anwender zur Nutzung zur Verfügung stellt. Als Cloud-Anwender werden nachfolgend ausschließlich Unternehmen und Organisationen betrachtet.

Cloud Computing ist eine Form der Bereitstellung von gemeinsam nutzbaren und flexibel skalierbaren IT-Leistungen durch nicht fest zugeordnete IT-Ressourcen über Netze. Typische Beispiele dafür sind die Bereitstellung von E-Mail-Diensten durch einen Internet-Service-Provider, bei einem Anbieter ausgeführte Software, z. B. für die Buchhaltung, oder Browserbasierte Anwendungen zum Kundenmanagement, bei denen über sichere Internetverbindungen auf Dienste eines Cloud-Providers zugegriffen wird.

Idealtypische Merkmale sind die Bereitstellung in Echtzeit als Self Service auf Basis von Internet-Technologien und die Abrechnung nach Nutzung. Damit ermöglicht Cloud Computing den Nutzern eine Umverteilung von Investitionskosten hin zu Betriebsaufwand. Die IT-Leistungen können sich auf Anwendungen, Plattformen für Anwendungsentwicklungen und Betrieb bzw. auf komplette Basisinfrastrukturen beziehen.<sup>3</sup>

## 3. Chancen durch Cloud Computing

### 3.1 Potenziale für kleine und mittelständische Unternehmen

Die Möglichkeit, Speicherkapazitäten, Software oder Rechenleistungen über das Internet zu beziehen, bietet Unternehmen jeglicher Größe die Chance, ihre IT-Kapazitäten zu flexibilisieren und benötigte Dienste je nach Umfang, Dauer der Nutzung sowie Anzahl der Nutzer zu bezahlen.

Durch diese anpassbare Struktur ist Cloud Computing für kleine und mittelständische Unternehmen eine interessante Alternative zum Kauf von Informationstechnologien, sei es in Form von On-Demand Software, sogenannter Software-as-a-Service (SaaS) oder als Infrastructure-as-a-Service (IaaS) in Form von Rechnerkapazitäten auf externen Servern oder als On-Demand Plattform, sogenannter Platform-as-a-Service (PaaS).

Cloud-Lösungen können entweder „öffentlich“ aus dem Internet bereitgestellt werden (Public Cloud) oder abgeschottet und dediziert innerhalb der eigenen IT-Infrastruktur betrieben werden (Private Cloud). Die Kombination beider Angebote wird als hybride Cloud bezeichnet. Im weiteren Verlauf beziehen sich die Ausführungen ausschließlich auf Public-Cloud-Services.

Klassische Anwendungssoftware setzt üblicherweise eine umfassende vom Anwender betriebene IT-Infrastruktur voraus. Dazu mussten in der Vergangenheit eigene Server in Betrieb genommen werden, was mit hohen Anschaffungs- und Betriebskosten einherging. Beim Cloud Computing werden Server genutzt, die vom Dienste-Anbieter bereitgestellt werden. Die Investitionskosten für das Bereitstellen der eigenen IT-Infrastruktur im Unternehmen entfallen. Cloud-Anwender haben dadurch deutlich geringere Support- und Pflegekosten.

In der Regel gehört die Organisation eines Rechenzentrums nicht zu den Kernkompetenzen von kleinen und mittelständischen Unternehmen. Daher ist es sinnvoll, diesen Bereich an einen sorgfältig ausgewählten Cloud-Anbieter zu vergeben und die unternehmensinternen Ressourcen auf die Kernkompetenzen des eigenen Unternehmens zu konzentrieren. Cloud-Dienste können individuell an die Erfordernisse eines Unterneh-

mens angepasst und bei Bedarf sehr schnell verringert oder erweitert werden. Das vereinfacht die IT deutlich und schafft mehr Raum für das Kerngeschäft.

### 3.2 Gesellschaftliche Vorteile

Cloud-Services sind ein Schlüssel zur Lösung vieler gesellschaftspolitischer Herausforderungen, von der demografischen Entwicklung über Bildung, Energiewende, Gesundheitswesen bis hin zu einer offenen, effizienten Verwaltung.

Beispiel Bildung: Schulen benötigen verlässliche IT-Infrastrukturen, die ihren speziellen Anforderungen gerecht werden. Sie verfügen häufig weder über ausreichende Mittel noch über die notwendigen Kenntnisse, um einen IT-Betrieb eigenständig zu realisieren.

