Eckpunkte für sicheres Cloud Computing

Leitfaden für die Auswahl vertrauens-würdiger Cloud Service Provider

BITKOM

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org
Ansprechpartner:	Dr. Mathias Weber Tel.: 030.27576-121 m.weber@bitkom.org
Verantwortliches Gremium:	BITKOM-Arbeitskreis Cloud Computing
Projektleitung:	Dr. Mathias Weber (BITKOM)
Copyright:	BITKOM 2013
Grafik/Layout:	Design Bureau kokliko/ Astrid Scheibe (BITKOM)
Titelbild:	Astrid Scheibe (BITKOM) unter Verwendung von © iStockphoto.com/Olena_T

Eckpunkte für sicheres Cloud Computing

Leitfaden für die Auswahl vertrauens-würdiger Cloud Service Provider

BITKOM

Verzeichnis der Abkürzungen

AGB	Allgemeine Geschäftsbedingungen
ASP	Application Service Providing
BDSG	Bundesdatenschutzgesetz
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BPaaS	Business Process as a Service
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC EAL4	Common Criteria - Evaluation Assurance Level 4
CDMI	Cloud Data Management Interface
CEPS	Centre for European Policy Studies
CIO	Chief Information Officer
COPPA	Children‘s Online Privacy Protection Act
CRM	Customer Relationship Management
CSP	Cloud Service Provider
CSV	Comma-separated values (Dateiformat)
EAM	Enterprise Architecture Management
ECP	European Cloud Partnership
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
FerD	Forum elektronische Rechnung Deutschland
FISA	Foreign Intelligence Surveillance Act
FTC	Federal Trade Commission
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
HIPAA	Health Insurance Portability and Accountability Act
HTTP	HyperText Transfer Protocol
IaaS	Infrastructure as a Service
ISO	International Standards Organization
IT	Informationstechnologie
IT SEC E3	IT Security Evaluation Criteria E3
KMU	kleine und mittelständische Unternehmen
LDAP	Lightweight Directory Access Protocol
LIBE	Innenausschuss des Europaparlaments
MaRisk	Mindestanforderungen an das Risikomanagement
NSL	National Security Letter
OCCI	Open Cloud Computing Interface
PaaS	Platform as a Service
REST	Representational State Transfer
RZ	Rechenzentrum
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SLA	Service-Level-Agreement
SOA	Service-orientierte Architektur
SOAP	Simple Object Access Protocol
SSL	Storage Structure Language
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
VM	Virtual Machine
XBRL	eXtensible Business Reporting Language
XML	Extensible Markup Language

Inhaltsverzeichnis

Verzeichnis der Tabellen

Verzeichnis der Abbildungen

1 Geleitwort – Cloud Computing auf dem Vormarsch

Prof. Dieter Kempf
BITKOM Präsident,
Vorsitzender des Vorstands Datev eG

Im Jahr 2012 hat gut ein Drittel (37 Prozent) aller Unternehmen in Deutschland Cloud Computing eingesetzt. Das hat der Cloud Monitor 2013 ergeben – eine gemeinsam von BITKOM, KPMG und PAC durchgeführte repräsentative Unternehmensbefragung. Im Vergleich zum Vorjahr entspricht das einem Anstieg von 9 Prozentpunkten. Weitere 29 Prozent der Unternehmen planten den Einsatz konkret oder diskutierten ihn. Für ein Drittel ist Cloud Computing (noch) kein Thema. In der Wirtschaft setzt sich Cloud Computing zunehmend in der Breite durch. So nutzten laut Cloud Monitor 2013 bereits fast zwei Drittel der Großunternehmen ab 2.000 Mitarbeitern Cloud Computing, im Mittelstand mit 100 bis 1.999 Mitarbeitern war es mit 45 Prozent fast die Hälfte.
Cloud Computing bringt gerade den mittelständischen Unternehmen handfeste Vorteile: In erster Linie profitieren sie von einem Zuwachs an Flexibilität. Der Wandel von Fixkosten zu variablen Kosten sowie die Bezahlung nach Verbrauch sind dabei wichtige Facetten.

Die Mittelständler erhalten IT-Leistungen mit einer im Eigenbetrieb nicht erreichten verlässlichen Verfügbarkeit und IT-Sicherheit, wobei oftmals außerdem die Kosten geringer ausfallen. Jedes Unternehmen sollte den Einsatz zumindest prüfen, um seine Wettbewerbsfähigkeit zu erhöhen.
Die überwiegende Zahl der Cloud-Nutzer setzt gegenwärtig auf interne Private Clouds. Vier von fünf Nutzern beurteilen ihre Erfahrungen mit Private Clouds positiv. Deutlich seltener erfolgte die Nutzung von Public Clouds. So sagen 79 Prozent der Unternehmen, die Public-Cloud-Lösungen ablehnen, dass sie Angst vor einem Datenverlust haben. Gerade kleine und mittelständische Unternehmen erreichen mit Cloud-Lösungen in der Regel ein deutlich höheres Sicherheitsniveau als mit IT-Systemen, die sie in Eigenregie betreiben. Die Sicherheit der Daten und das Vertrauen der Nutzer stehen im Fokus der Cloud Service Provider – sie stellen für diesen Bereich erhebliche Investitionen zur Verfügung.
Wegen des hohen Nutzens für den Mittelstand sollten Wirtschaft und Politik aus BITKOM-Sicht das Cloud Computing weiter vorantreiben. Dafür muss ein verlässlicher Rechtsrahmen geschaffen werden, damit Europa nicht hinter Länder wie die USA zurückfällt. Beim Datenschutz besteht mit der neuen EU-Verordnung die Chance, einheitliche Regelungen innerhalb des Europäischen Wirtschaftsraums zu schaffen. Zudem wird auf internationaler Ebene zu klären sein, unter welchen Voraussetzungen Sicherheitsbehörden auf Daten aus der Cloud zum Beispiel zum Zweck der Terrorabwehr zugreifen dürfen. Wir brauchen in der Cloud mehr Rechtssicherheit und mehr Transparenz in Fragen der nationalen Sicherheit.

Prof. Dieter Kempf
BITKOM Präsident

2 Management Summary

Adressaten und Ziele des Leitfadens

- Der kompakte Leitfaden adressiert primär Entscheider aus kleinen und mittelständischen Unternehmen (KMU) und stellt Eckpunkte für sicheres Cloud Computing auf. Damit sollen Interessenten die Entscheidung pro Cloud sowie die Auswahl für einen Cloud Service Provider erleichtert werden. In KMU wird der Mehrwert von Cloud-Angeboten oft unterschätzt. Deswegen werden im Leitfaden die aus der Cloud-Nutzung entstehenden Chancen verdeutlicht:
  - Durch Konzentration auf das eigene Kerngeschäft verkürzen Unternehmen ihre eigene Fertigungstiefe – sie können so Qualität, Wettbewerbschancen und Wachstum erhöhen. Größere Marktanteile wiederum senken Stückkosten und stärken Marktposition.
  - Standardisierte, aktualisierte und konsolidierte IT erleichtert und beschleunigt die Markteinführung neuer Produkte und leistet dadurch Wettbewerbsvorteile.
  - Die Verwandlung fixer Kosten aus Investitionen in variable Kosten ermöglicht es, das nicht mehr gebundene Kapital in die Entwicklung und Einführung neuer Produkte und den Ausbau des Vertriebs zu investieren.
  - Unternehmen erhöhen ihre Flexibilität, denn Cloud Services können nach Bedarf flexibel in Anspruch genommen werden, Kosten und Nutzen entsprechen so dem tatsächlichen Bedarf.
  - Unternehmen können Auslastungs-, Personalkapazitäts- und Know-how-, Technologie- und Haftungsrisiken an den Dienstleister verlagern – wie auch Kapitalbindung und Investitionsrisiken.
  - Cloud Computing bietet eine verlässliche Verfügbarkeit der IT-Services sowie ein Niveau der IT-Sicherheit, die mittelständische IT-Anwender ohne die professionelle Unterstützung von IT-Dienstleistern mit vertretbarem Aufwand nicht erreichen können.
- Im Zentrum des Leitfadens stehen Business-relevante Unternehmensanwendungen. Der Leitfaden soll aufzeigen: Wo liegen die Hebel im Cloud Computing, und welche prinzipiellen Lösungen gibt es, sie in Gang zu setzen? Mit der Beantwortung dieser Fragen wird das Vertrauen in die neuen Möglichkeiten des Cloud Computings gestärkt.
- Der Leitfaden ergänzt das BSI-Eckpunktepapier für sicheres Cloud Computing[1], an dem auch BITKOM beteiligt war, und bietet praktisch nutzbare Entscheidungshilfen.

Nutzung von Cloud-Services in Unternehmen – wo liegen die Hebel?

Unternehmen stellen heute besondere Ansprüche an die IT. Diese muss dem Unternehmen Marktchancen eröffnen, gleichzeitig aber auch sicher und zuverlässig sein. IT bzw. IT-Services müssen demnach folgende Eigenschaften besitzen: funktionell, schnell, skalierbar, flexibel, sicher, zuverlässig, hochverfügbar, kostengünstig, effizient und transparent. Cloud Computing, als echte Sourcing-Alternative, verspricht eine Antwort auf die Anforderungen, die das Business heute an IT stellt.

[1] Vgl. [BSI, 2010]

Unternehmensstrategie – Rahmen für die Nutzung von Cloud Computing

Cloud Computing ist eine strategische Option, die Unternehmen viel Potenzial bietet. Deren Realisierung kann durch begleitende Strategien und Maßnahmen verstärkt werden. Cloud Computing ermöglicht zudem eine Fokussierung auf die eigenen wertschöpfenden Prozesse in den Unternehmen. Gleichzeitig erhöht sich die unternehmerische Flexibilität. Die Notwendigkeit entfällt, ein eigenes Technologie-Portfolio für IT vorzuhalten. Der Nutzen kann verstärkt werden, wenn Strukturen zur strategischen und operativen Steuerung des Cloud Computing frühzeitig im Rahmen einer proaktiven Pilotierung und begleitet von einer kommunizierten IT-Cloud-Computing-Strategie entwickelt werden. Wesentliche zusätzliche Vorteile können aus einem übergreifenden Architektur-Management, einer angepassten Governance sowie einem strategischen und operativen funktionalen Anforderungs-Management gezogen werden.

Wirtschaftlichkeit

Cloud Computing bietet die Chance, Investitionsbedarfe im Bereich IT zu verringern und somit das in den bestehenden IT-Anlagen gebundene Vermögen für andere betriebliche Zwecke zu verwenden. Damit verändert sich zum einen die Bilanzstruktur des Unternehmens, zum anderen werden Up-front-Kosten für die Inbetriebnahme von IT-Anlagen reduziert. Darüber hinaus erlaubt die verbrauchsabhängige Fakturierung der bezogenen IT-Leistungen eine Feinsteuerung der Bedarfe und die Vermeidung von Leerkapazitäten. Dem gegenüber stehen Einmalkosten für die Inbetriebnahme der Cloud-Anwendung. Im Kapitel 5 werden die Chancen des Cloud Computings zur Verbesserung der eigenen Wirtschaftlichkeit getrennt nach Kostenfaktoren aufgezeigt.

Compliance, Datenschutz, IT-Sicherheit und Zertifizierung

Etwa zwei Drittel der kleinen und mittelständischen deutschen Unternehmen benötigen kompetente IT-Unterstützung, die durch Cloud Service Provider erbracht werden kann. Im Kapitel 6.1 sind die Punkte zusammengefasst, deren Beachtung nach aktuellen Gesetzen und Anforderungen für den IT-Betrieb notwendig ist.

Solange es keine weithin anerkannten internationalen Zertifikate für die Cloud Service Provider gibt, ist für den Cloud-Nutzer als Orientierung Folgendes wichtig: Normen und Zertifizierungen für Cloud Service Provider sollten sich an bereits bestehende und allgemein in der Branche akzeptierte Ansätze wie z. B. ISO 27001 und ISO 27002 anlehnen, die um essenzielle Cloud-Spezifika ergänzt werden.

Die verschiedentlich angebotenen Gütesiegel haben nur eine eingeschränkte Aussagekraft.

Interoperabilität, Integration und Standardisierung

Die Normierung der Cloud hinsichtlich Interoperabilität und Integration ist derzeit Gegenstand politischer Initiativen auf nationaler und europäischer Ebene. Auch die Industrie und die Verbände versuchen, einheitliche Standards auf dem Markt zu etablieren. Mit Ausnahme von Webservice-Standards und der universellen Auszeichnungssprache XML haben sich bisher noch keine Standards auf breiter Linie durchgesetzt. Deshalb muss für jeden einzelnen Geschäftsprozess geklärt werden, welche Cloud Services integrierbar sind. Die im Abschnitt 7.3 formulierten Kontrollfragen unterstützen den Verantwortlichen bei der erforderlichen Prüfung der Integrationsmöglichkeit von Cloud-Service-Angeboten in die vorhandene IT-Infrastruktur.

3 Nutzung von Cloud-Services in Unternehmen – wo liegen die Hebel?

Unternehmen stellen heute besondere Ansprüche an die IT. Diese muss dem Unternehmen Marktchancen eröffnen, gleichzeitig aber auch sicher und zuverlässig sein. IT bzw. IT-Services müssen demnach folgende Eigenschaften besitzen: funktionell, schnell, skalierbar, flexibel, sicher, zuverlässig, hochverfügbar, kostengünstig, effizient und transparent. Cloud Computing, als echte Sourcing-Alternative, verspricht eine Antwort auf die Anforderungen, die das Business heute an IT stellt.

