Cloud Computing – Was Entscheider wissen müssen

Ein ganzheitlicher Blick über die Technik hinaus

Positionierung, Vertragsrecht, Datenschutz, Informationssicherheit, Compliance

Leitfaden

BITKOM

Impressum

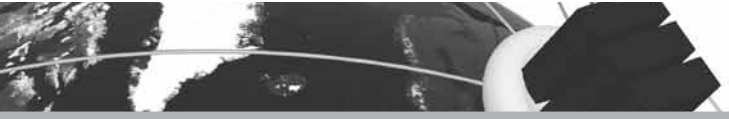
Herausgeber: BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner: Susanne Dehmel, Arbeitskreis Datenschutz
Thomas Kriesel, Arbeitskreis ITK-Vertrags- und Rechtsgestaltung
Lutz Neugebauer, Arbeitskreis Sicherheitstechnologien
Dr. Mathias Weber, Arbeitskreis Cloud Computing und Outsourcing

Redaktion: Dr. Mathias Weber

Redaktionsassistenz: Monika Kreisel

Gestaltung / Layout: Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)



Cloud Computing – Was Entscheider wissen müssen

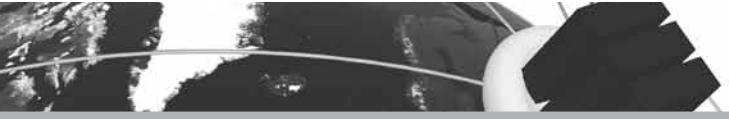
Ein ganzheitlicher Blick über die Technik hinaus

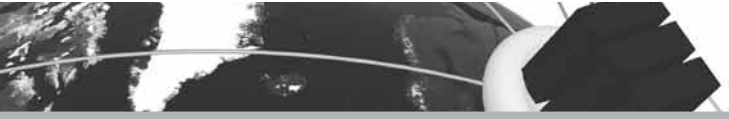
Positionierung, Vertragsrecht, Datenschutz, Informationssicherheit, Compliance

Leitfaden

BITKOM

Inhaltsverzeichnis





Abbildungen

Tabellen

Geleitwort

Cloud Computing bietet große Chancen für den High-Tech-Standort Deutschland. Dank Cloud Computing können Unternehmen Rechenleistungen, Speicherkapazitäten und Software in dem Umfang mieten, wie sie tatsächlich benötigt werden. Unternehmen sparen damit Kosten und werden deutlich flexibler. Gerade kleine und mittlere Unternehmen können auf diese Weise hochinnovative Leistungen in Anspruch nehmen, ohne in den Aufbau und die Wartung von großen Rechenzentren zu investieren. Cloud Computing ermöglicht es den Unternehmen, sich auf das Kerngeschäft zu konzentrieren. Sie können effizienter arbeiten, höhere Qualitäten anbieten und ihren Wettbewerbsvorteil weiter ausbauen. Davon profitiert die gesamte deutsche Wirtschaft.

Zusammen mit der Wirtschaft und der Wissenschaft hat das Bundesministerium für Wirtschaft und Technologie in diesem Jahr das Aktionsprogramm Cloud Computing gestartet. Der BITKOM ist dabei ein wichtiger Partner. Unser gemeinsames Ziel ist es, die großen Chancen von Cloud Computing für den Standort Deutschland frühzeitig zu erkennen und zu ergreifen. Wir wollen die Innovations- und Marktpotenziale besser erschließen, innovationsfreundliche Rahmenbedingungen schaffen und die Entwicklungen auch auf internationaler Ebene mitgestalten. Cloud Computing spielt aufgrund seiner großen technologischen und wirtschaftlichen Bedeutung auch in der neuen IKT-Strategie der Bundesregierung „Deutschland Digital 2015“ eine zentrale Rolle.

Viele Unternehmen sammeln gegenwärtig erste Erfahrungen mit Cloud Computing. Andere wissen noch gar nicht, welche Möglichkeiten Cloud Computing überhaupt bietet. Dieser Leitfaden gibt ihnen ausführliche und praxisrelevante Informationen und Empfehlungen zu diesem Thema in die Hand. Damit können die Vorteile von Cloud Computing schneller erkannt und besser genutzt werden. Mit dem Leitfaden leistet der BITKOM einen wichtigen Beitrag zu unserem Aktionsprogramm Cloud Computing. So wird Deutschland fit für die Zukunft.

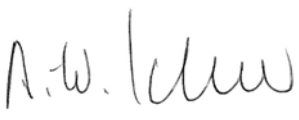
Rainer Brüderle
Bundesminister für Wirtschaft und Technologie

Cloud Computing leitet einen grundsätzlichen Richtungswechsel im Angebot und Einsatz von IT ein. Viele IT-Leistungen, die bislang individuell für einzelne Kunden gefertigt wurden, werden künftig in standardisierter Form aus dem Netz bezogen. Für die Nutzer bieten Cloud-Services einen Weg, ihre Handlungsfähigkeit im globalen Wettbewerb zu steigern und auch die Kosten zu senken. Viele Unternehmen sammeln gegenwärtig erste Erfahrungen im Einsatz von Cloud-Services. Sie wollen Cloud Computing breiter einsetzen, wenn ihre hohen Anforderungen an Datenschutz, Informationssicherheit und Integrationsfähigkeit mit den vorhandenen IT-Systemen erfüllt werden.

Cloud Computing eröffnet ganz neue Chancen, für einzelne Unternehmen wie für den Standort Deutschland. Um diese Chancen zu ergreifen, müssen industrielle Anbieter und Anwender sowie Politik und Wissenschaft zügig und gemeinsam handeln. Das Aktionsprogramm des Bundesministeriums für Wirtschaft und Technologie schaft dafür eine geeignete Grundlage. Der BITKOM bringt seine Projekte in das Aktionsprogramm mit dem Ziel ein, zur Entwicklung einer wettbewerbsfähigen Industrie für Cloud-Services am Standort Deutschland beizutragen.

Zu diesen Projekten gehört auch dieser Leitfaden „Cloud Computing – Was Entscheider wissen müssen“. Über 30 Autoren haben ihr Know-how zusammengetragen, um in konzentrierter Form auf die Fragen zu antworten, die sich Unternehmen beim Einsatz von Cloud Computing stellen.

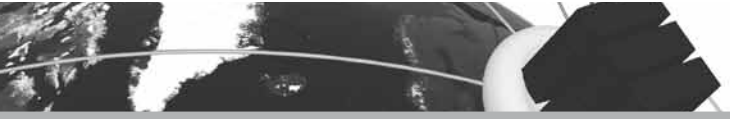
Allen Interessenten wünsche ich eine anregende Lektüre und viel Erfolg beim Einsatz von Cloud Computing.



Prof. Dr. Dr. h.c. mult. August-Wilhelm Scheer

Verzeichnis der Abkürzungen

AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
ASP	Application Service Providing
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BilMoG	Bilanzmodernisierungsgesetz
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BPaaS	Business Process as a Service
CI	Continuous Integration
CIO	Chief Information Officer
CMS	Compliance Management System
CobiT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRM	Customer Relationship Management
DB	Database
DCGK	Deutscher Corporate Governance Kodex
DDoS	Distributed Denial of Service
DIN	Deutsches Institut für Normung
ENISA	European Network and Security Agency
ERP	Enterprise Resource Management
EU	Europäische Union
FAIT	Fachausschuss für Informationstechnologie
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
GxP	Good {Manufacturing, Distribution, Clinical Laboratory, Automated Manufacturing, Documentation, ...} Practice
HGB	Handelsgesetzbuch
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IDS	Intrusion-Detection-System
IDW	Institut der Wirtschaftsprüfer
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPS	Intrusion-Prevention-System
IPSec	Internet Protocol Security
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
IT	Informationstechnologie
ITIL	IT Infrastructure Library



KontraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPI	Key Performance Indicator
KWG	Kreditwesen-Gesetz
LOB	Line of Business
MaRisk	Mindestanforderungen an das Risikomanagement
NIST	National Institute of Standards and Technology
OCCI	Open Cloud-Computing-Interface
OSI	Open Systems Interconnection
OVF	Open Virtualization Format
PaaS	Platform as a Service
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PS 330	IDW Prüfungsstandard 330
SaaS	Software as a Service
SAS	Statement on Auditing Standards
SecS	Security as a Service
SGB X	Sozialgesetzbuch (SGB) Zehntes Buch (X) Sozialverwaltungsverfahren und Sozialdatenschutz
SIEM	Security Incident and Event Monitoring
SLA	Service Level Agreement
SOX	Sarbanes-Oxley-Act
StGB	Strafgesetzbuch
TK	Telekommunikation
TKG	Telekommunikations-Gesetz
TLS/SSL	Transport Layer Security/Secure Sockets Layer
TMG	Telemediengesetz
UML	Unified Modelling Language
UrhG	Urheberrechtsgesetz
VLAN	Virtual Local Area Networks
VoIP	Voice over IP
VPN	Virtual Private Network
WAF	Web-Applikation Firewall
XML	Extensible Markup Language

Management Summary

Cloud Computing als neues Paradigma zur Erbringung von IT-Services

Cloud Computing wird in der Informationswirtschaft häufig als neuer technologischer Ansatz diskutiert, als ein nächster Schritt in der Evolution der Informationstechnologie. Cloud Computing ist aber mehr als ein Thema für das IT- oder das Technologie-Management von Unternehmen – es wird sowohl das Geschäftsleben als auch die Gesellschaft nachhaltig verändern. Die neuen Eigenschaften „Nutzung nach Bedarf" oder „Bezahlung nach Nutzung" sind wichtig – aber erst die stärkere Unabhängigkeit der Geschäftsprozesse von der Ressourcenvorhaltung, die Beschleunigung von Innovationen und die höhere Flexibilität für „atmendes" Business verleihen Cloud Computing die Sprengkraft einer Revolution im Business.

Cloud Computing lässt sich in zwei prinzipielle Organisationsformen und drei Service-Ebenen kategorisieren: Aus Private Clouds und Public Clouds werden Leistungen als Komplettsoftware, Plattform oder Infrastruktur bezogen. Das Businessszenario bestimmt im Rahmen einer ganzheitlichen Strategie, auf welche Formen des Cloud Computings zurückgegriffen wird. Entscheidend für den Einsatz sind neben den Anforderungen von technischer Seite vor allem die von Vertragsrecht, Datenschutz, Informationssicherheit und Compliance vorgegebenen Rahmenbedingungen. Diese stehen im Fokus des Leitfadens.

Vertragliche Regelungen

Der Cloud-Computing-Vertrag definiert zu erbringende Leistungen und wechselseitige Pflichten. Er muss alle notwendigen Vereinbarungen enthalten, um Cloud Computing in dem gesetzlich zulässigen Rahmen durchzuführen, auch Regelungen für den Datenschutz, Informationssicherheit und Compliance. Nach Möglichkeit sollte deutsches Recht vereinbart werden.

Ausgangspunkt ist der konkrete Bedarf des Kunden. Die Leistungsbeschreibung als zentraler Inhalt des Vertrags entscheidet darüber, welche gesetzliche Vertragstypen anzuwenden sind und damit, welche gesetzlichen Vorschriften bei Leistungsstörungen gelten. Diese sind häufig nicht praxistauglich. Es empfiehlt sich daher, in Service Level Agreements konkrete Kriterien der Leistungserbringung und Folgen von Störungen zu vereinbaren.

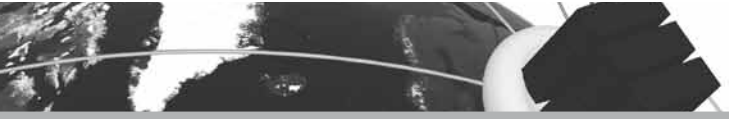
Als weiterer wichtiger Aspekt sind für die Software, die in der Cloud bereitgestellt wird, die erforderlichen Nutzungsrechte zu vereinbaren. Werden Subunternehmer durch den Cloud Anbieter eingebunden, sind insbesondere Regelungen zu treffen, um die gesetzlichen Vorgaben auch auf zweiter oder dritter Leistungsebene vollständig umzusetzen.

Die auf dem Markt angebotenen Cloud-Leistungen spiegeln in ihrer Vielgestaltigkeit die unterschiedlichen individuellen Kundensituationen wider. Bei der vertraglichen Umsetzung muss daher die kundenspezifische Ausgangslage mit ihren Anforderungen genau betrachtet werden, um die für den Vertrag notwendigen Vereinbarungsinhalte zu bestimmen sowie deren praktische Umsetzung zu ermöglichen.

Datenschutz

Der Datenschutz kann, muss aber nicht Hemmschuh des Cloud Computings sein. Entscheidend ist zum einen die Art der verarbeiteten Daten und zum anderen, in welcher Ausprägung Cloud Computing (Private oder Public) betrieben wird.

Unproblematisch ist die Verarbeitung von technischen oder wirtschaftlichen Daten in jeder Form der Cloud, sofern sie keine Geschäftsgeheimnisse darstellen. Fallen die Daten jedoch in die Kategorie HGB- oder steuerrelevante Daten, sind Einschränkungen durch die



Finanzverwaltung vorgegeben. Dem gegenüber fordern personenbezogene Daten und mehr noch die sensiblen Daten (z.B. Angaben zur Gesundheit oder Religion) erhöhten Schutzaufwand. In diesen Fällen können die potenziellen Einsparungen, die mit Cloud Computing angestrebt werden, meist nicht vollständig realisiert werden.

Lösungsansätze sind im Falle der Private Cloud die Einstellung von sog. Corporate Binding Rules im Konzernverbund oder der Abschluss von Verträgen mit externen Dienstleistern, wie sie aus der Auftragsdatenverarbeitung bisher schon bekannt sind. Bei der Verlagerung von personenbezogenen Daten in Drittländer mit nicht so hohem Schutzniveau wie in dem europäischen Wirtschaftsraum sind hierzu die EU-Standardvertragsklauseln zu verwenden. Der Einsatz von Public Clouds und Ableitungen hiervon wie z.B. Hybrid Clouds dürfte auf Grund der schwierigen Kontrolle von vertraulicher Verarbeitung der personenbezogenen Daten nur sehr eingeschränkt nutzbar sein. Es bieten sich hier allerdings Verschlüsselungslösungen an, sofern für die Verarbeitung die Weitergabe des Schlüssels nicht erforderlich ist.

Dies bedeutet, dass sich heute nur ein bestimmter Teil von Anwendungen nicht im Cloud Computing abbilden lässt. Dabei handelt es sich vor allem um Krankendaten, deren Zugänglichmachung für Dritte im StGB strafbewehrt untersagt wird. Die restriktiveren Forderungen einzelner deutscher Aufsichtsbehörden werden sich unter EU-Harmonisierungs-Gesichtspunkten nur bedingt durchsetzen lassen.

Informationssicherheit

Die Gewährleistung der Informationssicherheit nimmt im Rahmen von Cloud Computing eine zentrale Rolle ein. Dabei muss bereits zum Zeitpunkt der Entscheidung über den Einsatz sowie der anschließenden operativen Integration von Cloud-Computing-Systemen in betriebliche IT-Infrastrukturen ein definiertes Vorgehen zur Anwendung kommen. Ferner umfasst der sichere Betrieb eines Cloud Computings in technischer Hinsicht die Einhaltung der klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Konkret muss dazu die Sicherheit einzelner Komponenten einer Cloud-Computing-Architektur betrachtet und gewährleistet sein. Zudem tragen organisatorische Vorkehrungen zum informationssicheren Einsatz und Betrieb von Cloud-Computing-Architekturen bei.