Vor diesem Hintergrund wird beispielsweise über eine schulübergreifende intelligente Vernetzung mit digitalen Bildungsangeboten auf Basis von Cloud Computing diskutiert, bei der auch die an den Schulen befindlichen Infrastrukturbestandteile zentral verwaltet werden können.

Grundlage eines solchen Konzepts ist eine gemeinsam von allen Schulen nutzbare, sichere und hochverfügbare IT-Infrastruktur. Diese könnte den Schulen zentrale Dienste, wie zum Beispiel Identitätsmanagement, Lern- und Kommunikationsplattformen, Mediatheken oder Software, zur Verfügung stellen. Vorhandene Strukturen können dabei in einer einheitlichen IT-Plattform integriert werden, ohne die von den Schulen benötigte Eigenständigkeit zu reduzieren.

Auch auf die Herausforderungen bei der Energiewende (z. B. Smart Grid) oder auf intelligente Gesundheits- oder Verwaltungsnetze ließe sich ein Cloud-Ansatz übertragen.

## 4. Die wesentlichen Anforderungen an die Cloud-Nutzung

Rund 60 Prozent der Entscheidungsträger kleiner und mittelständischer Unternehmen wissen, was Cloud Computing ist, aber nur 12 Prozent planen den Einsatz oder haben Cloud Computing bereits eingeführt.<sup>4</sup>

Neben den Vorteilen der Cloud besteht offensichtlich auch Verunsicherung über den Einsatz dieser Technologie. Aspekte wie der Speicherort der eigenen Daten, eine mögliche Anbieterabhängigkeit oder Fragen der IT-Sicherheit tragen dazu bei.

Für eine sichere und verlässliche Nutzung von Cloud-Diensten sind unter anderem zu beachten<sup>5</sup>:

- Rechtskonformität der Geschäftstätigkeit bei einer Cloud-Nutzung,
- Schutz von Cloud-Daten,
- Informationssicherheit von Cloud-Daten und Prozessen,
- Portabilität einer Cloud-Computing-Lösung und
- Interoperabilität einer Cloud-Computing-Lösung.

Nachfolgend werden diese fünf Anforderungen dargestellt.

### 4.1 Rechtskonformität der Geschäftstätigkeit

Rechtskonformität umschreibt ein regelkonformes Verhalten eines Unternehmens in Bezug auf die gesetzlichen und regulativen Bestimmungen. Viele Unternehmen gehen über das gesetzliche Maß hinaus und folgen zudem selbstaufgelegten Compliance-Regeln und -Prozessen.

Ein Cloud-Anwender nutzt eine Cloud-Computing-Lösung (im Rahmen seines unternehmerischen Handelns) rechtskonform („compliant“), wenn er bei der Nutzung der Cloud-Computing-Lösung alle hierfür

anwendbaren Gesetze (Regelungen) sowie alle für sein Unternehmen (unabhängig von der Cloud-Nutzung) anwendbaren Gesetze (Regelungen) einhält. Um dies sicherzustellen, sind die genaue Kenntnis der entsprechenden Regeln und eine intensive Prüfung der potenziellen Cloud-Anbieter notwendig. Der Anwender ist in der Cloud-Nutzung für die Rechtskonformität verantwortlich, wie er dies heute schon für die Nutzung der IT im eigenen Unternehmen ist.

### 4.2 Datenschutz

Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind die Datenschutzbestimmungen der EU und des Bundes zu beachten. Personenbezogen sind Daten dann, wenn sie sich auf eine bestimmte oder eine bestimmbar natürliche Person beziehen.

Der Cloud-Anwender ist für die Einhaltung datenschutzrechtlicher Bestimmungen verantwortlich. Er muss den Cloud-Anbieter sorgfältig auswählen und regelmäßig im Rahmen seiner Möglichkeiten kontrollieren. Auch muss er sich über die möglichen Verarbeitungsorte seiner Daten im Vorfeld informieren. Liegen diese außerhalb des europäischen Wirtschaftsraumes, muss sich der Cloud-Anwender an die Regelungen des sog. „Drittstaatentransfers“ nach dem Bundesdatenschutzgesetz (BDSG) halten. Zum Beispiel ist dann darauf zu achten, dass im Drittland ein der EU ähnlicher Datenschutzstandard vorherrscht. Die Drittstaatenregelungen greifen nicht, wenn sich der Cloud-Anbieter etwa zur Einhaltung der sogenannten Safe-Harbor-Grundsätze, einer Art freiwilligen Selbstzertifizierung, und der Zusammenarbeit mit den EU-Datenschutzbehörden verpflichtet hat.