Cloud Computing ist längst in der Realität angekommen und etabliert sich zunehmend auch im Mittelstand als echte Sourcing-Alternative. Auf die vor mehr als drei Jahren gestellte Frage: »Cloud Computing – Hype oder Realität?« antworten heute laut Cloud Monitor 2013 ein Drittel der Unternehmen, dass sie Cloud-Services aufgeschlossen gegenüber stehen. Eine Vielzahl dieser Unternehmen setzt nach eigener Aussage zurzeit Cloud Computing ein bzw. nutzt in irgendeiner Form das Cloud-Prinzip und hat damit bereits heute positive Erfahrungen gesammelt. Besonders hervorzuheben ist dabei die schnelle Skalierbarkeit und die Verringerung des IT-Administrationsaufwands, welche die Nutzung von Cloud Services mit sich bringt.

Dabei sind die Vorteile und Chancen von Cloud Computing und die damit verbundenen positiven Auswirkungen für das Unternehmen überzeugend[2]:

- Schnellere Skalierbarkeit der IT-Leistungen
- Senkung der IT-Ausgaben
- Höhere Innovationsfähigkeit
- Bessere Performance und Verfügbarkeit der IT-Leistungen
- Unterstützung von Kollaboration
- Orts-, zeit- und geräteunabhängiger Zugriff
- Steigerung der Effizienz.

In vielen Bereichen und Branchen liefert Cloud Computing Antworten auf aktuelle Herausforderungen des Business, denen sich Unternehmen zunehmend gegenüber sehen: dynamische Projekte, kürzere Produktzyklen, schnellere Time-to-Market und immer schneller »veraltendes« Fach-Know-how. Auf diese Einflüsse und Veränderungen müssen Unternehmen heute reagieren, wollen sie im Markt weiterhin erfolgreich agieren. Dabei wird nicht nur der Druck auf das Management größer, sondern auch auf dessen IT. Geschäftsprozesse, die durch die IT gestützt und abgebildet werden, müssen schnell und flexibel den neuen Gegebenheiten angepasst werden. IT-Ressourcen müssen immer schneller und dynamisch skalierbar zur Verfügung stehen, um z. B. für die Produktentwicklung oder für Marketing-Kampagnen flexibel genutzt werden zu können. Mit dem Einsatz von Cloud Computing ist dies möglich. Es können neue Geschäftsprozesse und komplett neue Business-Modelle oftmals schnell und flexibel implementiert oder überhaupt erst ermöglicht werden; das Business wird agiler. Reorganisationen in Unternehmen, Unternehmenszusammenschlüsse und Akquisitionen werden erleichtert. IT-Ressourcen stehen innerhalb kurzer Zeit zur Verfügung bzw. können ebenso schnell anderen Projekten zugeordnet werden, falls dies erforderlich ist.

[2] Vgl. [KPMG, 2013]

Cloud-Strategie aus Unternehmensstrategie ableiten

Cloud-Nutzer gewinnen eine größere Wahlfreiheit bei den Anwendungen und bei den Anbietern, Fachbereiche in den Unternehmen übernehmen stärkere Verantwortung für die Prozessunterstützung mit IT. Dies sollte sich in einer das Business unterstützenden Cloud-Strategie widerspiegeln (vgl. Kapitel 4). Dabei steht nicht nur allein die Technologie im Fokus, sondern der ganzheitliche Blick auf Technik, Prozesse und Organisation.

Denn ein dynamisches und flexibles Bezugs- und Produktionsmodell von IT kann und wird stärker als bisher das Geschäft unterstützen und vorantreiben.

Wirtschaftlichkeit des Cloud-Einsatzes

Wird die durch die Verwendung von Cloud Services die IT grundlegend flexibilisiert, erzielt das Unternehmen langfristig bedeutende Kostenvorteile. Die Kostenstrukturen verändern sich nachhaltig. Fixkosten werden zu variablen Kosten. Ein Teil der Investitionskosten wandelt sich zu Betriebskosten. Die nutzungsabhängige Bezahlung und der Abschied von festen IT-Budgets bedeuten eine Kostenvariabilisierung. Aufgrund dessen entscheiden sich Unternehmen zunehmend für Cloud Computing u.a. wegen des Potenzials zur Kostensenkung (vgl. Kapitel 5).

Interoperabilität, Integration und Standardisierung

Bereits der Einsatz einzelner Cloud Services bringt deutliche Kosten- und Managementvorteile. Aber erst eine enge Verzahnung von IT, Cloud-Service und Business-Prozess erzielt das Optimum an Vorteilen. Das Unternehmen erhält damit durchgängige, automatisierte IT-Prozesse und kann das Business schnell und flexibel unterstützen. Die Grundlage hierfür bilden Interoperabilität und Standardisierung (vgl. Kapitel 7).

Datenschutz, Compliance und IT-Sicherheit

Cloud und Recht scheinen sich in der öffentlichen Diskussion diametral gegenüber zu stehen. Dem gegenüber belegt das Thema Sicherheit im Cloud Monitor 2013, im Gegensatz zu den vergangenen Jahren, nicht mehr die vorderen Plätze. Der Umgang in der Praxis mit rechtlichen Rahmenbedingungen und IT-Sicherheit sind zwei wesentliche Aspekte, denen Cloud-Nutzer auch heute verstärktes Augenmerk widmen. Rechtliche Implikationen, beispielsweise im Hinblick auf Datenschutz, Compliance und Haftung, spielen bereits in der Entscheidungsfindung eine wichtige Rolle für Unternehmen, die eine Form von Cloud Computing einsetzen wollen und sollten bereits frühzeitig betrachtet werden (vgl. Kapitel 5.1).

Hebel	Erläuterung
Skalierbarkeit, Flexibilität und Agilität	Bereits heute ist IT in den meisten Unternehmen ein geschäftskritischer Faktor. Aber erst durch die Möglichkeit, Business-Prozesse durch Cloud Services dynamisch zu unterstützen und damit schnell auf Änderungen im Markt zu reagieren und flexibel neue Märkte zu besetzen, trägt die IT wesentlich zum Erfolg und zur Wettbewerbsfähigkeit des Unternehmens bei.
Kürzere Implementierungszeiten / schnellere Realisierung	Einführung und Einsatz von Cloud Computing erfordern wie jedes »klassische« IT-Projekt Aufwände. Hohe Standardisierung sowie hohe Automatisierung von Provisionierung und Betrieb erlauben den schnellen Bezugs und die schnelle Nutzung der Cloud Services. Hierdurch werden Unternehmen schneller bei der Umsetzung von Projekten und bei der Reaktion auf Marktänderungen – unter der Voraussetzung, dass die gewählten Services die Unternehmensstrategie unterstützen (vgl. Kapitel 4).
Reduktion von Komplexität und Administration	Durch den gezielten Einsatz von Cloud Computing im Unternehmen reduzieren sich Hardware-nahe administrative Tätigkeiten auf ein Minimum. Die damit verbundene Verringerung der verwendeten Systeme reduziert ebenfalls die Komplexität der IT-Systemlandschaft.
Reduktion der IT-Ausgaben	Cloud Computing tritt aufgrund des hohen Grades an Virtualisierung, Automatisierung und Standardisierung an, die Kosten der IT zu senken. Bei einer Wirtschaftlichkeitsbetrachtung spielen jedoch nicht nur die reinen Bezugskosten eine Rolle, sondern es müssen auch die durch Cloud erzielten Vorteile monetär erfasst und mit in das Kalkül gezogen werden (vgl. Kapitel 5).
Verbesserung der Performance und Verfügbarkeit	Als reale Sourcing-Alternative muss sich Cloud Computing in die IT- und Prozesslandschaft des Unternehmens integrieren. Um akzeptiert zu werden, müssen Performance und Verfügbarkeit der Cloud Services dem bisher Erreichten zumindest vergleichbar sein. Aufgrund des hohen Grades an Automatisierung sowie des Betriebs in zertifizierten Rechenzentren erfüllen bereits heute viele angebotenen Cloud Services diese Anforderungen.

Tabelle 1: Hebel für den breiteren Einsatz von Cloud Computing aus der Sicht deutscher Unternehmen[3]

[3] Vgl. auch [KPMG, 2013]

4 Unternehmensstrategie – Rahmen für die Nutzung von Cloud Computing

Cloud Computing ist eine strategische Option, die Unternehmen viel Potenzial bietet. Deren Realisierung kann durch begleitende Strategien und Maßnahmen verstärkt werden. Cloud Computing ermöglicht zudem eine Fokussierung auf die eigenen wertschöpfenden Prozesse in den Unternehmen. Gleichzeitig erhöht sich die unternehmerische Flexibilität. Die Notwendigkeit entfällt, ein eigenes Technologie-Portfolio für IT vorzuhalten. Der Nutzen kann verstärkt werden, wenn Strukturen zur strategischen und operativen Steuerung des Cloud Computing frühzeitig im Rahmen einer proaktiven Pilotierung und begleitet von einer kommunizierten IT-Cloud-Computing-Strategie entwickelt werden. Wesentliche zusätzliche Vorteile können aus einem übergreifenden Architektur-Management, einer angepassten Governance sowie einem strategischen und operativen funktionalen Anforderungs-Management gezogen werden.

4.1 Optimaler Einsatz der Unternehmensressourcen

Die Unternehmensstrategie jedes Unternehmens beschäftigt sich mit Fragen, wie:

- Wo liegen die Kernkompetenzen und Fähigkeiten des Unternehmens?
- Wo und wie lassen sich die zur Verfügung stehenden Ressourcen am wirkungsvollsten einsetzen?
- Wo lassen sich zusätzliche Potenziale zugänglich machen (z. B. Time-to-Market)?
- Wie kann die Qualität der Produktionsprozesse verbessert werden (z. B. Ausfallsicherheit, Flexibilität)?
- Wie können die Kosten der Produktionsprozesse reduziert werden?

Im Zusammenhang mit Cloud Computing stellen sich dann als wesentliche Fragen:

- Sind der Betrieb und das Management der technischen Infrastruktur und Standardsoftware von übergeordneter Bedeutung für den Unternehmenserfolg?
- Kann es eine Organisation geben, die die Erbringung der erforderlichen Leistung wirtschaftlicher und für das Unternehmen besser gestalten kann?

Die Antworten auf diese Fragen werden nicht für alle Unternehmen gleich lauten. Wirtschaftlichkeit und Unterstützung differenzierender Unternehmenspositionen hängen stark von der Größe des Unternehmens und dem Geschäftsumfeld ab.

4.2 Entwicklung der IT-Strategie aus der Geschäftsstrategie

Die Komplexität der Unternehmenslandschaft aus Geschäftsprozessen und IT-Systemen erfordert einen ganzheitlichen und strategischen Blick. Die technischen Details und damit auch die Technologien verlieren an Bedeutung. Relevant hingegen wird die Gestaltung der Anforderungen aus dem Business an die IT-Systeme, insbesondere an das Zusammenspiel der Bestandteile. Als Antwort entstand die Disziplin Enterprise Architecture Management[4] mit dem Nutzenversprechen, dass eine systematische Ableitung der Anforderungen an die verschiedenen Ebenen der IT-Systeme erfolgt.

Wann unterstützt die IT-Strategie die Unternehmensziele, wann ist die IT-Architektur geeignet?

Mit wachsender Komplexität des Geschäftsumfeldes muss eine Konzentration auf die differenzierenden Unternehmensfähigkeiten erfolgen. Erfolgreich zu sein bedeutet, die Komplexität im Unternehmen wo möglich zu reduzieren, was auf verschiedene Weise erfolgen kann.

IT-Strategie-Elemente, die den Nutzen von Cloud Computing verstärken:

Der veränderte Sicht auf die Bedeutung und der Umgang mit den Technologie-näheren Ebenen der IT-Systeme bietet viele neue Chancen, deren Nutzen verstärkt werden kann. Wichtig sind in diesem Zusammenhang:

- die Reduktion der In-house-Komplexität zur Gewinnung von Flexibilität, Geschwindigkeit und Kostenvorteilen durch stufenweise Modularisierung,
- das Prinzip der Kapselung[5] aus dem Informations-Management zur Reduktion der Komplexität bei gleichzeitiger Wahrung der Integrierbarkeit der Daten und Arbeitsabläufe, z. B. durch Service-orientierte Architekturen (SOA)[6],
- die Einführung und Nutzung von Standard-Software zur Reduktion der Entwicklungs- und Wartungskosten bzw. Einführungs- und Integrationsaufwände,
- die Integration oder enge Kopplung der eigenen Geschäftsprozesse mit denen anderer Geschäftspartner auf eine Cloud-Computing-Plattform ohne Lock-in in das Geschäftspartner-Netzwerk und ohne hohe Investitionskosten und langfristige Bindungen.

4.3 Strategische Nutzenverstärker

4.3.1 Nutzenverstärker Architektur-Management

- Eine Architekturstrategie[7] unterstützt die Integration vieler verschiedener Anforderungen und Systeme, einschließlich der externen Systeme.
- Eine zentrale Steuerung erleichtert das zukünftige Zusammenwachsen der eigenen und der Cloud-Computing-Lösungen.
- Verträglichkeit der Datenmodelle von inhaltlich zusammenhängenden Funktionsbereiche (Domänen) – im eigenen Unternehmen, mit den Cloud Service Providern und angeschlossenen Geschäftspartnern wird erreicht
- Übersicht und Steuerung der Informationsflüsse kann mit Master Data Management[8] gewährleistet werden

4 Vgl. [EAM, 2011]
5 Zerlegung in Module mit der kleinsten Schnittstellenkomplexität
6 Vgl. [SOAC, 2013]
7 Enterprise Architecture Management ist dafür eine etablierte Methode, vgl. [EAM, 2011], [TFEAM], [TOGAF].
8 Master Data Management ist eine Disziplin zum Management der vollständigen inhaltlichen Synchronisation von Informationen im Unternehmen. Unvollständige oder widersprüchliche Informationsstände in den verschiedenen Domänen sind extrem ineffizient und kostenträchtig.