Cloud Computing fordert allerdings nicht nur Sicherheit, sondern kann diese auch bereitstellen. Hier spricht man von Security as a Service (SecS), welche Sicherheitsfunktionen als Service anderen Systemen zur Nutzung anbietet.

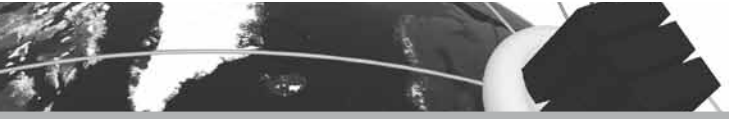
Cloud Compliance

Cloud Compliance bezeichnet die nachweisbare Einhaltung von Regeln bei der Nutzung oder Bereitstellung von Cloud Computing. Compliance schafft die erforderliche Transparenz und Sicherheit für alle beteiligten Interessengruppen (Stakeholder). Insoweit leistet Cloud Compliance einen wichtigen Beitrag, um die derzeitige Zurückhaltung bei potentiellen Kunden des Cloud Marktes aufzulösen. Damit ist Cloud Compliance zugleich ein Wegbereiter, um alle Vorteile des Cloud Computing für Anbieter und Provider vollumfänglich nutzbar zu machen.

Bis zur Durchsetzung am Markt sind noch eine Reihe an Hürden zu bewältigen. Diese betreffen beispielsweise die Neuartigkeit und Komplexität des Themas, die Vielzahl von Service-Angeboten und Geschäftsmodellen der Anbieter, unklare bzw. sich widersprechende Cloud Definitionen und ganz generell die fehlenden Standards im Markt.

Ein sinnvolles Werkzeug in dieser Situation ist ein Compliance Management System (CMS). Es unterstützt Anbieter und Nutzer gleichermaßen, die spezifischen Anforderungen zur Compliance risikoorientiert zu identifizieren, zu bewerten sowie zielgerichtete Maßnahmen zur Sicherung und Aufrechterhaltung der Compliance einzuleiten. Der Grundgedanke eines CMS lässt sich auf die Kernthemen Anforderungen, Risiken und Risikomaßnahmen komprimieren. Auf diese Kernthemen wird im Kapitel Cloud Compliance detailliert eingegangen.

Bei allem Optimismus, die derzeit erkennbaren Risiken des Cloud Computings durch geeignete Maßnahmen zur Compliance zu steuern und damit die Vorteile des Cloud Computings auf breiter Ebene nutzbar zu machen, wird aber auch auf derzeitig noch bestehende Grenzen verwiesen. Demnach können Situationen nicht ausgeschlossen werden, in denen eine zufriedenstellende Cloud Compliance nur mit unverhältnismäßigem Aufwand oder gar nicht erreicht werden kann. An der Lösung der damit verbundenen Compliance-Herausforderungen muss dringend gearbeitet werden.



1 Cloud Computing als neues Paradigma zur Erbringung von IT-Services

- Die IT hat zu einer Beschleunigung der Geschäftsprozesse geführt; sie unterstützt Unternehmen, schnell und flexibel auf geschäftliche Anforderungen zu reagieren und ermöglicht selbst neue Geschäftsmodelle und -prozesse. IT-Nutzer fordern daher vermehrt eine flexible IT, die sich an den Anforderungen des Business orientiert.

- Cloud Computing ist eine Form der Bereitstellung von gemeinsam nutzbaren und flexibel skalierbaren IT-Leistungen durch nicht fest zugeordnete IT-Ressourcen über Netze. Idealtypische Merkmale sind die Bereitstellung in Echtzeit als Self Service auf Basis von Internet-Technologien und die Abrechnung nach Nutzung. Damit ermöglicht Cloud Computing den Nutzern eine Umverteilung von Investitions- zu Betriebsaufwand. Die IT-Leistungen können sich auf Anwendungen, Plattformen für Anwendungsentwicklungen und –betrieb bzw. Basisinfrastruktur beziehen

- Der mit Cloud Computing eingeläutete Paradigmenwechsel bildet eine Herausforderung für Unternehmen als Ganzes. Durch Cloud Computing wird eine Änderung von Unternehmensstrategien notwendig. Wer Cloud Computing an die IT-Abteilung delegiert, verkennt das Wesen dieser Innovation.

- Der „Stammbaum“ von Cloud Computing gründet sich auf zwei Urformen, die Public und die Private Cloud. Andere Ausprägungen wie Hybrid Clouds, Virtual Private Clouds, Vertical (Community) Clouds sowie Horizontal Clouds sind Derivate, Kombinationen oder Speziallösungen dieser Urformen. Regionale Clouds bezeichnen spezifische Standorte der zugrundeliegenden IT und TK. Eine einfache Typisierung ergibt sich, wenn man Clouds anhand der organisatorischen und der Sourcing-Dimension unterscheidet.

- Darüber hinaus haben sich drei Service-Ebenen etabliert: IaaS, PaaS, SaaS. Mit BPaaS wird aktuell eine vierte Ebene diskutiert, die aus SaaS hervorgeht und noch näher an die Business-Prozesse heranrückt.

- Cloud-Computing-Services sind grundsätzlich für Unternehmen jeder Größenordnung interessant, jedoch werden sich Nutzungsschwerpunkte herausbilden: Kleine Unternehmen nutzen eher Public Clouds, während größere Unternehmen Private Clouds den Vorzug geben.

- Cloud Computing ist eine Antwort auf die aktuellen Herausforderungen von Unternehmen. Denn ein neuer Bezug und eine neue Produktion von IT kann stärker als bisher das Geschäft unterstützen. Dadurch entsteht eine Basisinnovation im Business. Mit „Evolution in der Technik, Revolution im Business“ lässt sich kurz zusammenfassen, was Cloud Computing ausmacht. Durch seine wirtschaftlichen Vorzüge wird Cloud Computing mittel- bis langfristig einen beträchtlichen Teil der traditionellen IT-Leistungsangebote ersetzen. Cloud Computing ist ein Paradigma, das die gesamte Informationswirtschaft, ihre Technologien und ihr Geschäft und somit auch die Beziehungen zwischen Anbietern und Kunden nachhaltig verändern wird.

- Mit Cloud Computing werden global bereits Umsätze im zweistelligen Milliarden-Dollar-Bereich erzielt. Der Cloud-Markt entwickelt sich in den nächsten Jahren auch in Deutschland mit einer jährlichen

Wachstumsrate, die bei 40 Prozent liegt. Integrationsprobleme mit vorhandenen IT-Systemen, das fehlende Vertrauen in Datenschutz- und Datensicherheits-Konzepte sowie die im Einzelfall unklare rechtliche Situation sind derzeit die größten Hemmnisse für eine schnellere Marktentwicklung in diesem Segment. Aber auch Herausforderungen bei der Integration oder ein generelles Misstrauen gegenüber Cloud-Anbietern haben als Hemmnisse große Bedeutung.

- Die Palette möglicher Einsatzszenarien für Cloud Computing ist breit. Bestehen noch keine unternehmenseigenen IT-Strukturen, so bieten Cloud-Services bereits heute eine Alternative zum Eigenbetrieb bzw. zum klassischen Outsourcing. Das Einsatzszenario wird sich an der Art des Service, dessen Bedeutung für den Kunden, dem Standardisierungsgrad und der Struktur des nutzenden Unternehmens orientieren.

- Ein erfolgreicher Einstieg in Cloud Computing gelingt, wenn alle Unternehmenseinheiten eine gemeinsame Strategie entwickeln, die auf Basis einer Analyse von Geschäftsprozessen und IT mit einem gemeinsamen Zielbild startet. Unter Berücksichtigung der Aspekte von Recht, Sicherheit, Datenschutz und Compliance können geeignete Services zu einem Cloud-Provider überführt werden. Dabei ist insbesondere zu beachten, dass Mitarbeiter sensibilisiert und die Einkaufsprozesse entsprechend vorbereitet werden.

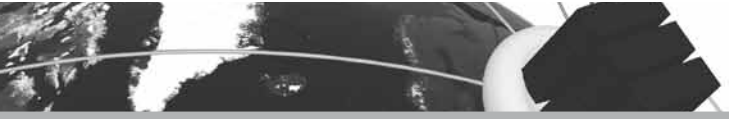
- Cloud-Computing-Technologien bewirken, dass die bisher im Wesentlichen lineare Wertschöpfungskette bei IT-Dienstleistungen aufbricht. So können z.B. durch Technologien zur dynamischen Lastverteilung Nutzer von Infrastructure as a Service Leistungen auch zu Anbietern dieser Leistungen werden. Ebenso lassen sich auch bisher nur intern genutzte Funktionalitäten relativ einfach im Software-as-a-Service-Modell externen Nutzern zur Verfügung stellen. Die steigende Zahl von Anbietern hochstandardisierter Funktionen erhöht den Preisdruck und unter Umständen auch die Flexibilität für einen Wechsel der Anbieter. In Summe entsteht ein innovatives, dynamisches Netzwerk von Anbietern und Konsumenten von IT Dienstleistungen.

- Den Vorteilen von Cloud Computing steht eine Vielzahl von Hemmnissen entgegen. Für den Erfolg des Cloud Computings ist ein klarer rechtlicher Rahmen zwingende Voraussetzung. Weitere Erfolgsfaktoren bilden aber auch ein ausreichender Datenschutz, die Interoperabilität zwischen den Cloud-Services (Unabhängigkeit von einem Anbieter), die Ausgewogenheit zwischen Individualität und hoher Standardisierung (Integration mit der vorhandenen IT-Landschaft in den Unternehmen) und organisatorische Voraussetzungen im Unternehmen.

1.1 Herausforderungen für Unternehmen

Die Unternehmen in westlichen Industriestaaten sehen sich einem Zeitalter zunehmender Flexibilität und nie dagewesener Geschwindigkeit wirtschaftlicher Prozesse gegenüber. Ausgelöst und befeuert wurde diese Beschleunigung durch die Errungenschaften der Informationstechnologie (IT) und der Telekommunikation (TK), insbesondere das Internet. Diese Zunahme an Dynamik und Geschwindigkeit fordert auch ihren Tribut von der IT. Die IT ist mehr denn je aufgefordert, schnell und flexibel auf geschäftliche Anforderungen zu reagieren, ja selbst auch neue Geschäftsmodelle und -prozesse zu ermöglichen.

Allerdings umfassen die Kosten für den Betrieb der IT-Infrastruktur einen nicht unerheblichen Teil der IT-Budgets in den Unternehmen. Analysten schätzen ihn auf etwa 75 Prozent. Dadurch haben IT-Verantwortliche wenig Raum für Innovation. Gleichzeitig arbeiten viele Rechenzentren wenig effizient. Besondere Beachtung verdient diese



Tatsache, weil die unterhaltenen Rechenressourcen in der Regel nicht den aktuellen Business-Anforderungen zur Verfügung gestellt, sondern vielmals für die Spitzenlasten bestimmter Services vorgehalten werden. Zuletzt bleibt noch die Herausforderung von Sicherheit und Transparenz – insbesondere, wenn die Zusammenarbeit in Projekten Unternehmensgrenzen überschreitet.

Cloud Computing ist nicht nur ein Thema für die IT-Abteilungen. Der Paradigmenwechsel ist eine Herausforderung für Unternehmen als Ganzes. Durch Cloud Computing wird eine ganzheitliche Änderung von Unternehmensstrategien notwendig. Hier sollte insbesondere die Aufgabenverteilung zwischen Fachabteilungen und IT-Abteilung geregelt werden. Dazu gehört beispielsweise festzulegen, wer die Verantwortung für Datensicherheit übernimmt und nach welchen Prozessen IT-Leistungen eingekauft werden. Cloud Computing fordert eine Umverteilung von Rollen und Kompetenzen und etabliert im Idealfall auch ein neues Rollenverständnis. Dadurch werden sich auch IT-Organisationen verändern – inhaltlich und personell.

1.2 Cloud Computing – Begriffsbestimmungen

1.2.1 Definition Cloud Computing

Cloud Computing ist eine Form der Bereitstellung von gemeinsam nutzbaren und flexibel skalierbaren IT-Leistungen durch nicht fest zugeordnete IT-Ressourcen über Netze. Idealtypische Merkmale sind die Bereitstellung in Echtzeit als Self Service auf Basis von Internet-Technologien und die Abrechnung nach Nutzung. Damit ermöglicht Cloud Computing den Nutzern eine Umverteilung von Investitions- zu Betriebsaufwand. Die IT-Leistungen können sich auf

- Anwendungen,
- Plattformen für Anwendungsentwicklungen und -betrieb,
- Basisinfrastruktur

beziehen.[1]

In Zukunft wird sich der operative Einsatz des Cloud-Computing-Paradigmas im industriellen wie auch privaten Umfeld weiter etablieren. Der Leitfaden beschreibt folglich einen Übergangszustand von konventionellen IT-Systemen hin zu Cloud-Computing-Systemen. Vor dem Hintergrund dieses Status quo sind die definierten Eigenschaften einer Cloud bzw. eines Cloud-Computing-Systems idealtypisch. Aus technischer Sicht spielt zur Erfüllung dieser Idealvorstellung z.B. der Automatisierungsgrad eine entscheidende Rolle. Dies betrifft insbesondere die automatisierte Bereitstellung von Services durch die Cloud, die in Abhängigkeit vom Nutzerbedarf erfolgt. Einer solchen hochflexiblen Nutzung von Cloud-Services stehen derzeit sowohl organisatorische als auch rechtliche Hemmnisse gegenüber, die der definitorischen Ausprägung des Cloud Computings entgegenwirken. Dieser Leitfaden richtet sich insbesondere auf den Umgang mit den Hemmnissen und bietet Orientierung für die zusätzlichen, praktischen Herausforderungen, welche sich aus dem Einsatz von Cloud-Computing in dieser Übergangsphase ergeben.

1.2.2 Service-Ebenen

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

1. Diese Definition ist konform zu der Definition des National Institute of Standards and Technology (NIST). Sie präzisiert die im ersten Leitfaden des BITKOM zum Cloud Computing (vgl. „Cloud Computing - Evolution in der Technik, Revolution im Business“, BITKOM-Leitfaden, Berlin 2009. Verfügbar auf www.cloud-practice.de) formulierte Definition mit dem Ziel, juristische Klarheit zu schaffen.

Tabelle 1: 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.

Bei der Betrachtung der Service-Ebenen lohnt ein intensiver Blick auf die Lizenzsituation: In einem echten SaaS-Modell sind die Lizenzkosten für die eingesetzte Software in der Nutzungspauschale eingepreist. Für Software-Provider bedeutet dies eine fundamentale Abkehr von etablierten Lizenzmodellen zur Softwarenutzung. Der Kunde muss im Vorfeld abklären, ob er für die (nicht Cloud-konforme) Bereitstellung von Lizenzen sorgen muss.

1.2.3 Merkmale wichtiger Cloud-Typen

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 (vgl. Abbildung 1).