Hilfestellungen bei der Einhaltung seiner datenschutzrechtlichen Verpflichtungen kann dem Cloud-Anwender zum Beispiel ein Zertifizierer bieten. Auch über die Verschlüsselung der Daten sollte der Anwender nachdenken. Wenn der Schlüssel beim Anwender verbleibt, verlieren die Daten durch die Verschlüsselung ihren Personenbezug.

<sup>4</sup> [http://www.pwc.de/de\\_DE/de/mittelstand/assets/Cloud\\_Computing\\_Mittelstand.pdf](http://www.pwc.de/de_DE/de/mittelstand/assets/Cloud_Computing_Mittelstand.pdf) (letzter Zugriff: 04.09.2012)

<sup>5</sup> Technologische und wirtschaftliche Aspekte wurden in der Publikation der PG Cloud Computing zum IT-Gipfel 2011 in Kapitel 5 mit Fokus auf Infrastructure-as-a-Service diskutiert: <http://www.it-gipfel.de/IT-Gipfel/Redaktion/PDF/anbieterwechsel-ag-2.property=pdf.bereich=itgipfel.sprache=de.rwb=true.pdf> (letzter Zugriff: 04.09.2012)

Der Cloud-Anwender sollte sich grundsätzlich bei seinem Cloud-Anbieter informieren, ob und welche staatlichen Stellen Zugriff auf die dem Cloud-Anbieter zur Verarbeitung anvertrauten Daten haben. Besonders nach dem 11. September 2001 haben viele Länder Anti-terror-Gesetze eingeführt oder novelliert, wie z. B. Kanada, Australien, England, Frankreich, Deutschland und Russland. Sicherheitsbehörden aus sehr vielen Ländern können Cloud-Anbieter zur Auskunft über ihnen anvertraute Daten zum Zwecke der Terrorismusabwehr auffordern. Art und Weise können sich unterscheiden. In der Konsequenz betrifft der Zugriff auf Daten durch staatliche Stellen im begründeten Verdachtsfall alle Unternehmen, unabhängig von einem in- oder ausländischen Firmensitz.<sup>6</sup>

### 4.3 Informationssicherheit

Informationssicherheit beinhaltet im Gegensatz zum Datenschutz auch die Gewährleistung der Authentizität von Informationen. Sie umfasst alle technischen und organisatorischen Maßnahmen zum Schutz von Daten und Prozessen vor Verfälschung, Zerstörung oder unzulässiger Weitergabe. Gegenstand sind sowohl










Unternehmensdaten als auch Prozesse und Prozeduren der Datenverarbeitung, also auch Informationen als Ergebnis der verarbeiteten Daten.

Informationssicherheit bei der Nutzung einer Cloud-Lösung bezieht sich auf diejenigen Daten, die der Cloud-Anwender im Rahmen der Nutzung an den Cloud-Anbieter übergibt, und diejenigen Daten, die während der Nutzung der Cloud-Lösung entstehen (im folgenden Cloud-Daten genannt).

Die Informationssicherheit dieser, dem Cloud-Anbieter anvertrauten Daten und Prozesse ist gegeben, wenn deren Verfügbarkeit, Unversehrtheit und Schutz vor unbefugtem Zugriff sichergestellt sind. Zu den aktiven Vorkehrungen des Anwenders für den Schutz seiner Informationen zählen die Datenverschlüsselung und die verschlüsselte Datenübertragung.

Die Verantwortung für die Informationssicherheit liegt beim Cloud-Anwender. Beim Cloud-Anwender verbleibt die organisatorische Verantwortung (Kontrollpflicht). Beim Cloud-Anbieter verbleibt die betriebliche Verantwortung (je nach Vertragsgestaltung z. B. für Backups) für die Informationssicherheit.