4.3.2 Nutzenverstärker Governance

Hier sind zwei wichtige Punkte hervorzuheben:

- Cloud Computing verändert die Rolle des CIO ...
  - ... vom Betriebsmanager einer Infrastruktur zum Manager einer Supply Chain interner und externer Service-Provider[9]
  - ... und verschiebt den Fokus zur stärkeren Ausrichtung des Informations-Managements an Unternehmensanforderungen und -Strategie[10] sowie
  - ... zur Entwicklungsfähigkeit (und Integrierbarkeit) des Informations-Managements des Unternehmens intern und mit seinen Geschäftspartnern als wesentlicher Aufgabe.

Eine der wichtigsten Aufgaben eines CIO wird zukünftig sein, diese Gesamtorchestrierung sowie die Funktionsfähigkeit der Gesamtlandschaft aller IT-Systeme – und damit auch deren Zukunftsfähigkeit – sicher zu stellen. Das proaktive Angebot von Cloud-Computing-Lösungen erleichtert die synergetische Steuerung der aufkommenden Business-Initiativen.

Daraus leiten sich Handlungsempfehlungen ab:

- an die Unternehmen:
  Festlegung der Rolle zur Wahrung der übergreifenden Unternehmensinteressen und des strategischen Blickes und Sicherstellung der Kompetenz und Durchsetzungskraft – dieses Mandat sollte die Unternehmensleitung mit Verantwortung und Kompetenz an den CIO delegieren.
- an den CIO:
  Frühzeitige Übernahme der Führungsrolle bei der Implementierung von Cloud Computing und der Rolle eines fördernden Partners für die Fachbereiche. Mit der einfachen Verfügbarkeit von Cloud-Computing-Lösungen im Markt ist eine andere Positionierung der IT und des CIO über kurz oder lang weder erfolgreich noch durchsetzbar.

4.3.3 Nutzenverstärker: Business-Steuerung statt Detailkontrolle

Cloud Computing ermöglicht eine stärkere Konzentration auf die Differenzierungsmerkmale des Unternehmens. Die Umsetzung wird unterstützt durch

- Ziel- und Anforderungsdefinitions- sowie Vergabefähigkeit, die Bedeutung der Fähigkeit zur Ausführung Technologie-naher Aufgaben sinkt.
- Wechsel zum End-to-End-Monitoring von Business-Prozessen. Ein effektives SLA-Monitoring auf höheren Schnittstellenebenen verschiebt den Fokus von Technologie-orientierten Kenngrößen zum Geschäftserfolgsbeitrag.
- Die Verankerung der unternehmenswichtigen Standards und Verfahren in den prozessualen Schnittstellen und SLA mit dem Cloud Provider sichert die Compliance der Unternehmensprozesse. Ein direktes (möglicherweise non compliant) Eingreifen unter Umgehung der definierten Policies kann damit einfach ausgeschlossen werden. Wenn diese Fähigkeiten und Erfahrungen im Unternehmen noch nicht gegeben sind, können sie gut in kleineren, schnellen Pilotprojekten mit Cloud Computing erworben werden.

9 Vgl. [IDG 2010]
10 Enterprise Architecture Management ist dafür eine etablierte Methode, vgl. [EAM, 2011]

4.3.4 Nutzenverstärker: Anforderungs-Management – Management by Command oder Management by Strategy

- Die optimale Nutzung der standardisierten Cloud-Computing-Services profitiert stark von einer strategischen Planung der funktionalen Anforderungen an die Lösungen sowie die Entwicklung einer Roadmap.

- Die Auswahl eines Cloud Computing Providers mit einem Leistungsportfolio, das den zukünftigen Anforderungen entspricht, vermeidet notwendige Wechsel, deren Bedeutung mit wachsender Interoperabilität jedoch sinkt.

- Es empfiehlt sich, die Entwicklungsperspektiven in den verschiedenen Zeitskalen zu berücksichtigen

- Eine Planung der Mengenanforderungen ist hierbei von geringerer Bedeutung, dies wird durch die Flexibilität des Cloud Computing bedient.

4.3.5 Nutzenverstärker: Lösungs-Suiten

- Suiten von Standard-Software-Solutions eines Providers oder eines Provider-Netzes als Lieferantennetz können verhindern, dass die Grenzen der Interoperabilität Business-relevant werden.

- Ein Anforderungs-Management kann den strategischen Planungshorizont der Business-Prozess-Roadmap und die abgeleitete IT-Solution-Landscape integrieren, um die Kongruenz von Einzellösungen und der anvisierten Zeithorizonte fest zu stellen.

- Durch geringere Einrichtungszeiten und -kosten im Cloud Computing können hier auch kurzfristige Nutzungszeiten einer spezialisierten Lösung rentabel sein. Eine systematische Evaluierung der Anforderungen ist jedoch sehr empfehlenswert, um Funktions- oder Dateninseln zu vermeiden.

4.3.6 Nutzenverstärker: Standards und Standard-IT-Lösungen

- Eine Strategie, die dort stark auf standardisierte Lösungen setzt, wo die Kosten einer Individuallösung durch den Differenzierungsvorteil nicht aufgewogen werden, erhöht den Nutzen aus Cloud Computing erheblich. Die schnelle Verfügbarkeit beispielsweise als SaaS erleichtert die parallele Evaluierung und den einfachen Umstieg.

- Die iterative Entwicklung einer Lösung entsprechend der fortlaufenden Detaillierung der Business-Anforderungen bedeutet, dass möglicherweise nur eine Individuallösung aufsetzend auf Cloud-Computing-Lösungen niedrigerer Leistungstiefe, also beispielsweise IaaS statt SaaS, möglich ist. Damit werden nicht alle Potenziale des Cloud Computings genutzt.

5 Wirtschaftlichkeit

Cloud Computing bietet die Chance, Investitionsbedarfe im Bereich IT zu verringern und somit das in den bestehenden IT-Anlagen gebundene Vermögen für andere betriebliche Zwecke zu verwenden. Damit verändert sich zum einen die Bilanzstruktur des Unternehmens, zum anderen werden Up-front-Kosten für die Inbetriebnahme von IT Anlagen reduziert. Darüber hinaus erlaubt die verbrauchsabhängige Fakturierung der bezogenen IT-Leistungen eine Feinsteuerung der Bedarfe und die Vermeidung von Leerkapazitäten. Dem gegenüber stehen Einmalkosten für die Inbetriebnahme der Cloud-Anwendung. Im Kapitel 5 werden die Chancen des Cloud Computings zur Verbesserung der eigenen Wirtschaftlichkeit getrennt nach Kostenfaktoren aufgezeigt.

5.1 Einführung

Neben Flexibilität und Agilität resultiert ein weiteres, wichtiges Argument, sich mit dem Einsatz von Cloud Computing im Unternehmen zu befassen, aus den potenziellen Kostenvorteilen. Inwieweit diese Kostenvorteile nutzbar gemacht werden können, hängt von der Ausgangslage und dem Umfang des Cloud-Einsatzes ab, wobei die Entscheidung für eine Service-Ebene nicht allein wirtschaftlichen Überlegungen folgen sollte[11]. Eine Orientierung bieten hier die Service-Ebenen IaaS, PaaS und SaaS (vgl. Abbildung 1). Die rechts in der Abbildung 1 gezeigten Hilfsfunktionen beziehen sich auf die jeweilige Service-Ebene.

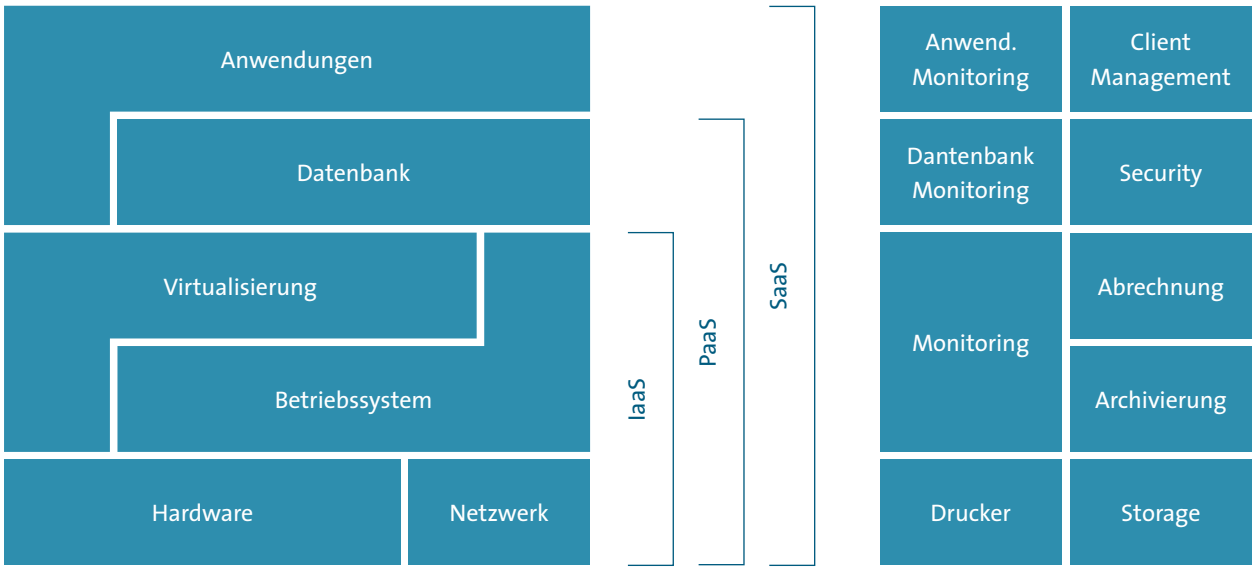

Abbildung 1: Architekturmodell und Hilfsfunktionen zur Wirtschaftlichkeit von Cloud-Services[12]

11 Vgl. dazu die Ausführungen im Kapitel 4
12 Vgl. dazu auch die Anlage 1 (Kapitel 9)

Der Entscheidung für einen Cloud Service Provider sollte zudem eine eingehende Untersuchung der Ist-Kosten vorausgehen. Nachfolgend werden die wesentlichen Faktoren im RZ-Betrieb zur Betrachtung der Wirtschaftlichkeit untersucht. Darüber hinaus bietet eine Check-Liste (vgl. Tabelle 5) eine Hilfestellung zur Bestimmung der Kostenstruktur und zu erwartender Verbesserungen der Wirtschaftlichkeit im Unternehmen.

5.2 Wirtschaftlichkeitsfaktoren

Die Wirtschaftlichkeit der Cloud-Nutzung richtet sich zunächst nach dem Einzelfall – also den Gegebenheiten und Anforderungen des betreffenden Unternehmens. Jedoch lassen sich einige allgemeine Gesetzmäßigkeiten in der Kostenbetrachtung aufzeigen. Dies betrifft zum einen übergeordnete Wirtschaftlichkeitsfaktoren, die die allgemeine Angebotsentwicklung im Bereich Cloud Computing betreffen (vgl. Abschnitt 5.2.1), zum anderen die konkreten Kostenfaktoren der Unternehmen (vgl. Abschnitt 5.2.2).

5.2.1 Allgemeine Wirtschaftlichkeitsfaktoren

Zu den allgemeinen Wirtschaftlichkeitsfaktoren von Cloud Computing gehören Faktoren, die den eigentlichen Kern des Cloud Computing ausmachen, wie z. B. die Abrechnungsform (Pay-per-use) oder die Form der Bedarfsdeckung (Self-Provisioning)[13] (vgl. Tabelle 2)

Für eine Wirtschaftlichkeitsbetrachtung müssen Cloud-Nutzer ihre Verbräuche und zukünftigen Bedarfe ermitteln.

13 Vgl. [Shr, 2011], [PBS, 2012], [Will, 2012] sowie [CC-ETRB, 2009] und [CC-WEWM, 2010]

Faktor	Erläuterung
Economies of scale	■ Bündelung der Kundenbedarfe ■ Günstige Einkaufspreise aufgrund des höheren Einkaufsvolumens ■ effektiverer Personaleinsatz, z. B. im Bereich Sicherheit ■ hoher Automatisierungsgrad - niedrigere Personalkosten ■ Zugang zu kostengünstigen Energieressourcen
Pay-per-use	■ grundsätzlich verbrauchsgesteuerte Abrechnung von Cloud Services ■ Bezugsgrößen bei Abrechnung variieren je nach Service-Ebene
Self-Provisioning	■ Kunden nutzen Cloud Services im Self-Service
Elastizität	■ Elastizität der Bedarfsdeckung durch Pay-per-use und Self-Provisioning Kapazitätsrisiko auf den Cloud Service Provider verlagert ■ Abbau von Überkapazitäten möglich
Time-to-Market	■ Cloud Service Provider bieten gängige Konfigurationen ■ Inbetriebnahme von RZ-Kapazitäten innerhalb von Stunden bzw. weniger Tag ■ Freischalten zusätzlicher User im Minutenbereich
IT-Sicherheit und Datenschutz	■ Management der Daten in großen Rechenzentren und durch professionell ausgebildetes Personal ■ Professionelle IT-Sicherheit
Technologieexpertise	■ Cloud Service Provider sorgt für neuesten Stand der Technologie
Downtime	■ Cloud-Nutzer vermeiden Doppelkapazitäten ■ Keine Bevorratung von Ersatzteilen

Tabelle 2: Wirtschaftlichkeitsfaktoren von Cloud Computing

5.2.2 Projektspezifische Faktoren

Neben den allgemeinen Wirtschaftlichkeitsfaktoren sind weitere, projektspezifische Faktoren zu berücksichtigen. Dazu gehören insbesondere

- die Service-Ebene:
  Als Faustregel gilt: Je höherwertig die genutzten Cloud Services sind, desto größer sind die Kosteneinspar-Potenziale, die in einer Einzelfallbetrachtung zu analysieren sind. Eine Hilfestellung dazu bietet die Checkliste in Tabelle 5.

- die gewählte Cloud-Organisationsform:
  Die Organisationsform hat entscheidenden Einfluss auf die Integrationsaufwände, die in dem jeweiligen Projekt zu bewerten sind.