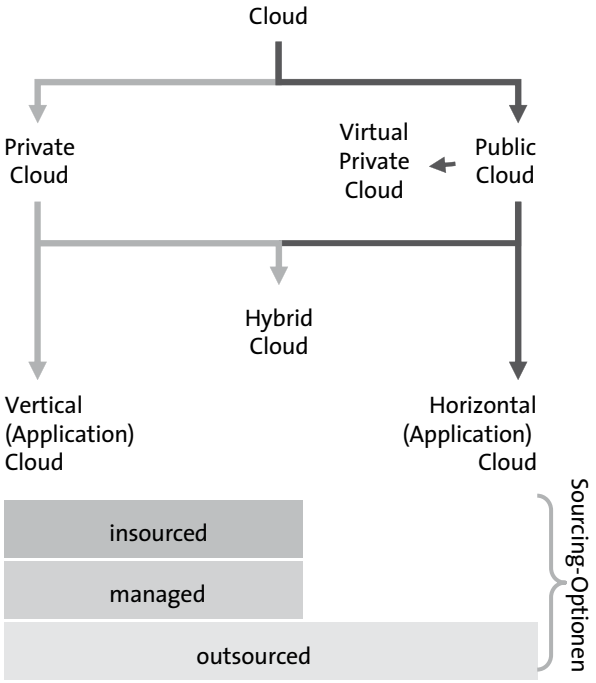
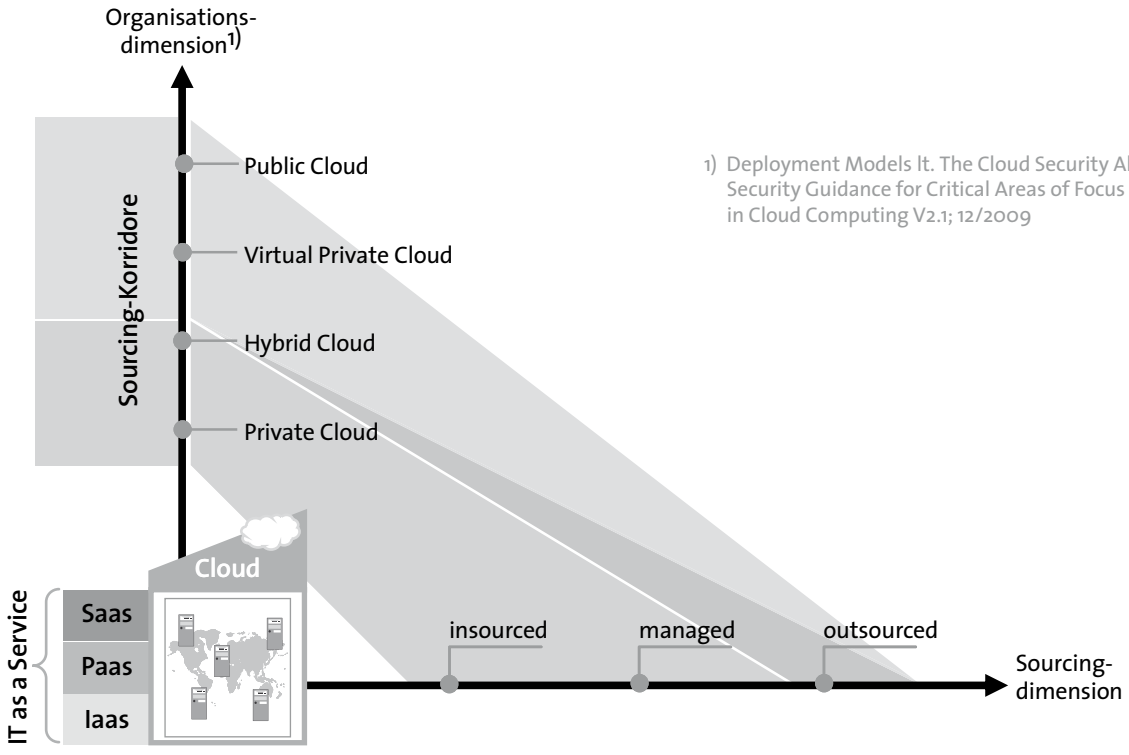


Abbildung 1: Stammbaum der Clouds

Analysiert man den derzeitigen Stand der Cloud-Diskussion, dann lassen sich die verschiedenen Cloud-Typen grob über zwei Dimensionen definieren (vgl. Abbildung 2),

- 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 2):



1) Deployment Models It. The Cloud Security Alliance; Security Guidance for Critical Areas of Focus in Cloud Computing V2.1; 12/2009

Abbildung 2: Typisierung von Clouds in zwei Dimensionen

Tabelle 2: Vergleich wichtiger Organisationsformen von Clouds

	Public Cloud / External Cloud	Virtual Private Cloud	Hybrid Cloud	Private Cloud / Internal 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.	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.	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.	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	Mittels Browser über das Internet auf IaaS-, PaaS- und SaaS-Services	Mittels Browser über Intranet (sichere VPN-Verbindung) auf IaaS-, PaaS- und SaaS-Services.	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.	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

	Public Cloud / External Cloud	Virtual Private Cloud	Hybrid Cloud	Private Cloud / Internal Cloud
Service Level Agreements	Standard (in der Regel nicht individuell anpassbar)	in Grenzen individuell anpassbar	Kombination aus individuell (Private Cloud) und Standard (Public Cloud)	kundenspezifisch frei definierbar
Sourcing Optionen	outsourced[2]	outsourced	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[3] möglich. Der Teil der Public Cloud ist outsourced.	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.

Vertical (Application) Cloud (Community Cloud)

Die Vertical (Application) Cloud – oder auch Community Cloud – ist eine Ausprägung der Private Cloud mit allen Vor- und Nachteilen dieser Cloud-Form. Sie stellt auf der SaaS-Ebene für eine definierte Gruppe von Unternehmen mit gleichen oder ähnlichen Geschäftsprozess- und Applikationsanforderungen („Community“) spezielle, standardisierte branchenspezifische Anwendungsbausteine zur Verfügung.

Horizontal (Application) Cloud

Eine Horizontal Cloud ist die SaaS-Ebene einer Public Cloud. Sie stellt branchenunspezifische (= horizontale) Anwendungslösungen bereit und verfügt damit auch über alle Vor- und Nachteile dieser Cloud-Form.[4]

Cloud-Computing-Services sind grundsätzlich für Unternehmen jeder Größenordnung interessant, jedoch werden sich Nutzungsschwerpunkte herausbilden (Abbildung 3).

2. im Eigentum eines externen IT-Dienstleisters befindliche und von diesem betriebene Cloud-Umgebung
3. insourced (Eigenbetrieb), managed (im Hause des Kunden durch einen externen Dienstleister), outsourced (im Hause des. Dienstleisters durch den externen Dienstleister)
4. Da die Begriffe Horizontal Cloud und Public Cloud oft in gleichem Sinne verwendet werden, finden sich deshalb für Horizontal Clouds häufig auch vereinfachende Begriffe wie z. B. “CRM-Cloud”, „Communication Cloud” oder auch “ERP-Cloud”.

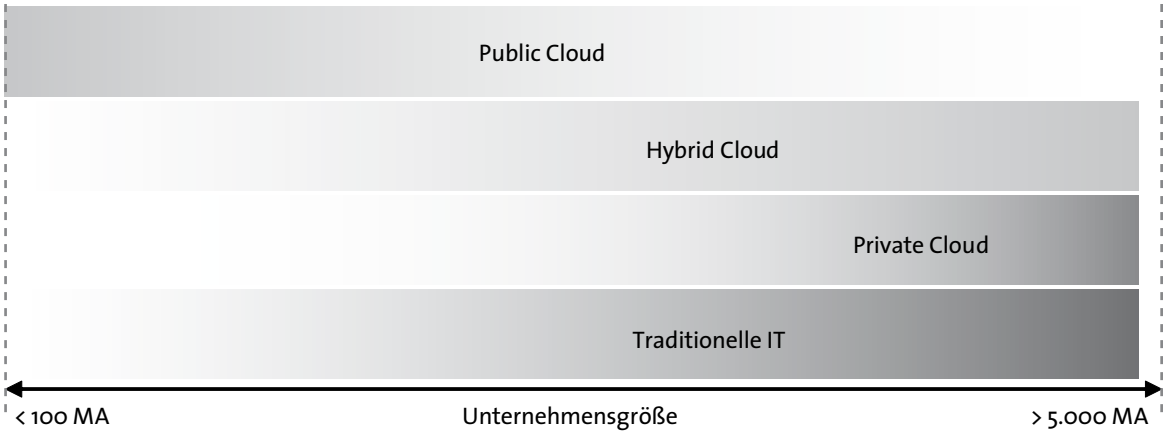


Abbildung 3: Nutzungsschwerpunkte – Typen von Clouds – Unternehmensgrößen

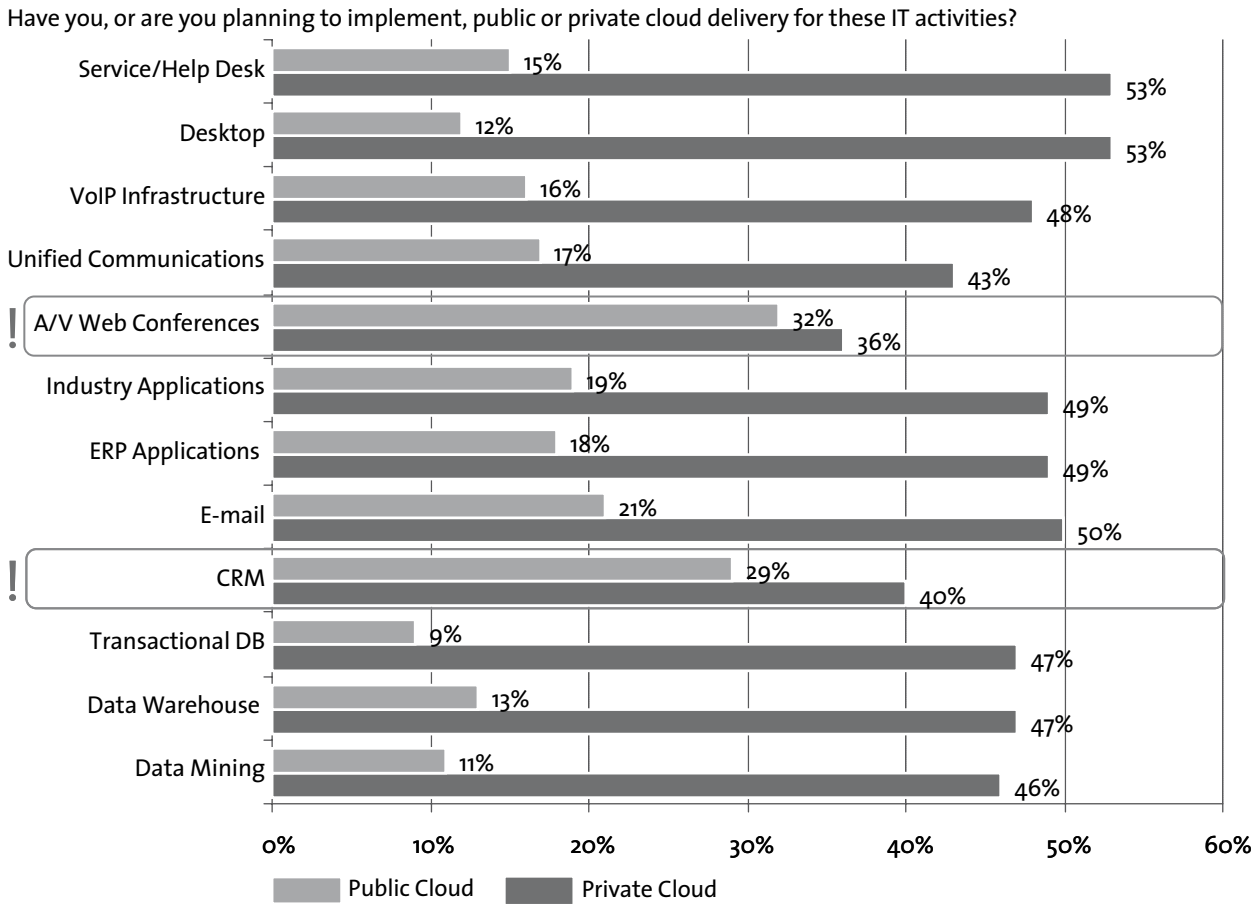


Abbildung 4: Anwendungsbereiche von Clouds und Organisationsformen

Kriterien	Cloud-Typen			
	Public	Virtual Private	Hybrid	Private
Kostenminimierung	■	◨	◨	□
Datensicherheit	◨	■	◨	■
Datenschutz	◨	■	◨	■
Compliance	□	◨	◨	■
Möglichkeit Innovation und Marktdifferenzierung	□	◨	■	■
Generierung von Wettbewerbsvorteilen	◨	◨	◨	■
Flexibilisierung der Geschäftsprozesse	■	◨	◨	◨
Vereinbarung individueller SLAs	□	■	◨	■
Sicherstellung allgemeiner End-to-end-Betriebssicherheit	□	◨	◨	■
Auditfähigkeit/-möglichkeit	□	■	◨	■
Sicherung (Weiternutzung) bestehender Investitionen	◨	◨	◨	■
Integration in bestehende Applikationslandschaften (Service Integration)	◨	◨	◨	◨
Vorhandensein und Verfügbarkeit von Unterstützungsfunktionen (Skill)	□	◨	◨	■
Sicherstellung allgemeiner End-to-end-Verfügbarkeit	□	◨	◨	■

■ möglich / voll erreicht ◨ mit Abstrichen möglich / erreicht □ nicht bzw. weniger gut möglich / erreicht

Abbildung 5: Bewertung der Cloud-Typen

Über die Anwendungsbereiche hinweg bestätigt sich die sehr deutliche Präferenz zur Implementierung von Private Clouds (vgl. Abbildung 4)[5]

Eine zusammenfassende erste Bewertung der Cloud-Typen im direkten Vergleich ist in der Abbildung 5 enthalten.

1.2.4 Regionale Dimension – Deutsche und Europäische Cloud

Bisweilen werden Clouds auch mit einem regionalen Zusatz versehen. Die regionale Angabe kann sich auch auf die Nutzergruppe der Cloud beziehen oder die Services bezeichnen, die die administrativen Einheiten nutzen bzw. für Bürger bereitstellen. Für den vorliegenden Leitfaden hingegen ist die Lokation der Rechen- und Netzressourcen entscheidend. Deutsche Cloud bedeutet dementsprechend, dass die Server und Netze dieser Cloud ausschließlich in Rechenzentren in Deutschland stehen. Analog wird eine europäische Cloud definiert.

1.3 Business-Potenzial des Cloud Computings – Treiber und Barrieren

Cloud Computing ist eine Antwort auf die Herausforderungen, denen sich Unternehmen gegenüber sehen. Denn ein neues Bezugs- und Produktionsmodell von IT kann stärker als bisher das Geschäft unterstützen. Dadurch entsteht eine Basisinnovation im Business.

Sie kann Kosten deutlich vermindern und Kostenstrukturen dauerhaft verändern. Ein Teil der Investitionskosten wandelt sich zu Betriebskosten. Die nutzungsabhängige

5. Source: IBM - Cloud Adoption, 06/2009, N = 1.090 IT and LOB decision makers. Percent who have implemented or plan to implement the workload. Respondents could select multiple items.

Bezahlung und der Abschied von festen IT-Budgets bedeuten eine Kostenvariabilisierung.

Unternehmen entscheiden sich für Cloud Computing eindeutig wegen des Potenzials zur Kostensenkung. Weitere Motive sind

- die verringerte Kapitalbindung (bedeutet größere finanzielle Spielräume sowie eine Verlagerung von langfristig fixen Investitionen zu variablen Kosten),
- eine mögliche Konzentration auf das Kerngeschäft,
- Umsetzbarkeit auch bei fehlendem Know-how,
- schnelle Realisierbarkeit sowie
- größere Flexibilität und Skalierbarkeit.