Abb. 1: Verschiedene Möglichkeiten der Cloud-Nutzung

Einsatzmodell	Dienstmodell	Betriebsmodell
 Private	 Applications (SaaS)	 Customer Owns Customer Operates
 Public	 Platform (PaaS)	 Customer Owns Provider Operates
 Hybrid	 Infrastructure (IaaS)	 Provider Owns Provider Operates

Quelle: Oracle, 2012

<sup>6</sup> Häufig wird im Zusammenhang mit Cloud Computing nur über den Patriot Act diskutiert. Grundsätzlich gilt, dass Unternehmen und Organisationen stets den geltenden Regelungen und Gesetzen in den Ländern, in denen sich der Hauptsitz befindet und in denen sie tätig sind, unterliegen. Siehe auch: [http://www.hoganlovells.com/files/News/c6edc1e2-d57b-402e-9cab-a7be4e004c59/Presentation/NewsAttachment/a17af284-7d04-4008-b557-5888433b292d/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20\(18%20July%202012\).pdf](http://www.hoganlovells.com/files/News/c6edc1e2-d57b-402e-9cab-a7be4e004c59/Presentation/NewsAttachment/a17af284-7d04-4008-b557-5888433b292d/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%202012).pdf), S. 13 (letzter Zugriff: 04.09.2012)



Die Internationale Standardisierungsnorm ISO 27001 bietet Kriterien für die IT-Sicherheit. Wer Cloud-Dienste nutzt, sollte auch über die Zertifizierung hinaus ein Verständnis dafür entwickeln, welche Sicherheitsmaßnahmen in der Cloud umgesetzt sind, und dies aktiv beim Cloud-Anbieter hinterfragen. Dies betrifft insbesondere Aspekte wie

- Virtualisierungssicherheit,
- Mandantenfähigkeit und -trennung,
- Systemisolation und Netzwerktrennung,
- Lebenszyklus von Daten in der Cloud und
- Prozesse zwischen Cloud-Nutzer und Cloud-Anbieter sowie
- Kontrollverfahren.

Für Deutschland gibt es darüber hinaus den [IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik \(BSI\)](#)<sup>7</sup> zur Erkennung und Vermeidung sicherheitsrelevanter Schwachstellen in IT-Umgebungen. Dieser kann als Grundlage für Gespräche zum Thema Sicherheit mit dem Cloud-Anbieter genutzt werden.

#### 4.4 Portabilität

Portabilität bezeichnet im Allgemeinen die Unabhängigkeit von Computerprogrammen (oder IT-Services) von ihrer spezifischen Implementierung auf einer bestimmten IT-Plattform.

Die Portabilität einer Cloud-Lösung ist der Grad der Unabhängigkeit der zur Verfügung gestellten Services eines Anbieters von ihrer Implementierung in der Cloud.

Die Portabilität von Cloud-Angeboten hat drei wesentliche Ebenen:

- Portabilität der Services,
- Portabilität der Schnittstellen und Austauschformate und
- Portabilität der Daten und Prozesse.

Die erste Ebene „Portabilität der Services“ betrifft die Möglichkeit zum Wechsel zwischen Anbietern derselben Lösung und somit die zur Realisierung des Cloud-Service notwendige Software. Services, bei denen die zur Realisierung des Service notwendige Software im Markt nicht unabhängig vom Service-Anbieter verfügbar ist, besitzen ein geringeres Maß an Portabilität, weil der betreffende Service von anderen Anbietern nicht in identischer Form angeboten werden kann. Eine höhere Portabilität besitzen Services, die auf derselben Software basieren und deswegen in ihrer Zielsetzung und ihrem Leistungsumfang von mehreren Cloud-Dienstleistern angeboten werden.

So ist beispielsweise der Wechsel von einem Anbieter einer Cloud-basierten Kollaborationslösung zu einem anderen Anbieter, dessen Angebot auf derselben Software basiert, in der Regel unkomplizierter als zu einem Cloud-Service, der mit anderer Software realisiert wurde. Mit Open-Source-Software realisierte Cloud-Services können außerdem auch unabhängig vom Hersteller der Software durch andere Cloud-Anbieter oder den Anwender selbst implementiert werden und gewährleisten somit ein recht hohes Maß an Portabilität.