- die Unternehmensgröße:
  Inwieweit die Größe des Unternehmens die Wirtschaftlichkeit des Cloud-Betriebs beeinflusst, hängt vom Anwendungsfall ab.[14] Jedoch kann durch den Einsatz von Cloud Computing die Komplexität der Anwendungslandschaft reduziert werden.

- die Datenmenge:
  Aufgrund des Pay-per-use-Preismodells besteht eine direkte Abhängigkeit zwischen den zu bearbeitenden Datenmengen und dem wirtschaftlichen Betrieb der Cloud-Plattform. Für ein konkretes Projekt z. B. im Bereich Business Intelligence oder Big Data sind den Cloud-Kosten die Vorhaltekosten für Analysekapazität entgegenzuhalten.

14 Vgl. [Forr 2009]

5.3 Vorgehensmodell zur Bewertung der Wirtschaftlichkeit

Die Untersuchung der Wirtschaftlichkeit von geplanten Cloud Anwendungen muss sich in die laufende IT-Bedarfs- und IT-Kapazitätsplanung einfügen (vgl. Abbildung 2). Wesentliche Voraussetzung für eine Wirtschaftlichkeitsbetrachtung ist eine detaillierte Kenntnis der eigenen IT-Kostenstruktur. Dazu wird in der Regel keine vollausgeprägte Kostenrechnung benötigt. Meistens wird es ausreichend sein, die bestehenden Kosten tabellarisch zusammenzufassen (vgl. Tabelle 3).

Vor allem benötigen Unternehmen eine verlässliche Datenbasis zu den bestehenden Kosten sowie den Auslastungen und Kapazitäten im IT-Bereich. Auf Basis des Pay-per-use-Modells des Cloud Service Providers lassen sich unter Berücksichtigung der Auslastung der vorhandenen Kapazitäten die notwendigen monatlichen Aufwände berechnen und den Einsparpotenzialen gegenüberstellen. Die Check-Liste in Tabelle 5 bietet hier eine Hilfestellung. Insbesondere sind die in Tabelle 3 aufgeführten Kostenfaktoren zu berücksichtigen:

Abbildung 2: Vorgehensmodell zur Wirtschaftlichkeitsbetrachtung

Faktor	Erläuterung
Gebäude	■ Stilllegung oder Beendigung der Anmietung von Gebäuden und Einrichtungen wie z. B. Alarmsysteme und Zugangsschutz
Infrastruktur	■ Reduzieren der Komplexität und Freisetzung von Kapazitäten
Softwarelizenzen	■ Bei SaaS Verlagerung der Lizenzkosten (Softwarelizenzen, Wartungsgebühren, Update- und Upgrade-Kosten) in die Cloud
Laufende Betriebskosten	■ Verminderung bei Kosten z. B. für Versicherungen, Reinigung, Überwachung, Energie
Management und Verwaltung	■ Cloud Computing entlastet die Mitarbeiter von Administrationsarbeiten und schafft Freiräume für innovative Projekte. ■ Reduzieren der Komplexität von Einkaufsprozessen und allgemeinen Verwaltungsprozessen
Wartung, Updates, IT-Security	■ Kosten vermindern sich durch Teilung mit vielen anderen Nutzern ■ Aktualisierungsaufwände für Sicherheits-Updates entfallen
Betrieb	■ Kosten für Client- und Server-Management sowie Anwender-Support vermindern sich bzw. verschwinden
Schulung IT	■ Es entfallen u.a. Kosten zur Fortbildung im Bereich Einrichtung, Betrieb und Wartung neuer Software-Releases
Schulung Endanwender	■ Schulungen der Endanwender erfolgt im Self-Service oder durch den Cloud Provider
Sicherheitskosten	■ Kostenvorteile können sich durch Verminderung lokaler Client-Installationen ergeben sowie durch Vereinfachung von Schnittstellen

Tabelle 3: Wichtige Faktoren bei der Ermittlung von Einsparpotenzialen durch Cloud Computing

5.4 Einführung von Cloud Computing

Aufgrund des weiter anhaltenden Ausbaus großer Rechenkapazitäten kann davon ausgegangen werden, dass die Preise für Rechenzeit weiterhin abnehmen werden. Im Bereich der Übertragungskapazitäten ist eine Abschätzung schwieriger, jedoch wird man zumindest von einem konstanten Preis-/Leistungsverhältnis ausgehen können. Diesen langfristigen Kostenvorteilen durch Cloud Computing sind Kosten z. B. für die Provider-Auswahl und die Einführung gegenzurechnen. Es entstehen weitere Kosten für Schulungsmaßnahmen aber auch – abhängig vom Umfang der Cloud-Nutzung – für ein regelmäßiges Monitoring des Cloud Service Providers (vgl. Tabelle 4).

Kostenart	Erläuterung
Auswahl des Providers	■ Kosten der Lieferantenauswahl und –bewertung (meist Einmalkosten) ■ Kosten für Vertragsgestaltung und rechtsanwaltliche Beratung
Einführungs-projektkosten	■ Aufwand für die Datenübernahme in das System des Cloud Service Providers ■ Reorganisation von Arbeitsabläufen und Organisation ■ Kosten für Maßnahmen zur Kontrolle und Überwachung des Cloud Service Providers ■ projektspezifische Aufwände für die Integration zu verbleibenden On-Premise-Systemen
Datenvolumina	■ Ggfs. Ausbau der externen Netzwerkanbindung für höhere Datenvolumina und redundanten Zugang
Schulung	■ Kosten für Mitarbeiterschulung
Monitoring und SLA-Kontrolle	■ Aufwände, die für das Monitoring und die SLA-Überwachung anfallen
Einfluss laufender IT-Projekte	■ die Einführung von Cloud-Services wird in der Regel die laufenden IT-Projekte beeinflussen – es können Integrationskosten zu On-Premise-Lösungen entstehen, die projektspezifisch zu schätzen sind.

Tabelle 4: Kosten für die Einführung von Cloud Computing (Auswahl)

Kostenstelle: Beschreibung	Kosten-typ	Kapital-bindung	Entfällt bei Cloud Services	Einspar-Potenzial
Gebäude: Grundstücke und Gebäude, Alarmsysteme (Feuermelder), Zugangsüberwachung (Videosysteme)	laufend	langfristig	Ja[15]	+++
Infrastruktur: Hardware, Netzwerk (Router[16]), Storage (SAN, NAS)	laufend	langfristig	Ja[17]	+++
Laufende Betriebskosten: Versicherungen, Reinigung, Klima, Kühlung, Energie	laufend	langfristig	Ja[18]	+++
Softwarelizenzen: Betriebssysteme, Monitoring-Software, Datenbank-Anwendungen	laufend	langfristig	Ja	+++
Management und Verwaltung: Management, Finanz-buchhaltung (Inventur, Abrechnung), Einkauf (Vertrags-management), Personalmanagement, Auditierung	laufend	langfristig	Ja	+++
Wartung und Updates (einschl. Test): Hardware, Netzwerk, Storage, Anwendungen	laufend	langfristig	Ja	+++
Kapazität: Abbau von Leerkapazitäten (Vorhaltekapazität für Lastspitzen)	laufend	langfristig	Ja	+++
Betrieb: Server Management, Client Management, Downtime, Monitoring, Anwendersupport (Helpdesk)	laufend	langfristig	Ja	++
Schulung IT: Hardware, Netzwerk, Storage, Anwendungen	laufend	langfristig.	Ja	++
Schulung Endanwender: Schulungserstellung und -durchführung	laufend	langfristig	Ja	++
IT-Sicherheit[19] Clientseitige Installation	laufend	langfristig	Ja	+
Orchestrierung von Services (Servicemanagement)	laufend	langfristig	Nein	-
Ggfs. Ausbau der externen Datenverbindung	einmalig	kurzfristig	Nein	-
Bereitstellung höherer externer Transfervolumina	laufend	langfristig	Nein	-
Providerauswahl: Allgemeine Information, Besuch von Fachtagungen	einmalig	n.a.	Nein	-
Einführungsprojektkosten: Altdatenübernahme, Schnittstellen, Reorganisation	einmalig	n.a.	Nein	-
Monitoring/SLA-Überwachung: Laufende SLA Überwachung	laufend	n.a.	Nein	-
Schulung: Self-Service Schulung	einmalig	n.a.	Nein	-
Einfluss laufender Projekte: Projektspezifisch	einmalig	n.a.	Nein	-

Tabelle 5: Check-Liste – Kostenfaktoren in der IT

15 Ggfs. sind verbleibende Anteile für On-Premise-Lösungen zu berücksichtigen.
16 Abhängig von der Netzwerkarchitektur
17 Vgl. Fußnote 15
18 Vgl. Fußnote 15
19 Soweit nicht unter Zugangskontrolle, Infrastruktur oder Softwarelizenzen berücksichtigt.

6 Compliance, Datenschutz, IT-Sicherheit und Zertifizierung

Nach Angaben des Statistischen Bundesamtes aus dem Jahre 2010 folgen ca. ein Drittel der kleinen und mittelständischen Unternehmen (KMU) einer IT-Sicherheitsstrategie, die Voraussetzung für Compliance und Datensicherheit ist. Zwei Drittel der KMU benötigen deshalb kompetente Unterstützung bei der Datenverarbeitung, die durch Cloud Service Provider erbracht werden kann. Im Abschnitt 6.1 sind die Punkte zusammengefasst, deren Beachtung nach aktuellen Gesetzen und Anforderungen für den IT-Betrieb notwendig ist.

Solange es keine weithin anerkannten Zertifikate für die Cloud Service Provider gibt, ist für den Cloud-Nutzer als Orientierung Folgendes wichtig: Normen und Zertifizierungen für Cloud Service Provider sollten sich an bereits bestehende und allgemein in der Branche akzeptierte Ansätze wie z. B. ISO 27001 und ISO 27002 anlehnen, die um essenzielle Cloud-Spezifika ergänzt werden. Dies schafft einen erheblichen Geschwindigkeitsvorteil und vermeidet gleichzeitig wettbewerbsrelevante Mehrkosten durch neue Zertifizierungen.

Die verschiedentlich angebotenen Gütesiegel sind nicht allgemein anerkannt und haben nur eine eingeschränkte Aussagekraft.

6.1 Datenschutz und Compliance[20]

Datenschutz und Compliance werden häufig als Hemmnis für die Nutzung von Cloud Computing genannt. Manche Unternehmen befürchten, Cloud Computing sei nicht mit dem Datenschutzrecht oder anderen Compliance-Anforderungen vereinbar; wer Cloud Computing nutze, verliere die Kontrolle über seine Daten. Diese Befürchtungen sind unberechtigt. Unternehmen können Leistungen aus der Cloud im Einklang mit dem Datenschutzrecht und anderen rechtlichen Anforderungen nutzen und behalten auch die volle Kontrolle über die Daten.

Auftragsdatenverarbeitung

Sofern ein Unternehmen personenbezogene Daten wie Namen, Anschrift, Geburtsdatum u.a. von Arbeitnehmern, Kunden, Lieferanten o.a. in der Cloud verarbeiten will, so dass der Cloud Service Provider Zugriff auf diese Daten nehmen kann, schließen Unternehmen und Cloud Service Provider einen Vertrag über Auftragsdatenverarbeitung. Damit ist gewährleistet, dass das Unternehmen die volle Herrschaft über die verarbeiteten Daten behält. Der Cloud Service Provider speichert, verarbeitet, löscht oder ändert die Daten nur auf Grund entsprechender Weisung seines Auftraggebers und behandelt sie vertraulich. Es ist damit vertraglich ausgeschlossen, dass der Cloud Service Provider die Daten für eigene Zwecke verwendet.

20 Vgl. zum »Datenschutz im weiteren Sinne«, also der Pflicht, wichtige Unternehmensdaten zu schützen, [CC-WEWM, 2010], Kap. 5, S. 60.

Datensicherheit

Datenschutz bedeutet außerdem, dass die Grundsätze der Datensicherheit gemäß Bundesdatenschutzgesetz eingehalten werden. Was diese Datensicherheit betrifft, also z. B. technische Maßnahmen zum Schutz der Vertraulichkeit, so können Cloud Service Provider mit ihrem spezialisierten Personal und hohen Investitionen in Sicherheitstechnik ein höheres Schutzniveau bieten als ein mittelständischer Cloud-Nutzer dies könnte. Vor dem Abschluss eines Vertrages über Auftragsdatenverarbeitung stellt der Cloud Service Provider dem Auftraggeber die nötigen Informationen zur Verfügung. Der Cloud-Nutzer muss prüfen, dass der Cloud-Anbieter die Sicherheitsmaßnahmen auch einhält, hierbei darf er sich auf Zertifikate wie ISO 27001 oder unabhängige Audits verlassen.

Angemessenes Datenschutzniveau

Der Einsatz von Cloud-Service-Providern ist nach deutschem Recht privilegiert, sofern die Daten innerhalb des Europäischen Wirtschaftsraumes[21] verarbeitet werden. Aber auch wenn ein Cloud Service Provider seinen Sitz außerhalb des Europäischen Wirtschaftsraumes hat oder Daten dort verarbeitet, dürfen deutsche Unternehmen im Normalfall diese Cloud nutzen, wenn sie bestimmte Voraussetzungen einhalten[22]. Die deutschen Datenschutzbehörden haben dies inzwischen anerkannt.

Safe-Harbor-Programm

Am wichtigsten ist es, dass ein angemessenes Datenschutzniveau besteht. In dem praktisch häufigsten Fall, nämlich bei Cloud Service Providern aus den USA, wird ein angemessenes Schutzniveau dadurch gewährleistet, dass der Cloud Service Provider am Safe-Harbor-Programm teilnimmt. Grundlage hierfür ist ein Abkommen, das die EU-Kommission im Jahr 2000 mit der US-Regierung geschlossen hat. Es gibt auch US-Cloud-Provider, die neben dem Safe-Harbor-Programm anbieten, mit dem Cloud-Nutzer einen sogenannten EU-Standardvertrag[23] zu schließen. Das ist eine weitere Möglichkeit, um ein angemessenes Datenschutzniveau herzustellen. Damit ist vertraglich sichergestellt, dass der Cloud-Provider in den USA die Daten nach EU-Datenschutzgrundsätzen verarbeitet und entsprechend schützt.