Mit dem Einsatz von Cloud Computing können neue Geschäftsprozesse und komplett neue Business-Modelle schneller implementiert werden; das Business wird flexibler. Reorganisationen in Unternehmen, Unternehmenszusammenschlüsse und Akquisitionen werden erleichtert.

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.

Auch die Standardisierung der IT-Services kann ein Argument für einen Einstieg in Cloud Computing sein – insbesondere für Unternehmen, die nicht über die finanziellen Ressourcen verfügen, selber eine ausreichende IT-Prozessunterstützung zu entwickeln oder einzukaufen. Die Einführung einer Cloud-basierten Lösung bietet dann eine Möglichkeit, dem Problem zu begegnen.

1.4 Bewertung von Cloud Computing als Evolution bzw. Revolution

Zahlreiche technologische Verbesserungs-Innovationen haben zum Cloud Computing geführt, das zu einer neuen Business-Qualität beitragen wird. Mit „Evolution in der Technik, Revolution im Business“ lässt sich kurz zusammenfassen, was Cloud Computing ausmacht. Durch seine wirtschaftlichen Vorzüge wird Cloud Computing mittel- bis langfristig einen beträchtlichen Teil der traditionellen IT-Leistungsangebote ersetzen.

Cloud Computing ist ein Paradigma, das die gesamte Informationswirtschaft, ihre Technologien und ihr Geschäft und somit auch die Beziehungen zwischen Anbietern und Kunden nachhaltig verändern wird. Kaum ein IT-Unternehmen wird sich diesem Paradigmen-Wechsel entziehen können.[6]

1.5 Marktentwicklung

Mit Cloud Computing werden global bereits Umsätze im zweistelligen Milliarden-Dollar-Bereich erzielt. Die Aussagen zur Größe des Marktes variieren jedoch stark – in Abhängigkeit von den Definitionen des Marktbeobachters. Außerdem wird oft nicht spezifiziert, für welche Organisationsform (Public oder Private Clouds) die Zahlen gelten.

Für den deutschen Markt liegen Studien der TechConsult GmbH[7] und der Experton Group AG vor. Experton Group schätzt die Ausgaben für Cloud-Technologien, Services

6. „For vendors, cloud computing is critically important for two key reasons - market growth and leadership disruption. The cloud model will propel IT market growth and expansion for the next 20 years and will help the industry to more rapidly develop and distribute a new generation of killer apps, and to more successfully penetrate small and medium-sized businesses. As this happens, industry leadership ranks will certainly change.“ (Frank Gens) Vgl.: IDC - Press Release, „Through 2014 Public IT Cloud-Services Will Grow at More Than Five Times the Rate of Traditional IT Products, New IDC Research Finds, 23 Jun 2010, http://www.idc.com/getdoc.jsp?containerId=prUS22393210 (Abruf: 15. Oktober 2010)
7. .Vgl. „Cloud Computing - Evolution in der Technik, Revolution im Business“, BITKOM-Leitfaden, Berlin 2009. Verfügbar auf www.cloud-practice.de

und Beratung in Deutschland im Jahre 2010 auf insgesamt 1,14 Milliarden Euro[8]. Der deutsche Cloud-Markt wächst bis 2015 mit jährlich über 40 Prozent. Und das bedeutet: Während 2010 „erst" 1,4 Prozent der IT-Ausgaben auf Cloud Computing entfielen, so werden es laut Experton Group im Jahr 2015 bereits 9,1 Prozent sein. Der Cloud-Markt nimmt also schnell an Bedeutung zu.[9]

Die weltweiten Ausgaben für Public Cloud Computing betrugen 2009 ca. 17 Mrd $ und damit etwa 4,7 Prozent der IT-Ausgaben. Im Jahre 2013 wird dieser Anteil auf 10,6 Prozent anwachsen[10] (vgl. Abbildung 7).

In einer Studie vom Juni 2010[11] prognostizierte IDC von 2009 bis 2013 eine Verdreifachung des Cloud-Marktes (vgl. Abbildung 8).

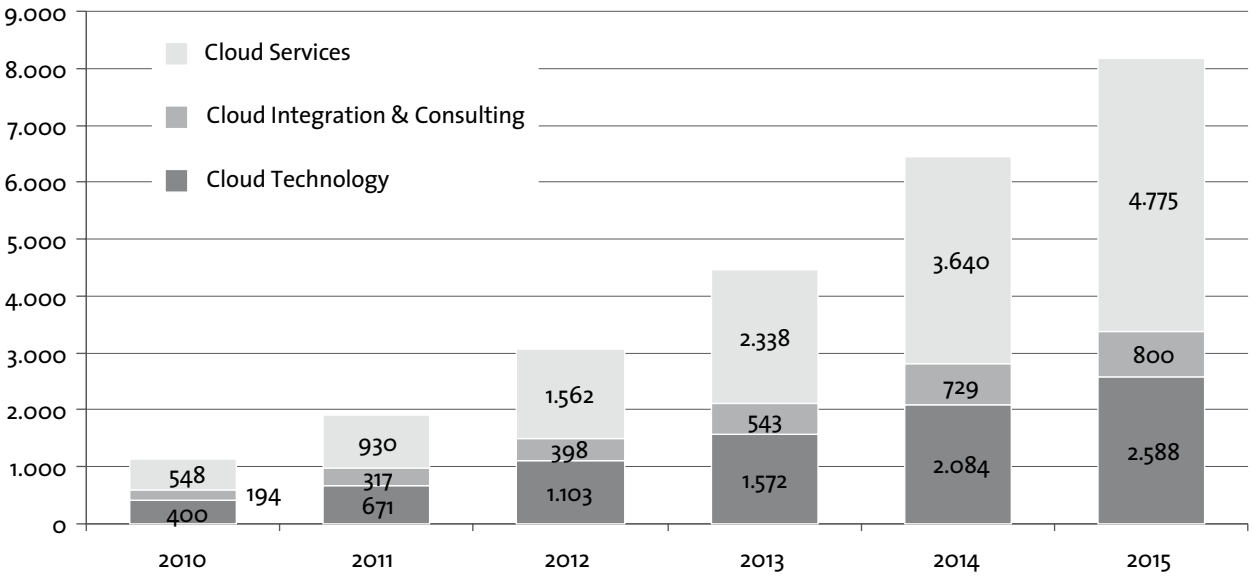


Abbildung 6: Entwicklung des deutschen Cloud-Marktes 2010-2015; Quelle: Experton Group, Oktober 2010

8. Vgl. Velten, Carlo; Janata, Steve (2010): Cloud Computing – Der Markt in Deutschland 2010-2015. Experton Group, Oktober 2010.
9. Diese These wird auch durch weitere Analysen gestützt. In einer Umfrage der Computerwoche vom August 2010 gaben knapp 85 Prozent der Befragten gaben an, dass sie sich mit dem Thema Cloud Computing auseinandersetzen. Knapp 30 Prozent nutzen bereits Cloud-Services. Lediglich 15 Prozent sprachen sich gegen den Einsatz von Cloud-Services. Vgl. Hackmann, Joachim (2010): CW-Umfrage zum Cloud Computing - User misstrauen Amazon und Google. URL: http://www.computerwoche.de/1938019 (:20.08.2010)
10. Quelle: IDC eXchange, „IDC's New IT Cloud-Services Forecast: 2009-2013," (http://blogs.idc.com/ie/?p=543), October 2009
11. IDC: Worldwide Software as a Service 2010-2014 Forecast: Software will Never Be the Same, June 2010

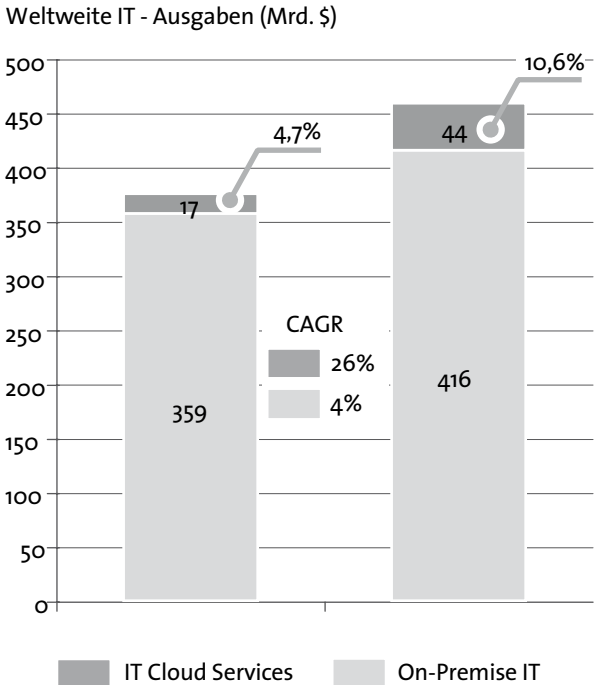


Abbildung 7: Ausgaben für Public Cloud Computing 2009-2013

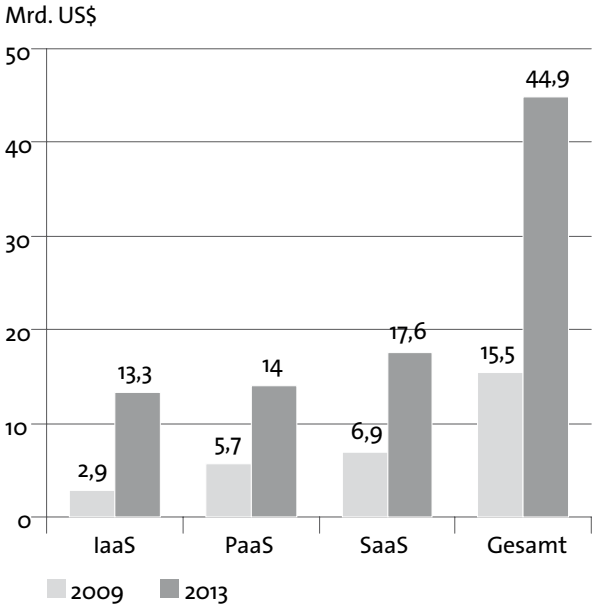


Abbildung 8: Entwicklung des weltweiten Cloud-Marktes 2009-2014

1.6 Einsatzszenarien

Die Palette möglicher Einsatzszenarien für Cloud Computing ist breit.[12]

Häufig greifen Nutzer auf einfache Infrastruktur-Dienste wie Computing-Services und Speicherdienste zurück, die vielfältig eingesetzt werden können, beispielsweise

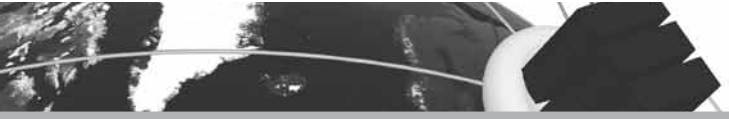
- für Test- und Entwicklungsszenarien,
- als Infrastruktur-Puffer für hohe Rechenlasten oder
- für rechenintensive Services beispielsweise im High Performance Computing.

Die Art der Services, ihr Standardisierungsgrad, ihre Bedeutung für den Kunden und die Struktur des nutzenden Unternehmens sind die wichtigsten Faktoren, die sich auf Einsatzszenarien auswirken.

Cloud Computing wird beispielsweise ergänzend zur bestehenden IT im täglichen Geschäft eingesetzt. Für den Nutzer stehen dann die speziellen Eigenschaften der in einer Cloud produzierten IT-Services wie z. B. die schnelle und flexible Verfügbarkeit der Ressourcen sowie deren dynamische Erweiterbarkeit im Vordergrund. Dies bietet Unternehmen die Möglichkeit, bestehende Lastspitzen gezielt abzufedern. Das Vorhalten kaum genutzter Ressourcen entfällt, und die Last der Abfederung trägt der Provider. Besonders interessant ist ein solches Mieten von Infrastruktur-Ressourcen für Start-ups oder Entwickler, die über keine eigene Infrastruktur verfügen. Dann wird Cloud Computing sogar zu einem Mittel, Business ohne eigenes Risiko zu ermöglichen.

Der schnelle Einstieg in neue Unternehmensfelder oder Märkte markiert ein weiteres Szenario, in dem Cloud Computing seine Vorzüge zur Geltung bringt. IT-Services aus einer Cloud stehen schnell zur Verfügung, so dass Geschäftsideen zügig umgesetzt werden können. Das verschafft den Nutzern einen klaren Geschwindigkeitsvorteil beim Eintritt in neue Märkte und Geschäftsfelder.

12. Konkrete Anwendungsszenarien werden auf dem Cloud-Portal des BITKOM www.cloud-practice.de vorgestellt.



Es wird erstmals möglich, neue geschäftliche Optionen dynamisch zu testen.

Weiterhin ist die Reduktion von Entwicklungszeiten ein häufiges Argument für Cloud-Computing. Entwickler testen zunehmend ihre neuen Applikationen auf Service-Plattformen und kommen durch den kurzfristigen Zugriff auf nahezu unbegrenzte Ressourcen schneller zu fertigen vermarktbaren Produkten.

Ein Spezialfall für ein solches Vorgehen können IT-Projekte größerer Unternehmen sein, die kurzfristig Ressourcen benötigen.

Über den (einfachen) operativen Einsatz hinaus kann Cloud Computing auch die IT-Strategie eines Unternehmens deutlich beeinflussen. Neben dem Einsatz von Cloud-Services als weitere Option gegenüber dem klassischen Outsourcing könnte beispielsweise auch die Disaster-Recovery-Strategie des Unternehmens durch Cloud-Archiving-Services ergänzt werden. Der Wandel könnte bis zur kompletten Ablösung der ursprünglichen Speichersysteme fortgeführt werden.

Bestehen noch keine unternehmenseigenen IT-Strukturen, so bieten Cloud-Services bereits heute eine Alternative zum Eigenbetrieb bzw. zum klassischen Outsourcing.

Besondere Bedeutung könnte Cloud Computing für Desktop-Services gewinnen: Via Cloud Computing werden Arbeitsplatz-Systeme situativ an die aktuellen Notwendigkeiten des Nutzers angepasst. Da die Anwendungen und Daten auf Medien in der Cloud vorgehalten werden, ist der Defekt eines portablen Endgeräts unbedeutend.

1.7 Management-Aufgaben bei der Einsatzvorbereitung und Nutzung von Cloud-Computing-Services

Die Vorteile, die sich aus Cloud Computing ergeben, sind sehr vielversprechend. Daher wird es in den meisten Unternehmen zu einer Nutzung von Cloud Computing kommen. Die Frage wird sein, wie diese Nutzung aussehen wird. Wird es zu Insellösungen in einzelnen Fachbereichen oder in der IT kommen, oder wird Cloud Computing strategisch im Unternehmen positioniert und angegangen?

Eine konkrete Gefahr ist die Entstehung von ungesteuerter und unkontrollierter Nutzung von Angeboten aus dem Internet. Einige Beispiele sollen das illustrieren:

- Die Nutzung von Services eines nicht vertrauenswürdigen Providers kann zu Verlust von Unternehmensgeheimnissen oder zu Missbrauch von Endkunden-Daten führen.
- Fehlende Kenntnisse im Bereich Compliance können zu strafrechtlichen Maßnahmen und Strafzahlungen führen.
- Fehlende technische Kenntnisse können dazu führen, dass verschiedene Services genutzt werden, die am Ende wieder nur mit sehr großem Aufwand in die Unternehmenslandschaft integrierbar sind.
- Des Weiteren haben viele Unternehmen in den letzten Jahren Projekte zur Konsolidierung von Hardware und Applikationen gestartet, die unter Umständen durch eine ungesteuerte Cloud-Computing-Nutzung torpediert werden.