Die zweite Ebene „Portabilität der Schnittstellen und Austauschformate“ betrifft den Wechsel zwischen Anbietern von Lösungen, die auf unterschiedlicher Software basieren. Hier ist oft die Integration der neuen Lösung mit anderen Teilen der IT- und Prozesslandschaft des Anwenders eine zusätzliche Herausforderung. Cloud-Services, die mit offenen Standards arbeiten, lassen sich potenziell einfacher zu einem anderen Anbieter übertragen, weil die zur Integration in die Prozesslandschaft des Anwenders notwendigen Schnittstellen vom neuen Anbieter implementiert werden können, ohne dass dazu beispielsweise das Einverständnis des ursprünglichen Anbieters notwendig ist.

7 [https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge\\_node.html](https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html) (letzter Zugriff: 04.09.2012)

Die dritte Ebene „Portabilität der Daten und Prozesse“ betrifft die Portabilität der in der Cloud lagernden Daten und Prozesse des Anwenders. Bei einem Wechsel von Cloud-Service-Anbietern muss es möglich sein (etwa mit Hilfe von standardisierten Schnittstellen), die evtl. vorhandenen Anwenderdaten sowie die innerhalb des Cloud-Service gespeicherten Prozesse aus einem Cloud-Service in einen anderen Cloud-Service (oder ins eigene Rechenzentrum) zu überführen. Je standardisierter und einfacher ein Umzug ist, desto höher ist die Portabilität der Cloud-Lösung.

Die Portabilität von Cloud-Lösungen (Services und Daten) ist ein sinnvolles Entscheidungskriterium für die Anbieter-Auswahl und sollte ein fester Bestandteil bei der Betrachtung der Kosten einer Cloud-Lösung sein. Hier ist auch zu prüfen, wie das Betriebsmodell (vgl. Kapitel 3) die Portabilität beeinflusst.

## 4.5 Interoperabilität

Interoperabilität beschreibt die Möglichkeiten, IT-Systeme, Hard- und Software über offene Standards und Schnittstellen so aufeinander abzustimmen, dass diese Systeme reibungslos miteinander kommunizieren und die Daten unter Berücksichtigung des Datenschutzes verarbeitet werden können.

Die Interoperabilität einer Cloud-Lösung ist der Grad an Kooperationsfähigkeit der Cloud-Lösung mit anderen IT-Diensten (z. B. mit anderen Cloud-Lösungen). Je größer die Kooperationsfähigkeit, desto einfacher (kostengünstiger) können Geschäftsprozesse über mehrere Cloud-Lösungen oder andere Implementierungen von IT-Diensten hinweg realisiert werden.

Die dauerhafte Interoperabilität zwischen (Cloud-)Produkten unterschiedlicher Hersteller wird durch die Verwendung von „offenen Standards“ beispielsweise zur Authentifizierung, für Kommunikationsprotokolle oder für Datenaustauschformate begünstigt. Von einem offenen Standard spricht man dann, wenn der entsprechende Standard in einer offenen und transparenten Weise entwickelt, gepflegt und veröffentlicht wird

und er unabhängig von der Wahl des Geschäftsmodells frei verwendbar ist.<sup>8</sup> Cloud-Angebote, die offene Standards unterstützen, ermöglichen es Herstellern anderer Cloud-Angebote auf diese Weise, interoperable Angebote zu erstellen, ohne dass diese etwa zu Vereinbarungen oder Lizenzzahlungen gegenüber dem ursprünglichen Anbieter verpflichtet werden. Dies fördert die Bildung sogenannter „Ökosysteme“ zueinander passender Lösungen und sichert somit langfristig Interoperabilität.

Daneben muss bei der Auswahl eines Cloud-Service darauf geachtet werden, ob dieser die zur Integration in die IT-Prozesse des Anwenders notwendigen Schnittstellen und Austauschformate unterstützt. Beispiele für wichtige Dokumentenaustauschformate und Schnittstellen sind OOXML und ODF.

<sup>8</sup> Eine weitgehend akzeptierte Definition des Begriffes „Open Standard“ findet sich im europäischen Interoperabilitätsrahmen für pan-europäische eGovernment-Services der EU: <http://ec.europa.eu/idabc/servlets/Doca2cd.pdf>, S. 9 (letzter Zugriff: 04.09.2012)

# 5. Zertifizierung und Standardisierung

## 5.1 Zertifizierung

Eine Zertifizierung ist ein Nachweis für die qualitative und sichere Erbringung von Services.