Besondere Lösungen in Ausnahmefällen

Es gibt Ausnahmefälle, vor allem in bestimmten Branchen, bei sensitiven und unternehmenskritischen Daten, die höhere Anforderungen stellen und besondere Lösungen erfordern. Im Normalfall, also bei der Mehrheit der im Unternehmen verarbeiteten Daten, ist es aber kein Problem, die Datenschutzanforderungen beim Cloud Computing einzuhalten. Durch vertragliche Vereinbarungen wird gewährleistet, dass der Cloud-Nutzer vollständig die Herrschaft über seine Daten behält und das notwendige Sicherheitsniveau besteht.

Compliance

Compliance bedeutet die Einhaltung des geltenden Rechts[24]. Die wichtigsten rechtlichen Anforderungen an Cloud Computing ergeben sich aus dem Datenschutzrecht. Ein Unternehmen, das das Datenschutzrecht einhält, erfüllt damit auch die wichtigste Compliance-Anforderung. Zusätzliche Anforderungen kommen dann hinzu, wenn bestimmte Dienste genutzt werden, beispielsweise wenn die Buchführung in die Cloud verlagert wird, oder in bestimmten Branchen, z. B. im Finanzsektor oder im Gesundheitswesen.

21 Das sind die EU-Staaten sowie Island, Liechtenstein und Norwegen.
22 Siehe hierzu im Einzelnen [KDOCC, 2011, S. 10 ff.]
23 Entscheidung der EU-Kommission vom 05.02.2010, 2010/87/EU
24 Vgl. zu den Einzelheiten: [CC-WEWM, 2010], Kap. V, S. 88 ff., insbesondere S. 91 ff. zum Compliance Management System

Checkliste

- Verarbeitung von personenbezogenen Daten oder Daten ohne Personenbezug?
- Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG
- Weisungsrechte des Auftraggebers
- Standorte der Rechenzentren
- Außerhalb EU/EWR: angemessenes Datenschutzniveau (Safe Harbor, EU-Standardverträge)
- Datenschutzmaßnahmen des Cloud-Anbieters
- Sicherheitsmaßnahmen des Cloud-Anbieters
- Mandantenfähigkeit und Mandantentrennung
- Benutzer- und Zugriffsmanagement
- Verschlüsselung der Daten und der Kommunikation
- Maßnahmen zur Datensicherung, Wiederherstellung und Verfügbarkeit des Dienstes
- Zertifikate (z. B. ISO 27001)
- Informationspflichten bei datenschutz- und sicherheitsrelevanten Vorfällen
- Behandlung der Daten bei Vertragsende
- Besondere Compliance- Anforderungen an bestimmte Dienste (z. B. GoBS, GDPdU für Buchführung)
- Branchenbezogene gesetzliche Anforderungen (z. B. MaRisk für Finanzdienstleister, EG Dual-Use-Verordnung)

Tabelle 6: Checkliste Datenschutz, Informationssicherheit und Compliance

6.2 IT-Sicherheit

6.2.1 IT-Sicherheit beim Cloud Service Provider[25]

Vertrauensentwicklung

Auf Grund der Dynamik im IT-Sicherheitsbereich sind genaue Beschreibungen technischer Maßnahmen eher hinderlich und schnell veraltet. Deshalb werden bei Leitfäden die zu beachtenden Bereiche genannt. Für die Realisierung sind dann ausgewiesene Spezialisten zu beauftragen. Zwischen CSP und Cloud-Nutzer ist ein Vertrauensverhältnis auf Grundlage von Zertifizierungen, erfolgreichem Betrieb – nachweisbar durch Bilanzzahlen – und Sorgfalt aufzubauen. Cloud Computing funktioniert nur mit Doppelsieg-Strategie.

Das Sicherheitsmanagement des CSP umfasst eine Reihe von Aufgaben, die für RZ und ASP Standard sind, wie Sicherheitskonzeption (IT-Grundschutz), Notfall-Management, Patch- und Änderungsmanagement, Informations- und Datenschutz etc. CSP können sich nach ISO 27000 oder BSI zertifizieren lassen. Gütesiegel bieten dem Cloud-Nutzer keine wirkliche Orientierung; sie sind nicht mit einem Zertifikat zu vergleichen[26].

IT-Sicherheit umfasst organisatorische, personelle und technische Maßnahmen nach dem aktuellen Stand der Technik.
Cloud Computing muss den deutschen Datenschutzbestimmungen gerecht werden, deshalb müssen personenbezogene Daten ausschließlich auf vom CSP kontrollierten Rechnern gespeichert und verarbeitet werden. Möglicherweise einbezogene Subunternehmer müssen die gleichen Anforderungen und Zertifizierungen wie der CSP erfüllen. Wenn ein CSP die nachfolgenden, als Basisanforderung genannten Punkte per Zertifizierung nachweisen kann bzw. eine Konformitäts-Erklärung abgibt, so ist der CSP vertrauenswürdig im Sinne dieses Leitfadens. Bei einer Konformitäts-Erklärung wird empfohlen, ein Audit durch einen zertifizierten Dritten durchführen zu lassen.[27]
IT-Sicherheit umfasst den Schutz vor Elementarschäden, z. B. durch Ausweich- bzw. Redundanzstandorte.
CSP-Standortsicherheit wird durch die in Tabelle 7 zusammengestellten Anforderungen beschrieben (Basisanforderung).

Die technischen Maßnahmen zur Gewährleistung der IT-Sicherheit nach BSI zeigt die Tabelle 8 (Basisanforderung). Analog spiegeln die Tabelle 9 die organisatorischen (Basisanforderung) sowie die Tabelle 10 die personellen Maßnahmen (Basisanforderung) wider.

Anforderungen
■ Redundante Versorgungskomponenten, Strom, Klima, Wasser, etc.
■ Rollenbasierte Zutrittskontrolle
■ Zwei-Faktor-Authentifizierung
■ Brandschutz
■ Robuste Infrastruktur, doppelte Netzanbindung, Notfallarbeitsplätze, etc.
■ Redundante Rechenzentren, Dokumentation und Kontrolle des Verfügbarkeits-Managements
■ Gebäudesicherheit, Zutrittskontrolle, sicherer Eingangsbereich
■ Kontrolle der Service-Dienstleister (Reinigung, Gebäudemanagement, Reparaturunternehmen etc.)

Tabelle 7: Anforderungen an die Standortsicherheit des Cloud Service Providers

25 Grundlage: [BSI, 2010]
26 Vgl. Abschnitt 6.3
27 Eine ausführliche Beschreibung der Basisanforderungen kann den BSI-Sicherheitsempfehlungen für Cloud-Computing-Anbieter entnommen werden (vgl. [BSI, 2010]).

Anforderungen	Maßnahmen
Serversicherheit	■ Schutz des Hosts (Firewall, Intrusion Detection, Integritätsprüfungen) ■ Sichere Grundkonfiguration (gehärtetes Betriebssystem) ■ Sandbox für jede virtuelle Maschine ■ Zertifizierte Hypervisoren (mindestens CC EAL4, IT SEC E3) ■ Gesicherte Images / Dienste des Providers ■ Bei IaaS Einsatz einer sicheren Sandbox-Umgebung, um Exploits auf Host-System zu verhindern ■ Auswertung der Systemdokumentationen, Logfiles etc.
Netzsicherheit	■ Redundante Vernetzung ■ Sicherheitsmaßnahmen gegen Netzangriffe, Malware ■ Sichere Konfiguration aller Cloud-Komponenten, Netzsegmentierung ■ Verschlüsselte Fernadministration ■ Verschlüsselte Kommunikation zwischen CSP und Cloud-Nutzer ■ Verschlüsselte Kommunikation zwischen Cloud-Computing-Standorten ■ Verschlüsselte Kommunikation mit Drittdienstleistern ■ Verschlüsselte Übertragung von Netzmanagement-Informationen ■ Analyse der VPN-Infrastruktur, der End-to-End-Verschlüsselungskette
Anwendungs- und Plattformsicherheit	■ Integration des Sicherheits-Managements im Software Life Cycle, Sicherheits-Gates, Vulnerability-Tests, Audits, etc. ■ Isolierung der Anwendungen, überwachte Schnittstellen ■ Automatische Überprüfung von Kunden-Anwendungen ■ Patch-und Änderungsmanagement, Kontrolle der Patch-Verträglichkeit ■ Kontrolle der Nutzung der Richtlinien zur Erstellung von sicheren Anwendungen
Informationssicherheit	■ Patch- und Änderungsmanagement ■ Lebenszyklus der Kundendaten bestimmen ■ Sichere Isolierung ■ Rollenbasierter Zugriff auf Informationen, z. B. mit LDAP ■ Regelmäßige Backup / Sicherungen (Umfang, Intervall, Speicherkonzept, Zeitpunkte und Dauer) ■ Vollständiges und zuverlässiges Löschen ■ Jede Komponente kann Ziel eines Angriffes sein und muss daraufhin untersucht und gehärtet worden sein (Ende-zu-Ende-Sicherheit).
Verschlüsselung und Schlüsselmanagement	■ Verwendung sicherer Verschlüsselungsverfahren ■ Zufällige Schlüssel mit ausreichender Länge ■ Sicherer asynchroner Schlüsselaustausch ■ Kurze Gültigkeit von Schlüsseln, sichere Aufbewahrung/ Vernichtung von Schlüsseln, z. B. mit SAML ■ Starke Authentifizierung für Cloud-Nutzer (zwei-Faktor-Authentifizierung)

Tabelle 8: Technische Maßnahmen

Organisatorische Maßnahmen

- Notfallplan
- Auswertung der Dokumentation der letzten Notfallübungen
- Sicherheitskonzept
- Periodische Sicherheitsprüfungen beim CSP und bei Subunternehmern durch zertifizierte Dritte
- Authentifizierung, Autorisierung, Administration, Audits, Awareness, Access Control
- Datenverarbeitung ausschließlich auf Weisung des Cloud-Nutzers, keinerlei Nutzung der Daten durch CSP für eigene Zwecke
- Penetrationtests beim CSP und bei Subunternehmern
- Monitoring durch den Cloud-Nutzer ermöglichen, SLA müssen überprüfbar sein.
- Logging und Monitoring von Administrationsaktivitäten
- Vier-Augen-Prinzip bei kritischen Administrationstätigkeiten
- Bereitstellung von Logdaten durch den CSP
- Information über Sicherheitsvorfälle
- 24/7 erreichbares Sicherheitsteam für Security Incident Handling und Trouble Shooting
- 24/7 Monitoring der Cloud-Dienste und unverzügliche Reaktion bei Sicherheitsvorfällen
- Umsetzung geeigneter Maßnahmen zur Verhinderung oder zumindest Erschwerung von internen Angriffen, die in der Multi-Tenant-Architektur möglich sind
- Herstellung von Transparenz und Vertrauen durch Bereitstellung ausführlicher Informationen für den Cloud-Nutzer.

Tabelle 9: Organisatorische Maßnahmen (Auswahl)

Personelle Maßnahmen

- Polizeiliches Führungszeugnis
- Bildungsweg, Qualifikationen, aktuelle und ehemalige Betriebszugehörigkeiten
- Persönliches Umfeld (Parteizugehörigkeit, etc.)
- Weiterbildung in IT-Sicherheit
- Schulung zu Social Engineering
- Kontrolle und Schulung von Awareness
- Überprüfung von externen Service Dienstleistern (Handwerker, Hausmeister etc.)
- Datenschutzverpflichtungen, Verschwiegenheitsverpflichtung

Tabelle 10: Personelle Maßnahmen (Auswahl)

6.2.2 IT-Sicherheit beim Cloud-Nutzer

Der Cloud-Nutzer muss die IT-Technik in den eigenen Räumen vor unbefugten Zugriff schützen. Dazu sind die in Tabelle 11 zusammengestellten Mindestanforderungen zu erfüllen. Bei ihrer Realisierung kann der Cloud-Nutzer vom CSP unterstützt werden.

Mindestanforderungen

- Rollenbasierte Zutrittskontrolle
- Zwei-Faktor-Authentifizierung
- Brandschutz
- Kontrolle der Service Dienstleister (Reinigung, Gebäudemanagement, Reparaturunternehmen etc.)
- Weiterbildung in IT-Sicherheit
- Schulung zu Social Engineering
- Kontrolle und Schulung von Awareness
- Notfallplan
- Auswertung der Dokumentation der letzten Notfallübungen
- Sicherheitskonzept
- Periodische Sicherheitsprüfungen

Tabelle 11: Mindestanforderungen an den Schutz der IT-Technik beim Cloud-Nutzer

6.3 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.

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 die Sicherheit mit einem Zertifikat zu bestätigen.

Hinsichtlich der Sicherheitsaspekte beim Cloud Computing können Zertifizierungen eine Orientierungshilfe für die Auswahl des Cloud Service Providers sein. Gleichwohl entbinden Zertifikate den Cloud-Anwender nicht von seiner Verantwortung.[28]

28 Der BITKOM hat seine Sicht auf die Zertifizierung in einer Stellungnahme an die EU-Kommission zusammengefasst (vgl. Anlage 4: Grundsätze der Zertifizierung aus BITKOM-Sicht)

7 Interoperabilität, Integration und Standardisierung

Die Normierung der Cloud hinsichtlich Interoperabilität und Integration ist derzeit Gegenstand politischer Initiativen auf nationaler und europäischer Ebene. Auch die Industrie und die Verbände versuchen, einheitliche Standards auf dem Markt zu etablieren. Mit Ausnahme von Webservices ws-* und der universellen Auszeichnungssprache XML haben sich bisher noch keine Standards auf breiter Linie durchgesetzt. Deshalb muss für jeden einzelnen Geschäftsprozess geklärt werden, welche Cloud Services integrierbar sind. Die im Abschnitt 7.3 formulierten Kontrollfragen unterstützen den Verantwortlichen bei der erforderlichen Prüfung der Integrationsmöglichkeit von Cloud-Service-Angeboten in die vorhandene IT-Infrastruktur.