Der Grund, warum diese Gefahren sehr real sind, ist die einfache Nutzung von Cloud-Computing-Angeboten. Jeder, egal ob aus IT oder aus den Fachbereichen, kann mit ein paar Klicks Services aus dem Internet nutzen. Jedoch ist nicht in jedem Fachbereich oder in der IT die benötigte Expertise zu rechtlichen und sicherheitstechnischen Aspekten vorhanden. Daher gilt es, eine ungesteuerte und unkontrollierte Nutzung im Unternehmen zu vermeiden.

Es ist deshalb zwingend notwendig, dass sich Unternehmensführung, Fachbereiche und IT gemeinsam mit dem Cloud Computing auseinandersetzen und eine konkrete Einsatz-Strategie entwickeln.

Hierzu sind Untersuchungen zu vielen Fragestellungen unabdingbar, z. B.:

- Welche Prozesse existieren im Unternehmen und welche können teilweise oder komplett in die Cloud gelegt werden?

- Welche Daten nutzt das Unternehmen und wie lassen sich diese in Bezug auf Sicherheit und Geheimhaltung klassifizieren?
- Welche Applikationen sind im Einsatz? Wo können sinnvoll existierende Applikationen durch Cloud-Lösungen ersetzt werden bzw. welche geplanten Applikationen lassen sich durch Cloud-Angebote realisieren?
- Welche Plattformen werden zur Applikationsentwicklung genutzt? Sollen in der Zukunft auch Applikationen „cloud-fertig" entwickelt werden, d. h. möglicherweise ist ein Wechsel der Plattform erforderlich?
- Welche Infrastruktur ist im Einsatz und wie kann diese sinnvoll durch die Cloud ergänzt werden?

Der Ist-Zustand sollte vollständig erfasst werden, um auf dieser Basis ein Zielbild zu erstellen, wie die IT-Landschaft des Unternehmens unter Einbeziehung von Cloud-Angeboten aussehen soll. Cloud Computing wird somit zu einem wichtigen Aspekt in der IT-Strategie eines Unternehmens. Das Zielbild kann dann auch von juristischer Seite vorab geprüft werden, bevor es zur konkreten Umsetzung kommt, d. h. mögliche Risiken in Bezug auf Compliance und Datensicherheit werden frühzeitig erkannt (vgl. Abbildung 9).

Mit einem solchen Bild vor Augen lassen sich Schritte festlegen (z. B. Durchführung von Transitionsprojekten), die in einer vorab definierten Zeit zum Ziel führen. Hier können durch regelmäßige Überprüfungen die Fortschritte überwacht werden.

Zusätzlich muss die Unternehmensführung veranlassen, dass allgemeine Entscheidungen und Vorbereitungen in Bezug auf den möglichen Einkauf von Cloud-Computing-Angeboten getroffen werden:

- Welche rechtlichen Aspekte und Service Level Agreements müssen von Cloud-Anbietern angeboten werden, damit das Unternehmen diese berücksichtigen kann?
- Gibt es eine Liste von bevorzugten Cloud-Anbietern, welche beim Einkauf berücksichtigt werden sollte?
- Wie kann der existierende Procurement-Prozess im Unternehmen erweitert werden, so dass Cloud-Angebote flexibel und effektiv zentral eingekauft werden können?

Dies ermöglicht die Schaffung eines Rahmenwerks zur allgemeinen Nutzung von Cloud-Angeboten in einem Unternehmen. Neben der Schaffung ist auch die Kontrolle der Einhaltung wichtig. So können technische Monitoring-Maßnahmen (Überwachung des IP-Verkehrs) oder

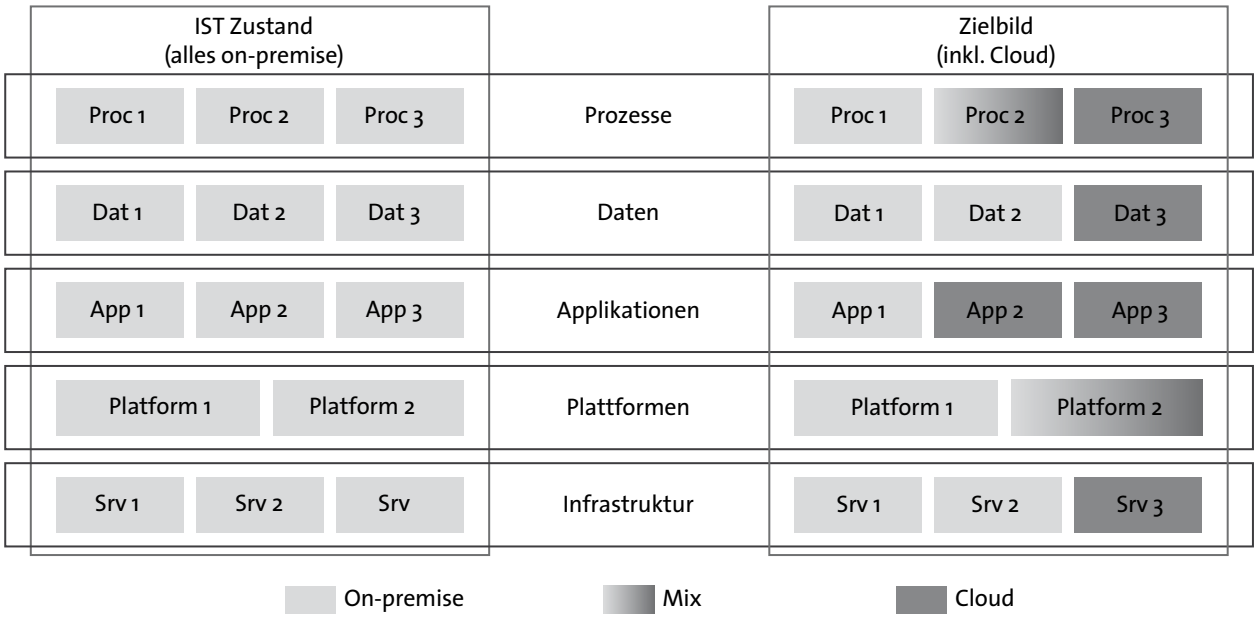
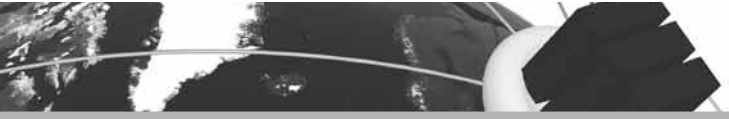


Abbildung 9: Strategieentwicklung unter Einbeziehung aller Beteiligten



regelmäßige Audits helfen, unerwünschte Cloud-Nutzung im Unternehmen zu entdecken und zu unterbinden.

Ein weiterer wichtiger Aspekt ist die Sensibilisierung der Mitarbeiter sowohl bezüglich der Vorteile, die Cloud mit sich bringen kann, als auch der möglichen Risiken. Ein Kommunikations- und ggf. Trainingsplan sollte somit Bestandteil einer Cloud-Strategie eines Unternehmens sein.

Zusammenfassend gilt: Ein von der Unternehmensführung gesteuerter und geförderter Umgang mit Cloud Computing hilft, die Vorteile zu realisieren und die Risiken zu minimieren.

1.8 Business-Modelle, Wertschöpfungsketten und -netze

Die klassische Wertschöpfungskette der IT-Dienstleistungen, die sich von der Beratung über das Design, der Implementierung und des Betriebs von Lösungen und IT-Infrastrukturen bis hin zur Wartung der Anwendungs- und IT-Landschaft erstreckt, erfährt durch die Spielarten des Cloud Computings (vgl. Abbildung 10) eine deutliche Veränderung. Cloud Computing eröffnet neue Möglichkeiten zur Erstellung und zum Bezug von IT-basierten Dienstleistungen, erhöht aber gleichzeitig die Komplexität, mit der die Bezieher der Leistungen umzugehen haben.

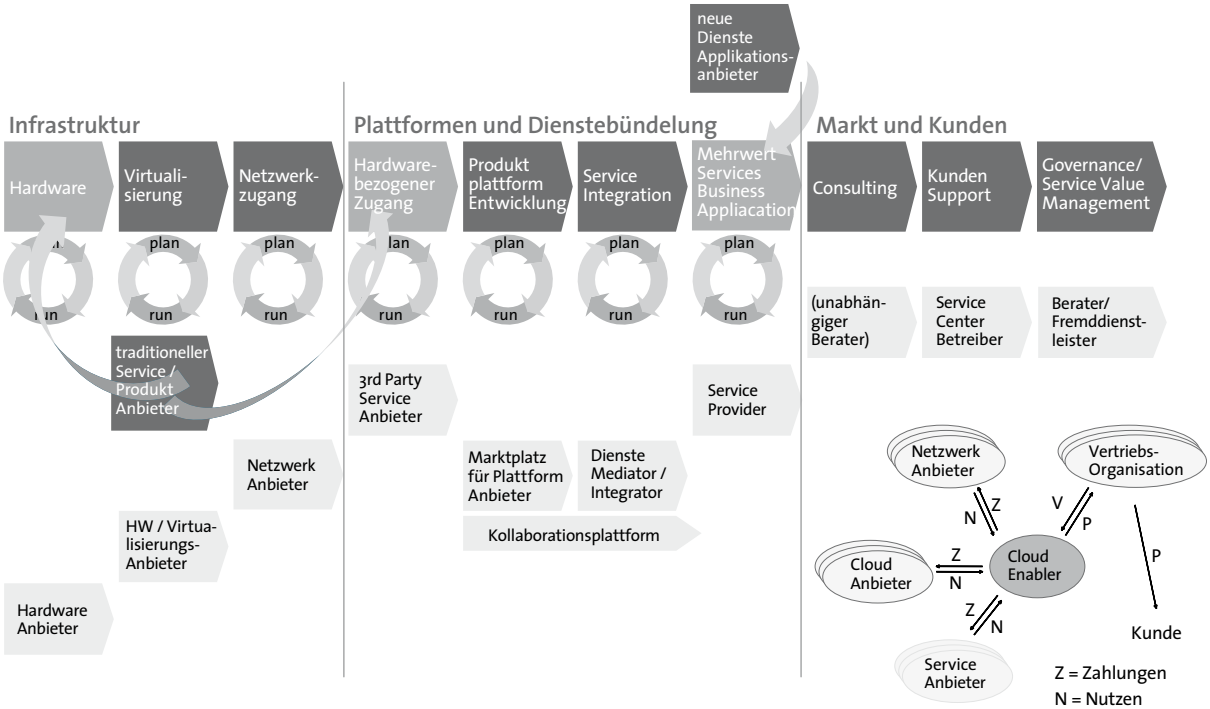
Auf Anbieterseite verlagert sich die Wertschöpfung bei der Erstellung von Business Applications von der Programmierung und Customisierung von Anwendungen hin zu Komposition und Konfiguration von Services. Gegenüber dem Betrieb von IT-Infrastrukturen wird das Management dieser zu Applikationen gebündelten Services immer wichtiger und werthaltiger.

Nutzer von Leistungen können gleichzeitig Anbieter von IT-basierten Services werden und sich damit neue Geschäftsfelder erschließen, weil es deutlich leichter und billiger wird, Spezialkompetenzen weltweit verfügbar zu machen. Prominentestes Beispiel ist wohl Amazon, das seine Kompetenzen bei Design und Betrieb massiver IT-Infrastrukturen seit längerer Zeit erfolgreich in der Form von Amazon Web Services auch extern vermarktet.

So zwingen neue Player im Markt die etablierten Anbieter, über ihre Position in der Wertschöpfungskette und die vom Kunden wahrgenommenen und honorierten Leistungen neu nachzudenken.

Cloud-Computing-Technologien bewirken, dass die bisher im Wesentlichen lineare Wertschöpfungskette bei IT-Dienstleistungen aufbricht. So können z.B. durch Technologien zur dynamischen Lastverteilung Nutzer von Infrastructure as a Service Leistungen auch zu Anbietern dieser Leistungen werden. Ebenso lassen sich auch bisher nur intern genutzte Funktionalitäten relativ einfach im Software-as-a-Service-Modell externen Nutzern zur Verfügung stellen. Die steigende Zahl von Anbietern hochstandardisierter Funktionen erhöht den Preisdruck und unter Umständen auch die Flexibilität für einen Wechsel der Anbieter. In Summe entsteht ein innovatives, dynamisches Netzwerk von Anbietern und Konsumenten von IT Dienstleistungen (vgl. Abbildung 10).

Die Grundlage für erfolgreiche Geschäftsmodelle in diesem Umfeld bilden partnerschaftliche Beziehungsgeflechte auf der Basis von Vertrauen in Netzwerken. Dies ist zwar schon bisher so gewesen, mit der Dynamik des globalen Marktes für Cloud Computing kommt aber eine neue Qualität in dieses Beziehungsgeflecht. Vertrauen kann nicht mehr langsam wachsen und auf die Beziehung zwischen oft auch persönlich bekannten Geschäftspartnern bauen. Transparenz in allen Aspekten eines Cloud-Leistungsangebots, qualifizierte Beratung und anerkannte Zertifikate für bestimmte Leistungsmerkmale helfen, dass Vertrauen schneller aufgebaut werden kann. Dies muss auch unterstützt und ergänzt werden durch neue technische Hilfsmittel, vertragliche Konstrukte (vgl. Kapitel 2) und vielleicht auch rechtliche Rahmenbedingungen.



Quelle: Leimeister / Krcmar,
vgl. http://bicc-net.de/news/bicc-open-labs-tum-kooperationsmoglichkeiten-mit-der-tum-forschung/20100323_Leimeister.pdf

Abbildung 10: Sich entwickelndes Cloud-Ökosystem

1.9 Cloud Computing – die Erfolgsfaktoren

Das fehlende Vertrauen in Datenschutz- und Datensicherheits-Konzepte sowie die im Einzelfall unklare rechtliche Situation sind derzeit die größten Hemmnisse für eine schnellere Marktentwicklung in diesem Segment. Ergänzend wird auch die Befürchtung formuliert, in zu große Abhängigkeit von Dienstleistern zu geraten oder die Kontrolle über Daten und Services zu verlieren.

In eine ähnliche Richtung zielen Bedenken bezüglich der Verfügbarkeit von Cloud-Angeboten oder – als schwächere Variante – der Performanz der genutzten Dienste. Auch mögliche Probleme bei der Integration oder das Unterlaufen von Governance-Anforderungen sowie fehlende SLA (vgl. Abschnitt 2.4.4) und adäquate Haftungszusagen (vgl. Kapitel 2) sind Hemmnisse für eine Adaption.

Die Akzeptanz von Cloud-Computing-Angeboten bei Anwendern setzt voraus, dass die Anbieter deren Vorzüge in Referenzprojekten dem Markt beweisen. In der Abbildung 11 sind die wesentlichen Erfolgsfaktoren für Cloud Computing aus der Sicht des CIO zusammengestellt[13].

Hieraus wird ersichtlich, dass viele der Sorgen des CIO mit juristischen Fragestellungen einhergehen. Zu den Erfolgsfaktoren zählen aber auch

- die Interoperabilität zwischen den Cloud-Services (Unabhängigkeit von einem Anbieter),
- die Ausgewogenheit zwischen Individualität und hoher Standardisierung
- organisatorische Voraussetzungen im Unternehmen.