Das Angebot von Cloud-Diensten ist komplex und vielfältig. Der Markt bietet für zahlreiche Bedürfnisse maßgeschneiderte Angebote. Auch aus diesem Grund gibt es derzeit keine Cloud-spezifischen Zertifizierungen. Allerdings existieren eine Reihe von internationalen Standards zur Zertifizierung einzelner Aspekte der IT, die auch für Cloud Computing relevant sind, wie zum Beispiel ISO 27001 im Bereich der Informationssicherheit (vgl. Kap 4.3).

Auf dem Markt existieren ergänzende Zertifikate – sogenannte „Hausstandards“ – im Umfeld der Cloud-Sicherheit, beispielsweise von Branchenverbänden oder Prüforganisationen. Diese Zertifizierungen zielen darauf ab, die Sicherheit einer Cloud auf Grundlage












eigener Anforderungskataloge zu prüfen und mit einem Zertifikat zu bestätigen. Aber dergleichen Zertifikate bieten keine Garantien oder Sicherheiten und entbinden den Cloud-Anwender auch nicht von seinen Kontrollpflichten.

## 5.2 Standardisierung

Für Cloud-Anwender, die insbesondere ein internationales Geschäftsumfeld bedienen, ist es sinnvoll, darauf zu achten, ob Cloud-Anbieter ihre IT-Infrastruktur auf bestimmte Standardisierungen hin ausrichten und so zumindest eine „Grundausstattung“ beispielsweise an definierten Schnittstellen bieten.

Weltweit gibt es rund 150 Organisationen, die sich mit Aspekten der Standardisierung im Cloud Computing befassen. Davon ist derzeit nur ein kleiner Teil relevant<sup>9</sup>:

Abb. 2: Wichtige Standardisierungsorganisationen im Cloud Computing

Auswahl	Allgemein	Cloud Computing	IKT, Sonstige
International		   	      
	USA		
Europa			
Deutschland		 	

Quelle: BMWi, Das Normungs- und Standardisierungsumfeld von Cloud Computing, 2012

Von diesen Organisationen im Normungs- und Standardisierungsumfeld seien exemplarisch erwähnt:

#### International:

- Die Cloud Security Alliance (CSA) setzt sich zusammen aus Anbietern von Cloud-Lösungen, Verbänden und Einzelpersonen. Sie zielt vor allem auf die Verbreitung von Best Practices im Bereich Sicherheit.  
[www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org)
- Das Open Cloud Consortium (OCC) ist ein gemeinsätziger Zusammenschluss von Unternehmen, Hochschulen und Behörden. Entwickelt werden sollen insbesondere Prüfmarken und Standards wie z. B. der MalStone Benchmark.  
[www.opencloudconsortium.org](http://www.opencloudconsortium.org)

#### Europa:

- EuroCloud ist ein europaweiter Zusammenschluss von Unternehmen, die Cloud-Lösungen anbieten (mit einer Sektion in Deutschland). Neben der Förderung von Akzeptanz und Vertrauen bezüglich Cloud-Lösungen gehört beispielsweise auch ein EuroCloud Star Audit („SaaS-Gütesiegel“) zu den Verbandszielen.  
[www.eurocloud.org](http://www.eurocloud.org)  
[www.eurocloud.de](http://www.eurocloud.de)
- SaaS-EcoSystem e. V. ist ein Zusammenschluss von Unternehmen, die Cloud- und SaaS-Lösungen anbieten. Neben dem Ziel, Cloud- und SaaS-Lösungen weiter in mittelständischen Unternehmen in Deutschland zu etablieren, hat der Verein die Standards „Trust in Cloud“ (SaaS) und „Cloud Experte“ erarbeitet.  
[www.saasecosystem.org](http://www.saasecosystem.org)

Eine weitergehende Übersicht sowie eine Beschreibung sämtlicher im vorstehenden Schaubild erwähnter Organisationen bietet eine Studie im Auftrag des BMWi<sup>10</sup>.

10 <http://www.trusted-cloud.de/de/878.php>

## 6. Orientierungshilfe zur Auswahl eines Cloud-Anbieters – wesentliche Leitfragen

Die im Folgenden genannten Leitfragen sollen beim Einstieg in die Überprüfung der fünf beschriebenen Anforderungen bei der Auswahl von Cloud-Computing-Angeboten helfen. Sie sind keineswegs erschöpfend und können insbesondere die Untersuchung der individuellen oder branchenspezifischen Anforderungen nicht ersetzen, bestenfalls ergänzen.