7.1 Interoperabilität

Interoperabilität wird als »die Fähigkeit unabhängiger, heterogener Systeme (verstanden), möglichst nahtlos zusammenzuarbeiten, um Informationen auf effiziente und verwertbare Art und Weise auszutauschen bzw. dem Benutzer zur Verfügung zu stellen, ohne dass dazu gesonderte Absprachen zwischen den Systemen notwendig sind«.[29] Im Kontext von Cloud Computing können die Anforderungen an Interoperabilität weiter konkretisiert und in Form von Zielen formuliert werden:

- Vermeidung von Vendor-Lock-in durch inkompatible Formate, Protokolle und Schnittstellen
- Gewährleistung der Kompatibilität zu bestehenden und künftigen zentralen Anwendungen[30] (Cloud-Services)
- Kompatibilität zu Client-Systemen und lokalen On-Premise-Anwendungen.

In Abhängigkeit von der Service-Ebene[31] ergeben sich für den Cloud-Nutzer unterschiedliche Anforderungen an die Interoperabilität (vgl. Tabelle 12).

Service-Ebene	Anforderungen an die Interoperabilität
IaaS	Als neuer Standard für das Ressourcen-Management von VM bildet sich momentan das Open Cloud Computing Interface (OCCI) heraus. Die Verwaltung der Speicherressourcen und deren Funktion münden in den Standard Cloud Data Management Interface (CDMI). Einschränkend ist festzuhalten, dass die genannten Standards noch nicht allgemein akzeptiert sind.
PaaS	Für die Middleware-Technologie PaaS werden in erster Linie nicht-Cloud-spezifische Standards wie HTTP, REST, SSL etc. für die Kommunikation zum Frontend und SOAP, ws-* und XML für die Anbindung von weiteren Cloud-Diensten verwendet. Die Durchsetzung spezieller Cloud-Standards zeichnet sich hier nicht ab.
SaaS	Bei SaaS findet die (fachliche) Interoperabilität auf unterschiedlichen Ebenen statt, die sich über Dateiformate (z. B. XML, TXT oder CSV), Semantik (z. B. XBRL, FerD), oder Anwendungsfunktionen (z. B. Sicherung/Abzug aller Daten) erstrecken.

Tabelle 12: Anforderungen der Cloud-Nutzer an die Interoperabilität nach Service-Ebenen

29 Quelle: Wikipedia
30 auch als Cloud-to-Cloud-Interoperabilität oder Inter-Cloud-Interoperabilität bezeichnet
31 Vgl. dazu Anlage 1

7.2 Standards

Standards sind für das Zusammenwirken unterschiedlicher Systeme von essenzieller Bedeutung. Nur auf der Basis von Standards können integrierte Lösungen in einer immer komplexer werdenden IT-Landschaft mit geringem Aufwand und ohne Reibungsverluste geschaffen werden. Voraussetzung ist, dass die Standards eine offene Struktur aufzeigen und von allen Beteiligten implementiert werden können. Standards werden in der Regel durch ein Gremium mit entsprechender Autorität festgelegt, es bilden sich aber auch Defakto-Standards, bedingt durch entsprechende Verbreitung oder Marktdominanz von Unternehmen oder Lösungen.

Da Cloud Computing ein relativ neues Phänomen ist, bilden sich Cloud-spezifische Standards für die Interoperabilität gerade erst heraus.[32] Aus Sicht des Cloud-Nutzers sind gerade technische Cloud-Standards nicht leicht zu bewerten.

Die ausgereiftesten und verbreitetsten Spezifikationen bzw. Standards sind mit Blick auf die Cloud-Interoperabilität:

- Webservices ws-*
- XML-Dateiformate.

Für Cloud-Anwender, die insbesondere ein internationales Geschäftsumfeld bedienen, ist es sinnvoll darauf zu achten, ob Cloud Service Provider ihre IT-Infrastruktur auf bestimmte Standardisierungen hin ausrichten[33] und so zumindest eine »Grundausstattung« beispielsweise an definierten Schnittstellen bieten.

7.3 Handlungsempfehlung und Kontrollfragen

Die technischen Standards zur Interoperabilität hängen der rasanten Entwicklung des Cloud Computings hinterher. Cloud-Standards, Interoperabilität und die Vermeidung von Vendor Lock-in sind Gegenstand politischer Aktivitäten auf nationaler und EU-Ebene[34]. Da entsprechende Zertifikate – wie auch Kriterien zu ihrer Erteilung – noch nicht zur Verfügung stehen und auch nicht kurzfristig zu erwarten sind, müssen sich Cloud-Nutzer bei ihren Entscheidungen zurzeit anders orientieren.

So empfiehlt es sich momentan, die Anforderungen an ein Cloud-System hinsichtlich Interoperabilität und Vermeidung von Vendor Lock-in von der vorhandenen Unternehmens-IT abhängig zu machen. Denkbar ist eine Prozessanalyse, welche Daten aus welchen Systemen in die Cloud-Anwendungen integriert werden sollen und umgekehrt. Basierend auf diesen Ergebnissen sollte die IT-Abteilung Aussagen zur technischen Umsetzung und Implementierung treffen. Dies kann nur im Zusammenwirken der Prozessverantwortlichen mit dem lokalen IT-Verantwortlichen sowie den Cloud Service Providern erfolgen.

Kontrollfragen

Die in Tabelle 13 formulierten Kontrollfragen sollen den Prozessverantwortlichen dabei unterstützen, die notwendigen Antworten von der IT-Abteilung zu erhalten, um die Nutzung von Cloud-Services zu bewerten. Sie dienen der Abschätzung, inwieweit sich ein Cloud-Angebot hinsichtlich der Interoperabilität zur Abbildung von Unternehmensprozessen eignet. Neben der Angabe von technischen Standards können die Antworten aber auch in Nutzungsvereinbarungen, Verträgen oder AGB liegen.

32 Vgl. [BCFZI, 2012]

33 Weltweit gibt es rund 150 Organisationen, die sich mit Aspekten der Standardisierung im Cloud Computing befassen. Davon ist derzeit nur ein kleiner Teil relevant (vgl. [BCFZI, 2012]).

34 Der BITKOM unterstreicht die Bedeutung der Standardisierung für die Förderung von Interoperabilität (zwischen verschiedenen Clouds sowie zwischen Cloud-Applikationen und traditionellen IT-Systemen), für Datenportabilität und zur Definition von Datenschutz- und Sicherheitsniveaus. Der Verband begrüßte in dem Zusammenhang die Berufung eines Steering Boards für die European Cloud Partnership (ECP). Der BITKOM erwartet, dass weitere Standardisierungsvorhaben im Cloud Computing einen bedeutenden Einfluss auf den europäischen Cloud-Markt ausüben werden und ist daher bereit, die Steuerungsgruppe bei seiner Arbeit zu unterstützen (vgl. [BSTCS, 2012]).

Kontrollfragen

- Ist es möglich, die Daten lokal zu speichern bzw. sichern und in welchem Format liegen sie dann vor?
- Welcher Aufwand und welche Kosten entstehen bei der Anfertigung von Sicherheitskopien aller Daten (Abzug)?
- Der Nutzer betreibt lokal installierte Anwendungen wie z. B. CRM, Mailsystem, Warenwirtschaftsprogramm etc. Können die Daten dieser Anwendungen in der Cloud verarbeitet werden und welche Prozesse/Schritte sind einmalig oder laufend dazu notwendig?
- Der Kunde nutzt Internet-basierte Anwendungen wie z. B. CRM, Mailsystem, Warenwirtschaftsprogramm etc. Können die Daten dieser Anwendungen in der neuen Cloud-Anwendung verarbeitet werden und welche Prozesse/Schritte sind einmalig oder kontinuierlich dazu notwendig?

Tabelle 13: Kontrollfragen zur Abschätzung, inwieweit sich ein Cloud-Angebot hinsichtlich der Interoperabilität eignet

8 Fazit

In der Nutzung von Cloud Computing sehen Experten große Vorteile. Dies gilt nicht nur für Großunternehmen, sondern insbesondere für den Mittelstand. Während Konzerne selbst über Kapital und Kompetenz für Beschaffung und Betrieb eigener IT verfügen, profitieren vor allem Mittelständler von den Cloud-Services. Diese Services werden in ständig wachsender Anzahl und vielfältigeren Formen angeboten.

»Mundgerechte« Angebote werden die eher einfachen, stark standardisierten Lösungen sein, bei denen der Schwerpunkt auf dem Kostenvorteil liegt. Lösungen, mit denen vertrauliche sowie personenbezogene Daten verarbeitet oder mit denen strategische Unternehmenskonzepte umgesetzt werden sollen, bedürfen dagegen eher einer umfangreicheren Vorbereitung und externer Beratung.

Dementsprechend können die im vorliegenden Leitfaden aufgeführten Listen, Hinweise und Erläuterungen bei der Abschätzung helfen, ob und wie angedachte Cloud-Lösungen risikoarm und ohne besondere Zusatzmaßnahmen erfolgreich eingeführt werden können. Gleichzeitig sind die potenziellen Anbieter identifizierbar.

Ergeben sich bei der ersten Prüfung jedoch komplexere Fragestellungen, so können anhand dieses Leitfadens die Möglichkeiten des Einsatzes von Cloud-Computing-Lösungen intensiver mit qualifizierten Beratern erörtert und bewertet werden – wie auch bei der Einführung komplexer Software. Bestehende bzw. vermeintliche Risiken beim Einsatz von Cloud Computing werden dabei aufgezeigt oder ausgeräumt. Wer Cloud Computing grundsätzlich ablehnt oder unberücksichtigt lässt, verzichtet auf vielfältige Möglichkeiten zur Steigerung der Wettbewerbsfähigkeit.

9 Anlagen

9.1 Anlage 1: Service-Ebenen im Cloud Computing und Cloud-Organisationsformen[35]

Die Einteilung der Services in die drei Service-Ebenen

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

hat sich weitgehend durchgesetzt (vgl. Tabelle 14).

Allen drei Ebenen ist gemeinsam, dass die IT-Leistungen als Dienste (»as a Service«) bereitgestellt werden.

Service-Ebenen	
IaaS	IaaS ist im Rahmen von Cloud Computing die Bereitstellung einer skalierbaren IT-Infrastruktur auf nicht eindeutig zugeordneten IT-Ressourcen über Netzwerk. Dieses Geschäftsmodell sieht eine Nutzung von Rechnerinfrastruktur nach Bedarf vor und bildet einen Gegenentwurf zum klassischen Erwerb. Die IT-Leistungen der Basisinfrastruktur stellen das Tätigkeitsfeld der Spezialisten für den IT-Betrieb sowie der IT-Dienstleister dar. Auf technologischer Ebene wird hier im Wesentlichen wenig veredelte Rechen- und Speicherleistung auf virtualisierten Servern sowie Netzwerkinfrastruktur-Funktionalität mit hohem Standardisierungsgrad und intelligentem System-Management als Service bereitgestellt.
PaaS	PaaS ist im Rahmen von Cloud Computing die Bereitstellung von gemeinsam nutzbaren Laufzeit- oder Entwicklungsplattformen auf nicht eindeutig zugeordneten IT-Ressourcen über Netzwerk. Dieses Geschäftsmodell stellt eine integrierte Laufzeit- und ggf. auch Entwicklungsumgebung als Dienst zur Verfügung, der dem Anwender gegenüber nach Nutzung abgerechnet wird. Mit den Cloud-Services der Ebene PaaS befassen sich System-Architekten und Anwendungsentwickler. PaaS beschreibt Services auf der Anwendungs-Infrastruktur-Ebene (Datenbanken, -Integration und Security), die auf Basis von technischen Frameworks, also Entwicklungs-Plattformen, angeboten werden. Mit ihnen lassen sich Anwendungskomponenten entwickeln und Plattform übergreifend integrieren.
SaaS	SaaS ist im Rahmen von Cloud Computing die Bereitstellung von gemeinsam nutzbarer Software auf nicht eindeutig zugeordneten IT-Ressourcen über Netzwerk. Unter SaaS versteht man ein Geschäftsmodell mit der Philosophie, Software als laufende Leistung basierend auf Internettechniken bereitzustellen, zu betreuen und zu betreiben, die in der Regel pro Aufruf abgerechnet wird und die Software nicht länger als Lizenz an einen Nutzer zu verkaufen. SaaS richtet sich an Anwender. Geschäftsanwendungen werden als standardisierte Services von einem Dienstleister bereitgestellt. Dabei sind ihre Anpassungs- und Integrationsmöglichkeiten oft eingeschränkt. Desktop-, Kollaborations- und Kommunikations-Anwendungen sowie industriespezifische Geschäftsabläufe, die vollständig von der Technologie abstrahiert sind, fallen in diesen Bereich.
BPaaS	Zusätzlich wird aktuell eine vierte Ebene diskutiert, die als (Business) Process as a Service gekennzeichnet wird. Sie geht aus der SaaS-Ebene hervor und wird durch eine stärkere Nähe zum Geschäftsprozess charakterisiert.

Tabelle 14: Service-Ebenen im Cloud Computing

35 Vgl. [CC-WEWM, 2010]

Der »Stammbaum« von Cloud Computing gründet sich auf zwei Urformen:

- die Public und
- die Private Cloud.

Die anderen Ausprägungen sind Derivate, Kombinationen oder Speziallösungen dieser Urformen.

Analysiert man den derzeitigen Stand der Cloud-Diskussion, dann lassen sich die verschiedenen Cloud-Typen grob über zwei Dimensionen definieren,

- eine organisatorische und
- eine Sourcing-Dimension.