13. Quelle: CIO Research, Vgl.: http://www.cio.de/knowledgecenter/netzwerk/861652/index2.html (Abruf am 24.09.10)

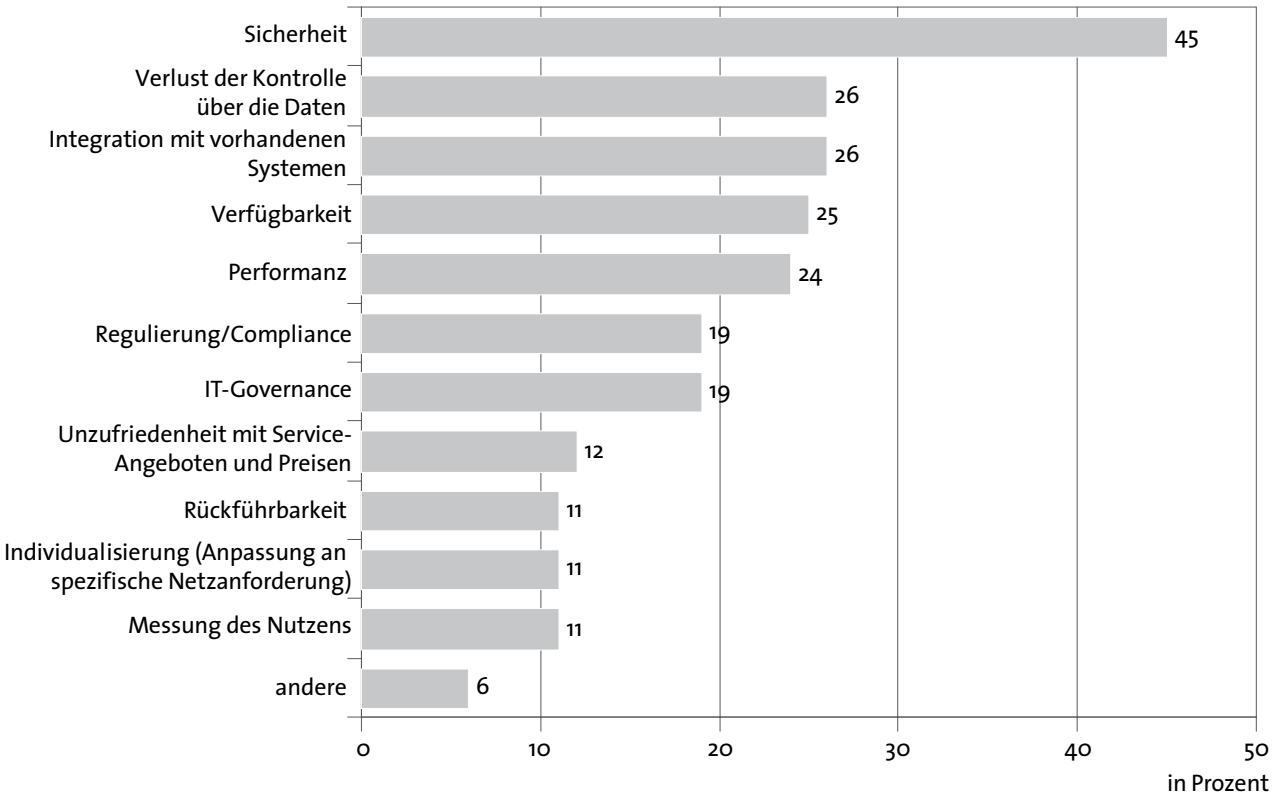


Abbildung 11: Erfolgsfaktoren von Cloud Computing aus CIO-Sicht

1.9.1 Sicherheit und Kontrollhoheit über die Daten

Die Gewährleistung der von Unternehmen geforderten Sicherheit im umfassenden Sinne ist entscheidend für die Akzeptanz von Cloud Computing. Dabei geht es vorrangig um den Schutz personenbezogener Daten, der Unternehmensdaten sowie der unterstützten Geschäftsprozesse (vgl. dazu Kapitel 3).

Der Dienstleister muss die Datenhaltung in seiner Cloud-Infrastruktur auf dem Stand der Technik gewährleisten, also die Kundendaten gegen physikalische und logische Fehler sowie gegen unbefugten Zugriff absichern.

Die Tatsache, dass der physische Zugriff auf die Datenbestände beim Einsatz von Cloud Computing nicht komplett unter eigener Kontrolle steht, führt bei IT-Entscheidern nicht selten zu Unbehagen. Die Bedenken können reduziert werden durch

- Transparenz,
- SLA sowie
- technische Lösungen und
- persönliche Ansprechpartner auf Anbieterseite.

Cloud-Anbieter und -Nutzer haben juristische Vorgaben zu beachten, die den Transfer von Daten aus dem Rechtsraum Deutschlands bzw. der EU einschränken (vgl. dazu Kapitel 2).

1.9.2 Verfügbarkeit und Performanz

Die Qualität eines Service spielt eine entscheidende Rolle, damit Cloud Computing als Sourcing-Alternative im Markt akzeptiert wird. Dabei müssen sich Cloud-Services am Qualitätsniveau lokal installierter Anwendungen messen

lassen. Wichtig für die Diskussion der Qualität sind die technischen Faktoren Performanz und Verfügbarkeit.

Um den IT-Service an den Belangen des Geschäfts zu orientieren, sollte für Cloud-Services die Vereinbarung von Service Levels möglich sein. Sie garantieren die Verfügbarkeit des Service entsprechend seiner Bedeutung für das Geschäft.

1.9.3 Rückführbarkeit

Im Vergleich zu bisherigen IT-Infrastrukturen wird bei Cloud-Computing-Angeboten ein umfassender Teil einer IT-Dienstleistung durch einen einzelnen Anbieter erbracht. Eine gewisse Abhängigkeit eines Nutzers von diesem Anbieter besteht also – insbesondere dann, wenn Anwendungen in der Cloud anbieterspezifische Schnittstellen zur Kontrolle der Cloud-Ressourcen nutzen.

Bei der Bewertung der Cloud-Angebote müssen Unternehmen daher immer die technische und ökonomische Dimension einer Rückführung berücksichtigen.

Offenheit und Standardisierung von Schnittstellen senken die Barriere für die Verwendung von Cloud-Services im Unternehmen.

1.9.4 Integrationsfähigkeit

Für den Business-Einsatz von Cloud Computing zählt, ob und wie sich angebotene Cloud-Services miteinander und in bestehende IT-Systeme integrieren lassen. Der Nutzer erwartet die ganzheitliche, performante und reibungsfreie Unterstützung seiner Geschäftsprozesse.

Technisch werden sich Cloud-Systeme problemlos koppeln lassen, wenn Standardschnittstellen vorhanden sind. Größere Herausforderungen stellen die Integration von Geschäftsprozessen bzw. die Integration hochflexibler Cloud-Dienste mit statischen klassischen Systemen dar.

Die Bedeutung der Integration zeigt sich, wenn die Applikationen Geschäftsprozesse unterstützen. Übernehmen Cloud-Services die Verantwortung für einen Geschäftsprozess oder -teilprozess, so müssen bereits im Vorfeld die Risiken seriös abgeschätzt werden. Die Verantwortung für die Prozessintegration trägt bei Public-Cloud-Services der Nutzer.

Schlussendlich muss der Einsatz von Cloud Computing organisatorisch im Unternehmen verankert sein.

1.9.5 Zufriedenheit mit Service-Angeboten und Preisen

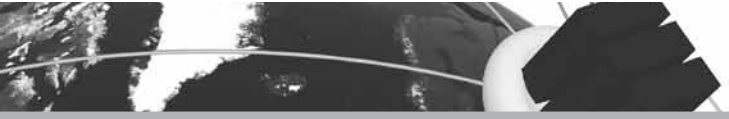
Ein weiterer Erfolgsfaktor für die Nutzung von Cloud-Services besteht in der Transparenz der Services. Dabei interessiert den Nutzer die Verteilung der Kosten auf die bezogenen Services sowie auf die den Service nutzenden Unternehmenseinheiten.

Public Cloud-Services werden zurzeit von den Anbietern unterschiedlich abgerechnet. In der Regel wird in Abhängigkeit von der Nutzung abgerechnet. Dabei hat sich für Infrastruktur- und Plattform-Angebote (IaaS, PaaS) eine ähnliche Struktur der Preisgestaltung herausgebildet. Diese ist jedoch durch die verschiedenen Komponenten[14] zumeist sehr komplex.

Die Zufriedenheit mit den Service-Angeboten und Preisen wird sich erhöhen, wenn Werkzeuge zum Monitoring und Reporting sowie für die Kostenermittlung zur Verfügung stehen. Diese ermöglichen es, Kostentreiber und Einsparpotenziale zu identifizieren.

Bei SaaS-Angeboten haben sich zum Teil sehr spezifische Abrechnungsmodelle etabliert, die generell nur schwer miteinander vergleichbar sind. Je stärker ein Geschäftsprozess standardisiert ist, desto besser ist die Vergleichbarkeit der Angebote anhand von angebotenen SLAs und Preisen.

14. CPU, Speicher, Datenverkehr, Nutzung von Schnittstellen



2 Vertragliche Regelungen für Cloud Computing

- Verträge definieren die zu erbringenden Leistungen und die wechselseitigen Ansprüche der Vertragspartner. Sie müssen alle Vereinbarungen enthalten, die erforderlich sind, um Cloud Computing in dem gesetzlich zulässigen Rahmen durchzuführen. Dazu gehören auch Regelungen für den Datenschutz (Kapitel 4), IT-Security (Kapitel 5) und Compliance (Kapitel 6).

- Für die Steuerung und Durchführung von Cloud Computing ist schon die Anzahl der Vertragspartner entscheidend: Ein Generalunternehmer vereinfacht die Vertragsbeziehungen und reduziert die Handlungsoptionen des Kunden. Verträge des Kunden mit mehreren Vertragspartnern für einzelne Cloud-Computing-Leistungen bedeuten mehr Komplexität und Steuerungsaufwand für den Kunden, sie können gleichzeitig größere Flexibilität für die Leistungen schaffen.

- Unerlässlich ist die klare Vereinbarung des für den Cloud Computing-Vertrag geltenden Rechts. Ausländische Rechtsordnungen sehen gesetzliche Regelungen und vertragliche Gestaltungen vor, die teilweise erheblich von deutschem Verständnis abweichen. Auch Konfliktlösungsmechanismen und Gerichtsstand oder Schiedsgerichtsvereinbarungen sind daher im Cloud-Computing-Vertrag zu vereinbaren.

- Die Leistungsbeschreibung ist zentraler Inhalt eines Cloud-Computing-Vertrags. Die Art der vereinbarten Leistungen entscheidet darüber, welcher gesetzliche Vertragstyp mit seinen gesetzlichen Regelungen zur Anwendung kommt. Einzelne Cloud-Computing-Leistungen können insbesondere miet-, dienst-, werk- oder leihvertraglichen Charakter haben. Im Cloud-Computing-Vertrag werden oft Leistungen unterschiedlicher gesetzlicher Vertragstypen kombiniert. Zwar wird ein Schwerpunkt oft auf mietvertraglichen Leistungen liegen, entscheidend sind aber stets die Arten und Charakteristika der konkret vereinbarten Leistungen. Gewährleistungsvorschriften gesetzlicher Vertragstypen sind unterschiedlich und für Cloud Computing in der Praxis oft wenig tauglich.

- Eine Lösung für die Beschreibung der vertraglichen Leistungen und die Folgen unzureichender Leistungen bieten Service Level Agreements (SLA), die Cloud-Computing-Leistungen mit ihren wichtigen Kriterien definieren und Folgen für Unterschreitungen vereinbarter Kriterien regeln.

- Anbieter und Kunden müssen für die einzusetzende Software über die notwendigen Nutzungsrechte für Cloud Computing verfügen. Sie müssen für den Einsatz in allen Ländern vorhanden sein, in denen die Leistungen zur Verfügung gestellt werden. Der Cloud-Anbieter muss über die notwendigen Rechte verfügen, um die Leistungen den Kunden bereitzustellen.

- Change Request-Verfahren sollten im Cloud-Computing-Vertrag ebenso vereinbart werden wie Regelungen zur Governance für die Cloud-Computing-Leistungen.

- Die Vergütung für Cloud-Computing-Leistungen wird oft rein nutzungsabhängig verstanden. Die denkbaren Vergütungs- und Abrechnungsmodelle beinhalten aber weit größere Spielräume für angemessene Lösungen aus Sicht von Kunde und Anbieter.

- Bei Einbindung von Subunternehmern des Anbieters sind die notwendigen Regelungen für Governance und Notfall-Management auch für die Subunternehmer detailliert zu vereinbaren. Das gilt umso mehr für Vereinbarungen zum Datenschutz.

- Für die Beendigung der Leistungen sollte der Cloud-Computing-Vertrag klare Regelungen für Kündigungen und das Exit-Management enthalten.

2.1 Verträge als Definitionen von Leistungen und Pflichten

Ziel von Verträgen ist, Leistungen und Ansprüche von Kunde und Anbieter zu definieren und zu dokumentieren. Gesetzliche Vertragsmodelle spezifisch für Cloud Computing existieren nicht, auch keine Standards für Verträge oder übliche Regelungen, die sich am Markt bereits durchgesetzt haben.

Die konkreten vertraglichen Vereinbarungen bilden daher die entscheidende Grundlage für die Frage, in welchem Umfang die Nutzung und Erbringung von Cloud-Computing-Leistungen rechtlich zulässig ist. In dem gesetzlich vorgegebenen Rahmen können und müssen die Interessen und Leistungen beider Vertragspartner in geeignete Vereinbarungen umgesetzt werden. Diese Verträge für Cloud Computing sind juristisch auch im deutschen Recht gut darstellbar.

Bedarfsanalyse des Kunden als Ausgangspunkt

Vor diesem Hintergrund ist es besonders wichtig, alle fachlichen und rechtlichen Anforderungen auch im Vertrag abzubilden. Dafür geben die im Kapitel 2 angesprochenen vertraglichen Aspekte eine Hilfestellung, die jedoch nicht beanspruchen, eine abschließende Checkliste für eine Vertragserstellung darzustellen.

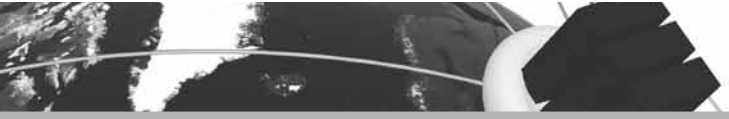
Die in den Kapiteln 3 und 4 angesprochenen Themen sowie die branchenspezifischen oder auch gesetzlichen Sonderregelungen sind je nach Bedarf zusätzlich zu identifizieren und in dem Vertrag abzubilden. Sie werden in den entsprechenden Kapiteln näher eingegrenzt. Besondere Anforderungen resultieren aus den Datenschutzgesetzen, soweit personenbezogene Daten (vgl. Abschnitt 3.2.2) durch Cloud Computing verarbeitet werden sollen. Eine differenzierte Betrachtung lohnt schon wegen der zusätzlichen Anforderungen aus dem Datenschutz. Andere Anforderungen an die IT-Sicherheit können sich wiederum aus dem Sicherheitsbedürfnis und Geheimhaltungsinteresse der Vertragspartner ergeben. Auch existieren für viele Branchen besondere gesetzliche Regelungen, die Einfluss auf die Ausgestaltung der Cloud-Computing-Leistungen haben, hier allerdings nicht näher dargestellt werden können.