### 6.1 Rechtskonformität

- Informiert der Cloud-Anbieter transparent darüber, an welchen Standorten/in welchen Ländern sein Service betrieben wird?
- Welche gesetzlichen Regelungen muss der Cloud-Anwender – unabhängig von einer Cloud-Nutzung – berücksichtigen?
- Kommt der Anbieter mit seinem Cloud-Service der erforderlichen Rechtskonformität für den Cloud-Anwender nach?

### 6.2 Datenschutz

- Welche Datenschutzmaßnahmen hat der Cloud-Anbieter implementiert? Wird das den Anforderungen des Kunden gerecht?
- Wie reagiert der Anbieter bei datenschutzrelevanten Vorfällen? Wie unterrichtet der Cloud-Anbieter im Falle eines datenschutzrelevanten Vorfalls?

### 6.3 Informationssicherheit

- Welche Sicherheitsmaßnahmen hat der Cloud-Anbieter implementiert? Wird das den Anforderungen des Kunden gerecht?
- Bietet der Anbieter eine Verschlüsselung der Daten und der Kommunikation an?
- Welche Maßnahmen ergreift der Anbieter, um die Verfügbarkeit seines Dienstes sicherzustellen?
- Welche Maßnahmen zur Sicherung und Wiederherstellung von Daten bietet er an?

- Wie reagiert der Anbieter bei sicherheitsrelevanten Vorfällen?
- Wie geht der Anbieter mit den Daten des Anwenders nach Beendigung des Vertragsverhältnisses um?
- Wie sieht das Benutzer- und Zugriffsmanagement aus?
- Kann der Anbieter Mandantenfähigkeit und Mandantentrennung gewährleisten?

### 6.4 Portabilität

- Kann der Cloud-Service auch vom Anwender selbst oder einem anderen Dienstleister/Cloud-Anbieter realisiert werden?
- Sind entsprechende Angebote im Markt verfügbar?
- Stellt der Service für die Integration in die Prozesslandschaft Schnittstellen und Austauschformate zur Verfügung, die auch von anderen Services bereitgestellt werden?
- Welche Schnittstellen und Verfahren stehen zur Verfügung, um die innerhalb eines Cloud-Service gespeicherten Daten und Prozesse zu exportieren?
- In welche anderen Cloud-Services lassen sich die aus dem fraglichen Service exportierten Daten und Prozessinformationen wieder importieren?

### 6.5 Interoperabilität

- Welche Schnittstellen und Austauschformate werden zur Integration eines Cloud-Angebotes in die Prozesslandschaft des Anwenders benötigt?
- Welche Schnittstellen und Austauschformate unterstützt der Cloud-Service?
- Bei welchen vom Cloud-Service unterstützten Schnittstellen und Austauschformaten handelt es sich um offene Standards?
- Beteiligt sich der Service-Anbieter an der Pflege und Weiterentwicklung der entsprechenden Standards?

# Anhang

## Übersicht der Mitwirkenden der Fachinitiative „Cloud Computing“

Claudia Mrotzek*	ORACLE Deutschland B.V. & Co. KG
Manfred Bauer	Cisco Systems GmbH
Peter Domschitz	Alcatel-Lucent Deutschland AG
Fouad El Sioufy	TÜV Rheinland Consulting GmbH
Martin Falenski	Initiative D21 e. V.
Peter Ganten	Univention GmbH
Dr. Jörg-Michael Hasemann	T-Systems International GmbH
Jens Mühlner	Deutsche Telekom AG
Dr. Norbert Niebert	Ericsson GmbH
Percy Ott	Cisco Systems GmbH
Dr. Johannes Prade	Nokia Siemens Networks GmbH & Co. KG
Bernhard Przywara	ORACLE Deutschland B.V. & Co. KG
Hendrik Reese	TÜV Rheinland i-sec GmbH
Boris Schmidt	Deutscher Verband für Telekommunikation und Medien e.V. (DVTM)
Dr. Gerhard Tobermann	ORACLE Deutschland B.V. & Co. KG
Mark Vasic	Deutsche Telekom AG
Johannes Wust	Hasso-Plattner-Institut für Softwaresystemtechnik GmbH

\* Leiterin der Fachinitiative