Allen Cloud-Typen ist prinzipiell gemeinsam, dass sie über die Cloud-typischen Eigenschaften und über drei, für den Endkunden »nutzbare« Service-Ebenen verfügen (vgl. Tabelle 15):

Organisationsform	Erläuterung
Public Cloud/ External Cloud	■ Beschreibung: Sie stellt eine Auswahl von hochstandardisierten skalierbaren Geschäftsprozessen, Anwendungen und/oder Infrastruktur-Services auf einer variablen »pay per use«-Basis grundsätzlich für jedermann gleichzeitig (Multimandantenfähigkeit) zur Verfügung. Die Nutzer sind organisatorisch nicht verbunden. Die Public Cloud zielt auf Skaleneffekte und Consumerisation of IT. Die Nutzer teilen sich die zugrunde liegende Infrastruktur. Eine Lokalisierung der Ressourcen ist in der Regel nicht gegeben. Eigentümer und Betreiber einer Public Cloud ist meist ein IT-Dienstleister. ■ Zugriff: Mittels Browser über das Internet auf IaaS-, PaaS- und SaaS-Services ■ Service Level Agreements: Standard (in der Regel nicht individuell anpassbar) ■ Sourcing Optionen: outsourced
Virtual Private Cloud	■ Beschreibung: Ist ein Spezialfall der Public Cloud. In einer Virtual Private Cloud wird dem Nutzer eine durch geeignete Sicherheitsmechanismen abgeschottete und individualisierte IT-Umgebung zur Verfügung gestellt. In der Virtual Private Cloud kann der Nutzer damit über eine quasi-individuelle Betriebsumgebung verfügen, die über ein Virtual Private Network (VPN) mit seiner IT verbunden ist. ■ Zugriff: Mittels Browser über Intranet (sichere VPN-Verbindung) auf IaaS-, PaaS- und SaaS-Services. ■ Service Level Agreements: in Grenzen individuell anpassbar ■ Sourcing Optionen: outsourced
Hybrid Cloud	■ Beschreibung: Eine Hybrid Cloud ist kein eigener Cloud-Typ, sondern bezeichnet Szenarien für jede Art von Kopplung zwischen traditioneller IT, Private Clouds und Public Clouds. Die Gesamtverantwortung verbleibt beim Kunden, die IT-Betriebsverantwortung wird geteilt: Sie liegt beim jeweiligen IT-Betriebsverantwortlichen. Die Herausforderung dieses Modells liegt in der Security- und Service-Integration der verschiedenen Cloud-Typen. ■ Zugriff: Für den Teil der Private Cloud: Sicherer Zugang mittels VPN; nur für den Kunden selbst, autorisierte Geschäftspartner, Kunden und Lieferanten. Für den Teil der Public Cloud: Mittels Browser über das Internet oder via VPN bei einer Virtual Private Cloud. ■ Service Level Agreements: Kombination aus individuell (Private Cloud) und Standard (Public Cloud) ■ Sourcing Optionen: Der Teil der Private Cloud kann vom Kunden selbst oder von einem Dienstleister (der i. d. R. nicht gleichzeitig Provider der Public Cloud ist) betrieben werden. Damit sind prinzipiell alle Sourcing-Optionen möglich. Der Teil der Public Cloud ist outsourced.
Private Cloud/ Internal Cloud	■ Beschreibung: Private Cloud bezeichnet die Bereitstellung von Cloud-Computing-Leistungen nur für vorab definierte Nutzer. Private Clouds sind nicht öffentlich. Management und Betrieb werden innerhalb eines Unternehmens oder einer gemeinsamen Organisation abgewickelt. Der Zugang ist beschränkt auf von dem Betreiber autorisierte Personen und erfolgt in der Regel über ein Intranet beziehungsweise ein Virtual Private Network (VPN). Private Clouds bieten also eine nach Cloud-Design-Kriterien erstellte effiziente, standardisierte, virtualisierte und sichere IT-Betriebsumgebung unter Kontrolle des Kunden (innerhalb der Kunden-Firewall). Private Clouds erlauben individuelle Anpassungen und können z. B. die Sicherheits- und Compliance-Nachteile von Public Clouds kompensieren, erreichen aber nicht deren Skaleneffekte. ■ Zugriff: Sicherer Zugang mittels VPN auf alle drei Service-Ebenen für einen eingeschränkten Nutzerkreis: i. d. R. nur für den Eigentümer der Private Cloud selbst, autorisierte Geschäftspartner, Kunden und Lieferanten ■ Service Level Agreements: kundenspezifisch frei definierbar ■ Sourcing Optionen: Private Clouds werden i. d. R. vom Kunden selbst oder nach seinen Vorgaben von einem externen Dienstleister betrieben. Damit sind für Private Clouds alle Sourcing-Optionen möglich.

Tabelle 15: Vergleich wichtiger Organisationsformen von Clouds

9.2 Anlage 2: Datenschutz – die rechtliche Ausgangssituation

International: Je nach Land genießt der Datenschutz weltweit einen sehr unterschiedlichen Status. Teils hat er, wie z. B. in Japan, Verfassungsrang, teils werden staatlichen Stellen sehr weitgehende Zugriffsrechte auf persönliche Daten eingeräumt, so z. B. in China. Vor diesem Hintergrund hat die OECD 1980 Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data erlassen. Durch die Guidelines, die empfehlenden Charakter haben, sollen die mitgliedstaatlichen Datenschutzbestimmungen harmonisiert werden. Die seit 1981 bestehende Europäische Datenschutzkonvention des Europarats ist demgegenüber in Deutschland geltendes Recht.

In der EU ist der Datenschutz in Artikel 8 der Grundrechte Charta verankert und insbesondere in Richtlinie 95/46/EG geregelt. Die Richtlinie fordert die Einhaltung bestimmter Anforderungen, um ausreichende Sicherheiten zu gewährleisten, wenn personenbezogene Daten aus Mitgliedsstaaten der EU in Länder mit einem geringeren Datenschutzniveau übermittelt werden.

In Deutschland wird der Datenschutz in mehr als 200 Gesetzen und Verordnungen geregelt, darunter insbesondere das Bundesdatenschutzgesetz und 16 Landesdatenschutzgesetze. Darüber hinaus entwickelte das Bundesverfassungsgericht im Jahr 2008 ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Es dient primär dem Schutz persönlicher Daten in IT-Systemen. Der Zugriff von Behörden auf personenbezogene Daten unterliegt einem Richtervorbehalt und ist auf wenige Ausnahmetatbestände beschränkt.

In den USA gibt es keine umfassenden gesetzlichen Regelungen zum Datenschutz. Ausnahmen bilden v.a. der Datenschutz von Kindern im Internet (COPPA) und gesundheitsbezogene Daten (HIPAA). Eine rein datenschutzrechtliche Aufsicht existiert nicht. Für die Durchsetzung verschiedener Datenschutzgesetze mit Verbraucherbezug ist die Federal Trade Commission (FTC) zuständig. Nach dem USA Patriot Act haben US-Behörden die Möglichkeit, von Unternehmen, die in den USA tätig sind, unter bestimmten Voraussetzungen die Herausgabe personenbezogener Informationen zu verlangen. Eine Anforderung ist erlaubt, wenn sie

- auf Grundlage einer gerichtlichen Anordnung oder eines National Security Letter basiert und
- die betroffene Information im Besitz, Aufbewahrung oder Kontrolle eines in den USA tätigen Rechtsträgers ist.

Ein Datenaustausch zwischen EU-Ländern und den USA ist trotz der unterschiedlichen Datenschutzregeln auf Basis des Safe Harbor Agreements möglich. Unternehmen, die diesem Abkommen beitreten, verpflichten sich damit, bestimmte datenschutzrechtliche Bestimmungen zu beachten. Damit wird auch von der EU grundsätzlich anerkannt, dass die entsprechenden Unternehmen unabhängig von der unterschiedlichen Rechtslage in den USA und der EU einen ausreichenden Datenschutz praktizieren.

9.3 Anlage 3: Staatliche Zugriffe auf Cloud-Daten

Cloud Computing bietet, verglichen mit den bisherigen Modellen dezentraler IT-Versorgung, enorme Vorteile nicht nur hinsichtlich der Leistungsfähigkeit und der Effizienz von IT-Systemen. Auch in Fragen der Datensicherheit sind Cloud-Lösungen den bisherigen in aller Regel weit überlegen.
Dennoch bestehen bei Kunden, in Politik und Öffentlichkeit oft grundsätzliche Bedenken hinsichtlich des Schutzes der an einen Cloud-Dienstleister übergebenen Daten. International tätige Anbieter von Cloud-Diensten sehen sich ihrerseits mit der Herausforderung konfrontiert, die an ihren jeweiligen Standorten geltenden, meist unterschiedlichen, teils sogar gegenläufigen rechtlichen Vorschriften zu erfüllen.

Zwar existieren in den meisten Staaten der Welt Zugriffsrechte auf Cloud-Daten und ein Vergleich europäischer und nordamerikanischer Staaten zeigt deutlich, dass

sowohl europäische als auch nordamerikanische Staaten unter bestimmten Voraussetzungen Zugriff auf Daten ausüben können[36].
Die aktuelle Diskussion entzündet sich aber insbesondere an den in den USA geltenden Vorschriften (USA Patriot Act[37]), die US-Behörden unter bestimmten Voraussetzungen auch dann Zugriff auf Daten geben sollen, wenn sie außerhalb der USA erhoben und gespeichert werden.

Der Patriot Act wird in diesem Zusammenhang häufig mit Cloud Computing-Produkten von Anbietern mit amerikanischen Mutterkonzernen in Verbindung gebracht. Es wird argumentiert, dass aufgrund des Patriot Acts die in ihren Systemen gespeicherten Daten US-amerikanischen Ermittlungsbehörden ohne größere Hürden zur Verfügung gestellt und jegliche europäischen Datenschutzverpflichtungen missachtet werden könnten.

Eine Studie, die u.a. das Centre for European Policy Studies (CEPS) im Oktober 2012 für den Innenausschuss des Europaparlaments erstellt hat, kritisiert in diesem Zusammenhang die Zugriffsmöglichkeiten der US-Behörden nach dem FISA-Amendment Act 2008. Die Studie fordert, dass solche Zugriffe durch internationale Verträge geregelt werden[38]. Diese Kritik zeigt, dass die EU-Kommission und die US-Regierung ihre Bemühungen um ein entsprechendes Abkommen vorantreiben sollten. Es ist daher Aufgabe der Politik, an einer supranationalen Anpassung der Rechtsrahmen zu arbeiten und so Rechtssicherheit herzustellen. Denn nicht nur für Cloud-Anbieter, sondern für alle datenverarbeitenden Unternehmen, die auf beiden Seiten des Atlantiks aktiv sind, stellen gegenläufige rechtliche Verpflichtungen aus der amerikanischen und der europäischen Rechtsordnung eine Rechtsunsicherheit dar. Dies gilt insbesondere auch vor dem Hintergrund, dass bei länderübergreifenden Ermittlungen zu Straftaten die Regierungen bereits jetzt regelmäßig in Amtshilfeverfahren zusammenarbeiten[39].

Mehr noch als für die Rechtsräume der EU und der USA bedarf es einer Verbesserung der Rechtssicherheit für Länder, die nicht von dem Safe Harbor Agreement oder der einschlägigen OECD-Richtlinie erfasst werden.
Debatten auf Basis ungenauer Informationen und fehlende Rechtssicherheit halten verunsicherte Unternehmen davon ab, die Möglichkeiten des Cloud Computings einzusetzen. Dies führt dazu, dass einerseits die positiven gesamtwirtschaftlichen und gesellschaftlichen Potenziale von Cloud Computing zur Steigerung ihrer Wettbewerbsfähigkeit nur verlangsamt oder nicht in vollem Umfang gesehen werden.

Andererseits wird der Fokus auf die reale Gefahrenlage verzerrt. Die größte Gefahr für Datenmissbrauch geht nicht von nach jeweils geltendem Recht legalen Zugriffen von Sicherheitsbehörden, sondern von nicht-staatlichen Akteuren aus. Das Hauptaugenmerk für die Sicherheit und den Schutz von Daten sollte daher auf die Abwehr dieser Angriffe gelegt werden. Wesentliche Herausforderungen sind deshalb

- die Abwehr nicht-legitimierter Angriffe nicht-staatlicher Akteure (Organisierte Kriminalität, kriminelle Einzelpersonen) wie auch
- die Abwehr staatlich unterstützter oder tolerierter Angriffe zum Zwecke der Wirtschaftsspionage oder eines Cyberwars.

36 »Governmental access to data stored in the Cloud – including cross-border access – exists in every jurisdiction« (vgl. [Maxw, 2012]) In diesem White Paper vergleichen die Autoren das Wesen und das Ausmaß staatlicher Zugriffe auf Cloud-Daten in vielen Ländern der Welt.

37 USA PATRIOT Act – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001: Der Patriot Act ist ein amerikanisches Bundesgesetz, das am 25. Oktober 2001 vom Kongress als direkte Reaktion auf die Terroranschläge am 11. September 2001 verabschiedet wurde. Er dient der Bekämpfung des Terrorismus und der Spionageabwehr und enthält den Erlaubnistatbestand, dass die amerikanische Regierung in begründeten Verdachtsfällen Informationen über Tatverdächtige von in den USA tätigen Unternehmen anfordern darf (vgl. S. 38). Dies gilt also zunächst für alle Firmen, die in den USA geschäftlich tätig sind, gleich ob es sich um eine amerikanische oder ausländische Firma handelt.

38 http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050, S. 35.

39 1.) Vertrag zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen vom 14. Oktober 2003
2.) Zusatzvertrag zum Vertrag zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen vom 18. April 2006.
3.) Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität vom 1. Oktober 2008, am 19. April 2011 in Kraft getreten (aber über die praktische Anwendung wird noch mit den USA verhandelt, bisher offenbar noch kein Datenaustausch).