Zunächst bedarf es demzufolge einer Bedarfsanalyse.

Die geeigneten Vertragskonstruktionen und Vertragsinhalte können nur anhand der konkreten Ausgangssituation des Kunden und der von ihm gewünschten Leistungen bestimmt werden. Dies erscheint vielleicht banal, wird aber gerade in dem vielseitigen und dynamischen Bereich des Cloud Computings in der Praxis vernachlässigt.[15]

Im ersten Schritt sind die fachlichen Anforderungen anhand von Soll-Kriterien zu beschreiben. Welche Leistungen sollen aus technischer, prozessökonomischer und wirtschaftlicher Sicht bezogen werden, um betriebliche Prozesse zu beschleunigen, qualitativ zu verbessern oder ökonomischer zu gestalten?

15. Bei der Erstellung der Bedarfsanalyse können Fachabteilungen, Rechtsabteilung und Verbände (etwa Berufsverband für spezifische Anforderungen) wertvolle Hinweise liefern.



Die Inhalte sind vollständig darzustellen und soweit notwendig, zu priorisieren, etwa in einer Bewertungsmatrix. Technische „Muss-Kriterien“ sowie auch branchenspezifische rechtliche „Muss-Kriterien“ (etwa aus Spezialgesetzen) stellen „K.O. Kriterien“ dar. Ergebnis dieser Bedarfsanalyse ist eine Zusammenstellung der Anforderungen als Grundlage zur Auswahl geeigneter Angebote. Zu diesem Zeitpunkt ist grundsätzlich noch keine Festlegung auf eine bestimmte Form von Cloud Computing (vgl. Tabelle 2) erforderlich.

So vielgestaltig und unterschiedlich wie der Bedarf des Kunden sind die Anforderungen. Zur Veranschaulichung einige Beispiele:

- Ein Kunde will seine eigene Softwareentwicklung auf einer virtuellen Plattform mit dort bereitgestellter Programmierumgebung mit entsprechendem Speicherplatz durchführen. Seine Priorität ist eine kostengünstige Lösung, nicht unbedingt gesteigerte Sicherheitsanforderungen.
- Ein anderer Kunde möchte das Kundenbeziehungs-Management seiner fünf Vertriebsorganisationen zentral verwalten. Für ihn hat der Schutz vor unberechtigtem Zugriff auf diese Daten, etwa durch seine Marktkonkurrenten, höchste Priorität.
- Ein anderer Kunde plant, technische Simulationen kostengünstiger durchzuführen. Es handelt sich um komplexe Berechnungen, die eine hohe Rechenleistung beanspruchen. Personenbezogene Daten sind nicht betroffen.

Die Ergebnisse der Analyse technischer, fachlicher und kaufmännischer Anforderungen sind auch Grundlage für die Ermittlung rechtlich zwingend notwendiger oder gewünschter Inhalte vertraglicher Regelungen. Oft sind ergänzende Anforderungen aus bereits bestehenden Verträgen des Kunden mit anderen Vertragspartnern einzubeziehen, auch für die Integration der Cloud-Computing-Leistungen in die IT-Umgebung des Kunden.

Ziel des Kapitels

Ziel des Kapitels 2 ist eine Hilfestellung für die praxisgerechte Regelung der Rechte und Pflichten beider Vertragspartner. Meist sind unterschiedliche Leistungen und Leistungsarten[16] abzubilden. Die Darstellung soll folgende Fragen beantworten, die in einem Cloud-Computing-Vertrag zu regeln sind. Die Ziffern in den Klammern verweisen auf die entsprechenden Unterkapitel.

- Wie viele Vertragsparteien gibt es und welche Leistungen übernehmen sie? (Abschnitte 2.2, 2.4, 2.10)
- Welches nationale Recht gilt für welche Rechte und Pflichten? (Abschnitt 2.3)
- Wer hat Zugriff auf welche Leistungen und welche Daten? In welchem Land werden Leistungen erbracht und die Daten gespeichert? (Abschnitt 2.4)
- Wie werden Änderungen im Bedarf umgesetzt und was geschieht bei Abweichungen in der Vertragserfüllung? (Abschnitte 2.5, 2.6)
- Wie wird die Vergütung für welche Leistungen berechnet? (Abschnitt 2.9)
- Wie werden spezifische rechtliche Anforderungen und interne Vorgaben des Kunden umgesetzt? (Abschnitt 2.8).

Vielfalt der Kundenanforderungen und Eingrenzungen

Die Fragestellungen für einen Cloud-Computing-Vertrag werden in diesem Leitfaden nach deutschem Recht dargestellt. Das gilt auch für die Ausgangsfrage, ob deutsches Recht anzuwenden ist.

Viele Regelungen werden auch in Cloud-Computing-Verträgen durch Standardtexte getroffen, die nach deutschem Recht besonderen Vorschriften für die Einbeziehung, Auslegung und Wirksamkeit unterliegen (AGB-Recht).[17]

16. Nutzung von Hardware, Plattform, Software, Schnittstellen; Anbindung an Systeme des Kunden etc.
17. Darauf kann im Folgenden aufgrund der Unterschiedlichkeit der Ausgangssituationen, Anforderungen und Lösungen nicht näher eingegangen werden.

Der Einstieg des Kunden in Cloud Computing kann unterschiedlich sein:

- Entweder sollen aus Sicht des Kunden völlig neue Leistungen erbracht oder
- zuvor durch den Kunden erbrachte Leistungen in die Cloud „ausgelagert“ werden.

Daraus können unterschiedliche Anforderungen an die Vorarbeiten bis zum Beginn der Erbringung von Cloud-Computing-Leistungen (etwa für Schnittstellen oder Migration) folgen, die vertraglich zu berücksichtigen sind. Üblicherweise sollte das Thema Betriebsübergang – anders als bei vielen Outsourcing-Vorhaben – für Cloud Computing keine Rolle spielen.[18]

Gegenstand für die folgende Darstellung vertraglicher Themen sind „klassische“ IT-Leistungen als Bereitstellung von IT-Ressourcen, Plattformen und Anwendungen. Andere Leistungen unter Einsatz von IT, etwa Telekommunikation (VoIP), erfordern zusätzliche Betrachtungen der dafür spezifischen Themen und Anforderungen.

Der Fokus der Ausführungen liegt auf Public Cloud und Cloud-Formen, die einen Anteil von Public Clouds beinhalten.[19] Bei reinen Private Clouds ausschließlich für die interne Nutzung nur eines Unternehmens stellen sich die angesprochenen Themen nicht als Neuerung dar. Demgemäß sollten die angesprochenen Themen bereits bekannt und geklärt sein.

Grundlage der Darstellung ist die im Abschnitt 1.2.1 formulierte Definition von Cloud Computing.

2.2 Anzahl der Vertragspartner

2.2.1 Zahl der Vertragspartner und Abwicklungsmodelle

Vor Aufnahme einer vertraglichen Beziehung steht notwendigerweise die Auswahl eines geeigneten Vertragspartners. Aufgrund der Vielgestaltigkeit der Kundenanforderungen im Bereich Cloud Computing und dem erklärten Ziel der flexiblen, nutzungsabhängigen und günstigen Zurverfügungstellung von IT-Leistungen werden Anbieter nur in seltenen Fällen alle Leistungen aus einer Hand erbringen können. Sind auf der Leistungsseite aber mehrere Unternehmen tätig, entsteht bereits im Vorfeld die Frage nach der für den konkreten Fall geeigneten Abwicklungsform. Da somit bereits zu Projektbeginn eine entscheidende Weichenstellung für das gesamte Cloud-Computing-Projekt erfolgt, ist es von essentieller Bedeutung, die Vorteile und Problemfelder der hier beschriebenen Abwicklungsmodelle im Auge zu behalten und bei der Entscheidung zu berücksichtigen.

2.2.2 Ein Vertragspartner – Cloud aus einer Hand

Wie bereits im vorangegangenen Abschnitt dargestellt, wird es eher der Ausnahmefall bleiben, dass ein Anbieter sämtliche vertragsrelevanten Tätigkeiten selbst erbringt. Dies wird am ehesten dann in Frage kommen, wenn Standardangebote für bestimmte Geschäftsmodelle oder Branchen im Fokus stehen oder der Anbieter z. B. aufgrund internationaler Ausrichtung die notwendige Ressourcenoptimierung bereits intern verfügt.

18. Deshalb werden rechtliche Voraussetzungen und Auswirkungen (§ 613a BGB) nicht dargestellt. Auch auf Anforderungen aus verschiedenen Betreibermodellen insbesondere für Private und Hybrid Clouds (etwa Managed Private Cloud) kann hier nicht eingegangen werden.
19. Hybrid Clouds, Anbindung von Legacy-Systemen an Public Clouds etc.

Vorteile bestehen bei diesem Modell in zumindest zweierlei Hinsicht:

- So besteht trotz gemeinsamer Ressourcennutzung eine höchstmögliche Transparenz für den Kunden, in wessen Verfügungsgewalt sich seine Daten befinden.
- Darüber hinaus reduziert sich die Komplexität der unterschiedlichen Problemfelder (Datenschutz, Compliance, etc.) ganz deutlich.

Auf der anderen Seite wird der Anbieter hier auf Kundenwünsche jenseits des angebotenen Leistungsspektrums unter Umständen nur eingeschränkt reagieren können. Da eine technische Weiterentwicklung in diesem Umfeld stets mit zusätzlichem Aufwand für den Anbieter verbunden ist[20], können sich hinsichtlich Flexibilität und Einsparpotenzial Grenzen ergeben.

2.2.3 Ein Vertragspartner – Cloud Provider als Generalunternehmer

Während das im Abschnitt 2.2.2 beschriebene Modell eher die Ausnahme darstellen dürfte, wird nachfolgend ein häufiges Szenario bildlich dargestellt: die Konstellation, in der ein Kunde in einer Vertragsbeziehung nur mit einem SaaS-Anbieter steht, der seinerseits Plattform- und Infrastrukturleistungen durch Subunternehmer in Anspruch nimmt (siehe Abschnitt 2.10). Die identische Situation liegt vor, wenn der Kunde in seinem Vertragsverhältnis mit dem SaaS-Anbieter weitere PaaS- und IaaS-Leistungen nutzen will (vgl. Abbildung 12).

Die Vorteile dieser Konstellation liegen aus rechtlicher Sicht darin, dass es trotz weitgehender Flexibilität und den damit verbundenen wirtschaftlichen Vorteilen aus Kundensicht bei einem Vertragspartner bleibt, der für die Leistungserbringung in Gänze verantwortlich ist. Auch in praktischer Hinsicht hat der Kunde hier im Idealfall nur einen Ansprechpartner, was die Abwicklung deutlich vereinfacht und entsprechendes Know-how auf Kundenseite entbehrlich macht. Allerdings muss aus Kundensicht darauf geachtet werden, dass der Anbieter notwendige vertragliche Verpflichtungen (z. B. in datenschutzrechtlicher Hinsicht) an seine Subunternehmer weitergibt und der Kunde die für ihn notwendigen Informationen und Bestätigungen hierüber erhält.

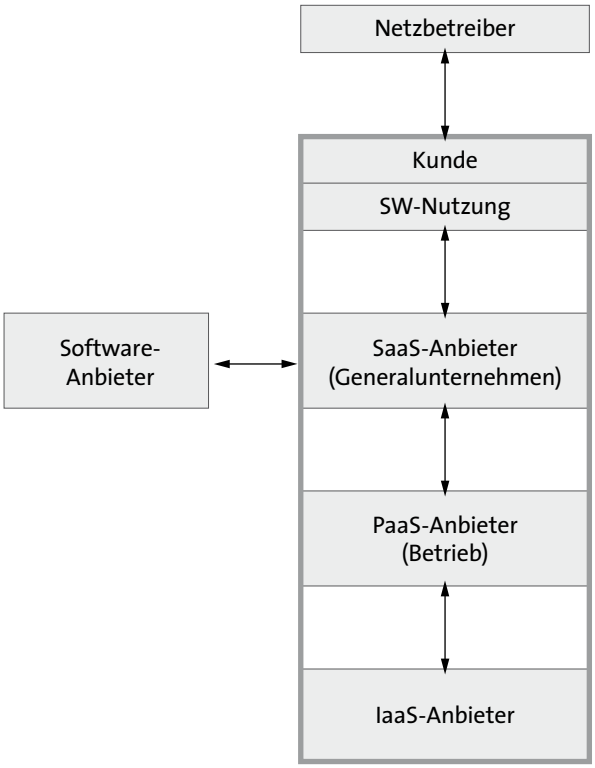


Abbildung 12: Cloud-Provider mit Subunternehmern

2.2.4 Sonderfälle PaaS und IaaS

Neben dem in Abschnitt 2.2.3 dargestellten Hauptanwendungsfall, dass ein Kunde verschiedene Cloud-Computing-Leistungen über seinen SaaS-Anbieter bezieht, ergeben sich noch folgende Sonderfälle:

- Der Kunde betreibt z.B. ein Systemhaus zur Entwicklung von Software und benötigt eine Entwicklungsumgebung. Dazu schließt der Kunde einen direkten Vertrag mit einem PaaS-Anbieter (vgl. Abbildung 13 Mitte), der seinerseits die Infrastrukturleistungen durch einen Subunternehmer in Anspruch nimmt.

20. und nicht mit dem bloßen Auswechseln eines Subunternehmers

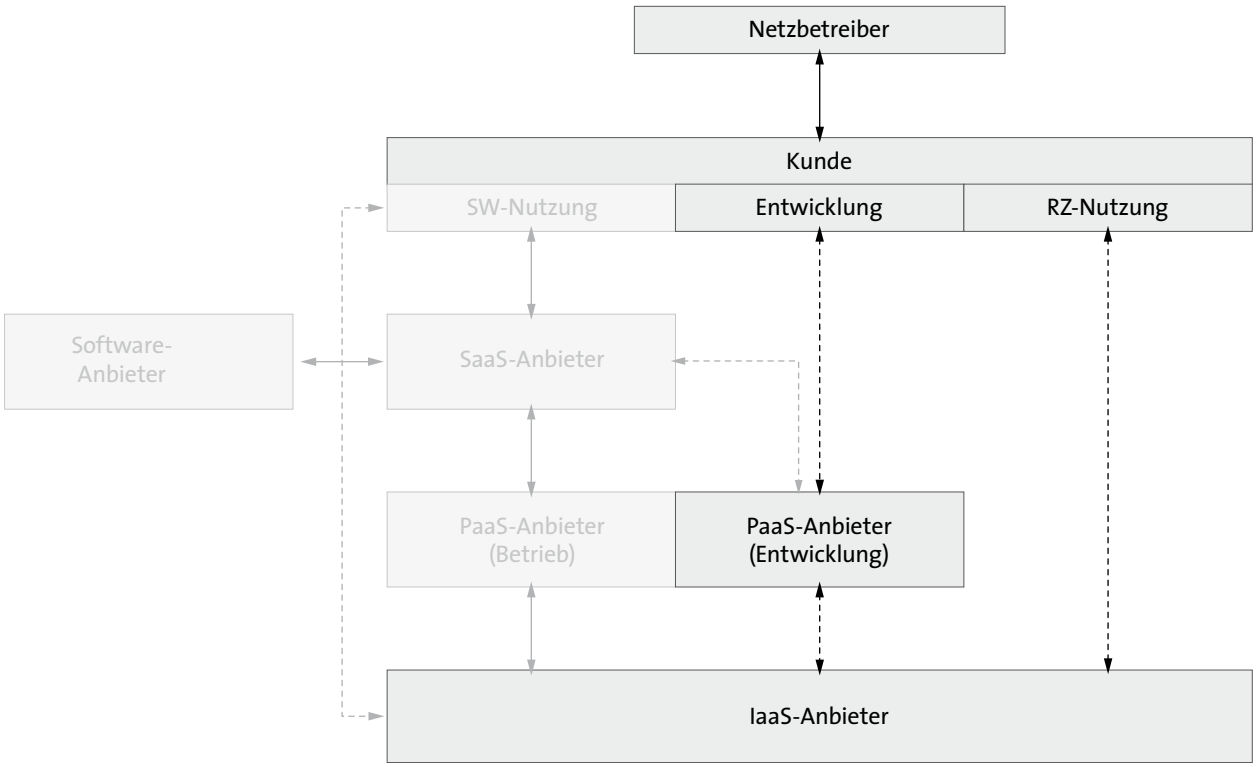


Abbildung 13: Verträge für PaaS und IaaS

In der zweiten Konstellation ist der Kunde beispielweise ein IT-Service-Provider, der sowohl eine eigene Entwicklungsumgebung als auch ein eigenes Rechenzentrum betreibt und zusätzliche Rechenkapazität nur zur Abdeckung von Spitzenzeiten benötigt. In diesem Fall schließt der Kunde den Vertrag direkt mit dem IaaS-Anbieter (vgl. Abbildung 13 rechts).