9.4 Anlage 4: Grundsätze der Zertifizierung aus BITKOM-Sicht

- BITKOM regt an[40], Erleichterungen für die Wahrnehmung der Weisungs- und Kontrollbefugnisse des Cloud-Kunden bei Inanspruchnahme von Cloud-Diensten zu schaffen – durch Förderung von Selbstverpflichtungen[41] und Verhaltenskodizes sowie deren Anerkennung als Nachweis zur Erfüllung der Sorgfalts- und Kontrollpflichten des Cloud-Kunden.
  Es sollten freiwillige Zertifikate mit einheitlichen und transparenten Prüfverfahren durch sachverständige Dritte als Nachweis der Erfüllung der Kontrollpflichten des für die Datenverarbeitung Verantwortlichen etabliert werden.
  Schließlich sind die Anforderungen an die Datensicherheit im Rahmen von Cloud-Dienstleistungen weiter zu entwickeln und entsprechende Rahmen für Zertifizierungen zu setzen.

- Cloud-Kunden, die personenbezogene und andere schützenswerte Daten in die Cloud geben, tragen die Verantwortung, dass diese entsprechend deren unterschiedlich ausgeprägten Schutzbedarf angemessen geschützt werden. Um dieser Verantwortung gerecht zu werden, müssen Cloud-Kunden ihre Dienstleister sorgfältig aussuchen und überprüfen. Für die Auswahl brauchen sie Angaben, anhand derer sie die Eignung eines Anbieters für ihre Datenverarbeitungszwecke erkennen können. Was die Kontrollpflichten angeht, so sind sie für den Cloud-Kunden oftmals nicht umfassend selbst zu bewältigen, da es einer Cloud-Infrastruktur immanent ist, dass sie gerade nicht an bestimmte Orte gebunden ist.

- Ein guter Ansatz für mehr Transparenz und Unterstützung der Cloud-Kunden bei ihren Kontrollpflichten ist ein abgestimmtes System von qualitativ vergleichbaren Arten von Nachweisen, wie z. B. Selbstverpflichtungen, branchenspezifische Verhaltenskodizes und Zertifizierungen, die imstande sind, die Konformität der Datenverarbeitung mit den gesetzlichen Vorschriften – und den besonderen Anforderungen des jeweiligen Unternehmens oder bestimmter Branchen – festzustellen und gegenüber den Betroffenen zu bezeugen.[42]

- Mit der Anerkennung der Vorlage von Selbstverpflichtungen als Nachweis für die Erfüllung der Kontrollpflichten des für die Verarbeitung Verantwortlichen werden Vor-Ort-Kontrollen vermieden.

- Es wird Konstellationen geben, in denen ein Bedarf des Anbieters oder des Kunden nach einem besonderen Nachweis für die Einhaltung der Datenschutzvorschriften bzw. besonderer Vorkehrungen für ein hohes Datenschutz- und Datensicherheit-Niveau besteht. Hierfür müssen entsprechende Nachweise in Form von Zertifizierungen gefördert und anerkannt werden.

- Um dieser Zielsetzung gerecht zu werden, sollte die Zertifizierung eine angemessene Prüftiefe und -weite aufweisen. Der Bedarf des einzelnen Cloud-Kunden oder Nutzers ist – abhängig von seinem Kontext – sehr unterschiedlich. »Allgemeine« Zertifikate würden daher eher verwirren als nutzen. Deshalb ist es unentbehrlich, einen allgemeingültigen Rahmen der Zertifizierung zu erarbeiten und innerhalb dieses Rahmens die branchenspezifischen Anforderungen zu ermitteln, die dann für die Zertifizierung geprüft würden.

- Zertifizierungsmöglichkeiten sollten einem einheitlichen, objektiven Standard folgen, der eine Vergleichbarkeit der Anbieter und ihrer Datenschutzmaßnahmen ermöglicht. Die Prüfkriterien für die Erteilung des Testats sind auf gesetzlicher Grundlage für den europäischen Binnenmarkt einheitlich festzusetzen. Die Festlegung der Prüfkriterien sollte durch ein Verfahren erfolgen, in dem Datenschutzbehörden

40 Vgl. [BSTCS, 2012]
41 Selbstverpflichtungen auf Community- und Verbandsebene sind individuellen Selbstverpflichtungen von Unternehmen vorzuziehen.
42 Damit würde die Ausübung des Selbstbestimmungsrechts durch den Betroffenen und die Verantwortungsübernahme durch die verantwortlichen Stellen optimal unterstützt.

sowie Vertreter von Anbietern und Nutzern der Auftragsdatenverarbeitung beteiligt werden.[43] Dabei sind Möglichkeiten zu schaffen, welche die Schutzbedürftigkeit der Daten berücksichtigen.[44] Das Testat sollte durch qualifizierte private Stellen vergeben werden. Die Eignung der testierenden Stelle sollte durch eine Akkreditierung nachgewiesen werden. Die testierende Stelle sollte für fehlerhafte Testate haften.[45] Bei der Spezifizierung von Zertifizierungen sind neben den notwendigen Mindest-Qualitätsstandards auch die Kosten-Nutzen-Aspekte für Cloud-Provider zu betrachten.

- Neben dem Datenschutz gibt es noch eine Reihe weiterer Themen, bei denen es sinnvoll ist, Anbietern die Möglichkeit zu geben, für ihren Dienst die rechtliche Eignung selbst zu erklären. Ergänzend zu den datenschutzrechtlichen Selbstverpflichtungen kann eine Selbsterklärung Aussagen zu Compliance mit nationalen Rechtsordnungen, Interoperabilität, Datenportabilität und zur Servicequalität enthalten und somit redundante Zertifikate und den damit verbundenen Zertifizierungsaufwand ersetzen.

- Bei der Zertifizierung ist es wichtig, dass Normen und Zertifizierungen sich an bereits bestehende und allgemein in der Branche akzeptierte Ansätze wie z. B. ISO 27001 anlehnen, die um essenzielle Cloud-Spezifika ergänzt werden. Dies schafft einen erheblichen Geschwindigkeitsvorteil und vermeidet gleichzeitig wettbewerbsrelevante Mehrkosten durch neue Zertifizierungen.

43 Vgl.: http://www.trusted-cloud.de/documents/Thesenpapier_Datenschutz.pdf

44 z. B. müssen medizinische Daten oder Daten, die einem Berufsgeheimnis unterliegen, durch höherwertige Schutzmaßnahmen abgesichert werden als Adressdaten eines Onlinegewinnspiels.

45 Vgl.: http://www.trusted-cloud.de/documents/Thesenpapier_Datenschutz.pdf

10 Quellen

[BCFZI, 2012] Booz & Company und FZI: Das Normungs- und Standardisierungsumfeld von Cloud Computing – Eine Untersuchung aus europäischer und deutscher Sicht unter Einbeziehung des Technologieprogramms »Trusted Cloud«. Studie für das Bundesministerium für Wirtschaft und Technologie (BMWi), Abschlussbericht, Januar 2012, http://www.bmwi.de/DE/Mediathek/publikationen,did=476730.html

[BPO, 2005] »Business Process Outsourcing – BPO als Chance für den Standort Deutschland«, Leitfaden, BITKOM 2005. http://www.bitkom.org/files/documents/BITKOM_Leitfaden_BPO_Stand_20.09.05.pdf

[BSI, 2010] »Sicherheitsempfehlungen für Cloud Computing Anbieter – Mindestanforderungen in der Informationssicherheit«, Eckpunktepapier, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2010, https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html

[BSTCS, 2012] Stellungnahme des BITKOM zur Cloud-Strategie der Europäischen Kommission, Berlin, 27.12.2012

[CC-ETRB, 2009] »Cloud Computing – Evolution in der Technik, Revolution im Business«, Leitfaden, BITKOM 2009, http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf

[CC-WEWM, 2010] Cloud Computing – Was Entscheider wissen müssen. Ein ganzheitlicher Blick über die Technik hinaus: Positionierung, Vertragsrecht, Datenschutz, Informationssicherheit, Compliance, Leitfaden, BITKOM 2010, http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Cloud_Computing-Was_Entscheider_wissen_muessen.pdf

[CITOP, 2007] Compliance in IT-Outsourcing- Projekten. Leitfaden zur Umsetzung rechtlicher Rahmenbedingungen. BITKOM 2007. http://www.bitkom.org/files/documents/BITKOM-Leitfaden_Compliance.pdf

[EAM, 2011] Enterprise Architecture Management – neue Disziplin für die ganzheitliche Unternehmensentwicklung. Leitfaden, BITKOM 2011, http://www.bitkom.org/files/documents/EAM_Enterprise_Architecture_Management_-_BITKOM_Leitfaden.pdf

[Forr, 2009] Forrest, William (March 2009): »Clearing the air on cloud computing«, McKinsey, vgl.: http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/McKinsey_Cloud%20matters.pdf

[IDG 2010] With a Push from Cloud Computing, IT Shifts toward Supply Chain Model, Survey by IDG Research, October 2010 – im Auftrag von CA

[KDOCC, 2011] Konferenz der Datenschutzbeauftragten, Orientierungshilfe Cloud Computing, http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

[KPMG, 2013] »Cloud-Monitor 2012. Eine Studie von KPMG in Zusammenarbeit mit BITKOM – durchgeführt von PAC«, März 2013

[Maxw, 2012] Maxwell, Winston; Wolf, Christopher: A Global Reality: Governmental Access to Data in the Cloud. A comparative analysis of ten international jurisdictions. A Hogan LovellsWhite Paper, 23 May 2012, vgl.: http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20%281%29.pdf

[MDM, 2011] The Practical Value of MDM. A DataFlux White Paper, 2011. http://www.information-management.com/media/pdfs/PracticalValue_MDM.pdf

[PBS, 2012] Pankaj, A., Biyani, R., Salil, D., Cloud Powering an Enterprise, McGraw-Hill 2012

[Phi, 2012] Phifer, Gene; Heiser, Jay: Look Before You Leap Into Cloud Computing. Gartner, Published: 25 May 2012. http://www.gartner.com/id=2027315

[PSITO, 2006] »Public Sector: IT-Outsourcing/Public Private Partnership. Erfahrungen mit Risikopartnerschaften bei der IT-gestützten Modernisierung der öffentlichen Verwaltung«, Leitfaden, BITKOM 2006. http://www.bitkom.org/files/documents/PPP_ITO_E-Government_fin.pdf

[RAOP, 2008] »Rechtliche Aspekte von Outsourcing in der Praxis«, Leitfaden, BITKOM 2008. http://www.bitkom.org/files/documents/BITKOM_Publikation_Outsourcing-V.1.0_2008.pdf

[Shr, 2011] Shroff, G., Enterprise Cloud Computing, Cambridge University Press 2010

[SOAC, 2013] Softwareorientierte Architekturen in der Cloud. Leitfaden des BITKOM, 2013, http://www.soa-know-how.de/soa-in-der-cloud

[Stadt, 2012] Stadtmueller, Lynda: »Tips for Choosing a Cloud Service Provider«, Stratecast | Frost & Sullivan, March 2012

[tc, 2012] »Cloud-Einsatzgrad hat sich binnen eines Jahres nahezu verdoppelt«, IT-Cloud-Index Mittelstand Q4/2012 von techconsult und HP Deutschland, http://www.it-cloud-index.de/

[TFEAM] A Comparison of the Top Four Enterprise-Architecture Methodologies, Roger Sessions, ObjectWatch, Inc., http://msdn.microsoft.com/en-us/library/bb466232(d=printer).aspx

[TOGAF] TOGAF™ – Das Enterprise Architekture Framework der Open Group, Version 9 (www.opengroup.org/togaf)

[TT, 2012] »Sichere Nutzung von Cloud-Anwendungen am Beispiel des TeleTrusT – Bundesverband IT-Sicherheit e.V. als Praxisleitfaden für Verbände und KMU«, Publikation von TeleTrusT – Bundesverband IT-Sicherheit e.V., Mai 2012, http://www.teletrust.de/uploads/media/2012-TeleTrusT_Cloud_Computing.pdf

[Will, 2012] Williams, B, The Economics of Cloud Computing, Cisco Press, 2012

11 Autoren

- Arnd Böken,
  Graf von Westphalen Rechtsanwälte Partnerschaft
- Benjamin Brake, IBM Deutschland GmbH
- Susanne Dehmel, BITKOM e.V.
- Vincent James, Microsoft Deutschland GmbH
- Dieter Krißgau, Datev eG
- Claudia Mrotzek, Oracle Deutschland B.V. & Co. KG
- Dr. René Niebuhr, Comitando Management Beratung
- Dr. Michael Pauly, T-Systems International GmbH
- Kurt Rindle, IBM Deutschland GmbH
- Dr. Peter Spitzner, Detecon International GmbH
- Tim Stadelmann,
  Atos Consulting & Technology Services
- Dr. Mathias Weber, BITKOM e.V.
- Prof. Dr.-Ing. Sabine Wieland, Deutsche Telekom AG,
  Hochschule für Telekommunikation Leipzig

Weiterhin wirkten am Leitfaden mit

- Dr. Holger K. von Jouanne-Diedrich, Atos IT Solutions and Services GmbH
- Jan Kottmann, Google Germany GmbH
- Dr. Markus Leberecht, Intel GmbH
- Bernhard Przywara, Oracle Deutschland B.V. & Co. KG
- Ralf Stieglitz, Bull GmbH
- Timo Ulmer, Bürotex metadok GmbH
- Stephan Weinert, Computacenter AG & Co. oHG
- Dr. Hans Peter Wiesemann, DLA Piper UK LLP

12 Sachwortverzeichnis

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 140 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu gehören fast alle Global Player sowie 800 leistungsstarke Mittelständler und zahlreiche gründergeführte, kreative Unternehmen. Mitglieder sind Anbieter von Software und IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org