In der praktischen Durchführbarkeit sind diese Konstellationen komplexer, insbesondere in ihrer Kombination miteinander und mit SaaS. Solche Kombinationen von Leistungen und Leistungserbringern setzen spezifisches Know-how oder eingehende Beratung voraus und bergen die Gefahr, dass die Verantwortung für das Funktionieren der „Gesamtleistung" beim Kunden selbst verbleibt. Dies bezieht sich bereits auf das bloße Zusammenwirken der Teilleistungen aus technischer Sicht sowie auch darauf, dass in vertraglicher und rechtlicher Sicht keine unerwünschten Diskrepanzen auftreten. Im Extremfall können bei internationalem Bezug auch unterschiedliche Rechtsordnungen zur Anwendung kommen (vgl. Abschnitt 2.3.1).

Auf der anderen Seite bieten solche Konstellationen die größtmögliche Flexibilität für den Kunden, da er nicht auf das Angebot eines Anbieters angewiesen ist, sondern sich für das in wirtschaftlicher, technischer und rechtlicher Hinsicht „ideale" Teilangebot entscheiden kann.

2.3 Rechtswahl und Klärung unterschiedlicher Auffassungen

2.3.1 Rechtswahl

Cloud Computing macht vor nationalen Grenzen nicht halt. Im Gegenteil: Es gehört zu den Charakteristika von Cloud-Diensten, dass sie aus einem oder mehreren auch während der Leistungserbringung wechselnden Ländern erbracht werden. Selbst wenn man für die weitere Erörterung zugrunde legt, dass sowohl Anbieter als auch Kunde juristische Personen mit Sitz im Inland sind, ergeben sich daraus vielfältige Anknüpfungspunkte für unterschiedliche Rechtsordnungen.

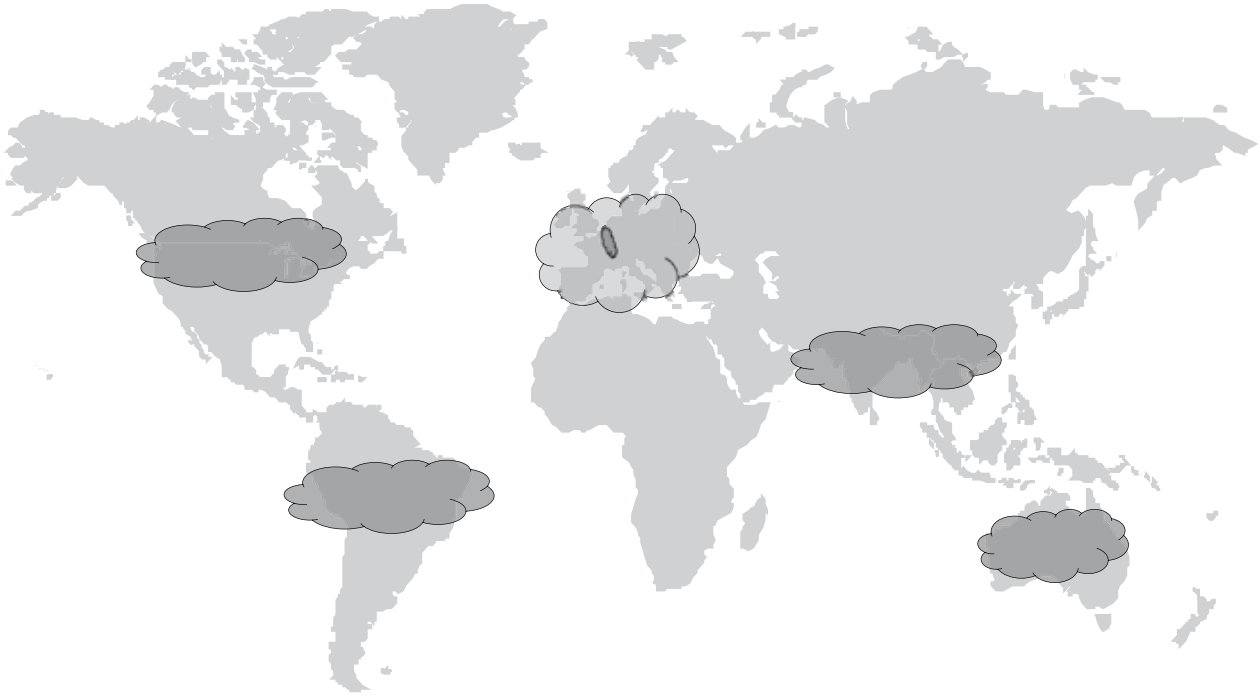


Abbildung 14: Cloud-Leistungen rund um den Globus

- Vertragliche Rechtswahl
  Wegen der möglichen Vielzahl von Rechtsordnungen, die auf diese Weise durch die Cloud-Dienste betroffen werden können, ist eine vertragliche Rechtswahl unerlässlich. Grundsätzlich sind die Parteien eines Vertrages bei der Wahl des anwendbaren Rechts frei. Ausnahmen bestehen u. a. dort, wo durch die Rechtswahl zwingende Regelungen des Rechts eines Staates nicht umgangen werden können.
  Gleichwohl ist auch für das Cloud Computing nicht jede Rechtsordnung zweckmäßig. Es besteht ein Zusammenhang zwischen anwendbarem Recht, Vertragssprache und Gerichtsstand (vgl. Abschnitt 2.3.2). Entspricht die Vertragssprache nicht der Sprache des anwendbaren Rechts, können sich Probleme bei der Auslegung rechtlicher Begriffe ergeben.[21]
  Diesem Problem kann man dadurch begegnen, dass die deutsche Vertragsversion verbindlich ist und die englische Version nur als zusätzliche Information dient. Ist dieser Weg nicht möglich, sollten bei den zentralen Begriffen zumindest in Klammern die Begriffe der anwendbaren Rechtsordnung in der Originalsprache hinzugefügt werden. Bei Verträgen in englischer Sprache und anwendbarem deutschen Recht sollten also z. B. zumindest die deutschen Rechtsbegriffe in Klammern hinter den englischen Begriffen eingefügt werden. Aus deutscher Sicht ist die vertragliche Vereinbarung deutschen Rechts ratsam.
- Keine vertragliche Rechtswahl – Rom I
  Treffen die Parteien des Cloud-Computing-Vertrages keine ausdrückliche Rechtswahl, kommt die EG-Verordnung Nr. 593/2008 vom 17. Juni 2008 („Rom I") über das auf vertragliche Schuldverhältnisse anzuwendende Recht zur Anwendung. Rechnet man einen derartigen Vertrag zu den Dienstleistungsverträgen, unterliegt der Vertrag gem. Art. 4 der Verordnung dem Recht des Staates, in dem der Dienstleister seinen gewöhnlichen Aufenthalt hat. Ist ein anderer

21. So entspricht der Begriff „warranty" nicht unbedingt der deutschen Haftung für Mängel

Vertragstypus einschlägig, unterliegt er dem Recht des Staates, in dem die Partei, welche die für den Vertrag charakteristische Leistung zu erbringen hat, ihren gewöhnlichen Aufenthalt hat. Diese Frage kann aber schwierig zu beantworten sein. Schließt z. B. die in Deutschland ansässige Vertriebsgesellschaft des Anbieters den Vertrag im Namen der US-Mutter und der indischen, der englischen und der ukrainischen Tochtergesellschaft und erbringen alle diese Gesellschaften Cloud-Services, kann die Ermittlung des anwendbaren Rechts zum Problem werden.

- Zwingendes Recht
  Nicht alle Aspekte eines Vertrages unterliegen der getroffenen Rechtswahl. So richten sich Sachen- und Urheberrechte nach dem Recht des Staates, in dem sie entstanden sind. Bei Rechtsverletzungen kann auch der Ort, an dem in die Rechte eingegriffen wurde, eine Rolle spielen. In diesen Fällen können die Parteien des Vertrages die Rechtslage nicht durch vertragliche Abreden gestalten. Sie können jedoch durch die Wahl der Länder, in denen sie im Rahmen der Cloud-Services tätig sind, das zwingend anwendbare Recht beeinflussen.
- Deliktische Ansprüche – Rom II
  Eine Rechtswahl ist nur bei vertraglichen Schuldverhältnissen möglich. Geht es um außervertragliche Schuldverhältnisse, wie z. B. deliktische Schadensersatzansprüche (wie Datendiebstahl), ergibt sich das anwendbare Recht aus EG-Verordnung Nr. 864/2007 vom 11. Juli 2007 („Rom II“).

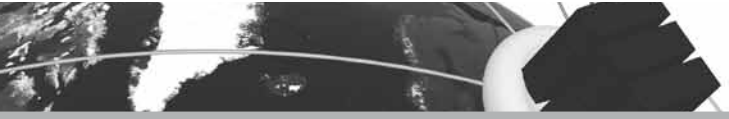
2.3.2 Gerichtsstand

- Land der Rechtswahl
  Der Gerichtsstand hat Auswirkungen auf die Vollstreckbarkeit einer späteren Gerichtsentscheidung. Außerdem wird ein Gerichtsverfahren immer dann schwierig, wenn sich die Richter mit einer Rechtsordnung auseinandersetzen müssen, in der sie nicht ausgebildet wurden. Ist der Vertrag z. B. auf Deutsch abgefasst und liegt der Gerichtsstand in Deutschland, sollte auch deutsches Recht anwendbar sein.
- Verfahrenssprache – Vertragssprache
  Das Problem ist ebenso gelagert wie bei dem oben beschriebenen Verhältnis der Vertragssprache zum anwendbaren Recht. Auch hier ist empfehlenswert, dass die Vertragssprache und die Verfahrenssprache gleich sind. Weichen sie voneinander ab, müssen in einem Rechtsstreit alle Dokumente übersetzt werden. Bei den Übersetzungen besteht die Gefahr von Ungenauigkeiten, weil sich Rechtsbegriffe nicht exakt übersetzen lassen. Sie erhalten ihre Bedeutung aus der zugrunde liegenden Rechtsordnung.
- Vollstreckbarkeit von Gerichtsentscheidungen
  Bei der Wahl des Gerichtsstands sollten die Parteien nicht nur ihr Augenmerk darauf richten, in welcher Rechtsordnung sie sich „wohl“ fühlen. Zu beachten ist auch, wo eine eventuelle Gerichtsentscheidung vollstreckt werden soll. Das Anerkennungsverfahren ausländischer Entscheidungen im Zielland kann so schwierig sein, dass es unter Umständen lohnender ist, das gesamte Gerichtsverfahren im Zielland zu führen.

2.3.3 Schiedsklausel

Schiedsverfahren sind eine Alternative zu Verfahren vor den staatlichen Gerichten. Die Schiedsrichter können aufgrund ihrer Sachkunde gewählt werden. So werden auch technisch komplizierte Vorgänge oder branchenübliche Verfahren von dem Schiedsgericht schneller beurteilt. Dadurch arbeitet das Schiedsgericht unter Umständen schneller als ein staatliches Gericht. Auf der anderen Seite muss sich das Schiedsgericht für den konkreten Fall erst konstituieren, was geraume Zeit in Anspruch nehmen kann. Die Vergütung der Schiedsrichter kann je nach Vergütungsvereinbarung höher sein als die Gerichtskosten für staatliche Gerichte. Auf der anderen Seite gibt es bei Schiedsverfahren üblicherweise nur eine Instanz. Die Voraussetzungen, unter denen Schiedsentscheidungen in den betroffenen Ländern vollstreckbar sind, müssen vor Vereinbarung der Schiedsklausel geprüft werden.

Problematisch sind Schiedsverfahren insbesondere dann, wenn sich die beteiligten Parteien in der Schiedsklausel



auf den vollständigen Verzicht ihres rechtlichen Gehörs vor den staatlichen Gerichten einigen. Damit entfällt eventuell sogar die Möglichkeit einer Berufungsinstanz.

Das Verfahren bietet zudem immer wieder Raum für „Strategische Spiele", die in dieser Art bei ordentlichen Gerichten – nicht zuletzt wegen einer dort gefestigten Zivilprozessordnung und meist umfassender Rechtsprechung – nicht denkbar wären. Dies kann vordergründige Kosten- oder allgemeine Effizienzerwägungen schnell obsolet werden lassen.

2.4 Leistungsbeschreibung und Service Level Agreements

2.4.1 Definition vereinbarter Leistungen für Cloud-Computing

Wie auch im Abschnitt 2.2 dargestellt, ist zwischen dem Vertragsverhältnis des Kunden mit einem Cloud-Computing-Anbieter einerseits und andererseits den Vertragsverhältnissen mehrerer Cloud-Anbieter untereinander für eine Cloud zu unterscheiden. Im Folgenden werden die vertraglichen Beziehungen zwischen dem Kunden und dem Cloud Computing-Anbieter näher betrachtet.

Wie in jedem Fall der Erbringung von IT-Leistungen durch Dritte ist die Leistungsbeschreibung von entscheidender Bedeutung. Insoweit ergibt sich kein Unterschied zwischen Cloud Computing und „klassischem" Outsourcing oder dem sonstigen Bezug von IT-Leistungen von Dritten. Es gilt, die Leistungsbeschreibung so detailliert wie möglich zu formulieren.

Eine sorgfältige Leistungsbeschreibung setzt voraus, dass der Kunde nach seiner Sourcing-Strategie die extern zu beauftragenden Leistungen möglichst genau definiert.

Dies schließt die Entscheidung ein, inwieweit er Cloud-Computing-Leistungen in Anspruch nehmen möchte:

- Benötigt der Kunde die Nutzung einer bestimmten Anwendung – SaaS?
- Soll eine Laufzeit- und Entwicklungsumgebung genutzt werden – PaaS?
- Plant der Kunde die Nutzung von IT-Infrastruktur – IaaS?

Unabhängig davon sind die Besonderheiten des Cloud Computings, die Flexibilität und Skalierbarkeit der Leistungen, exakt in der Leistungsbeschreibung abzubilden. Nur dann wird eine vertragsgemäße Flexibilität und Skalierbarkeit später von einer Vertragsänderung durch Change Request (vgl. Abschnitt 2.5) abgrenzbar.

2.4.2 Vertragstypologische Einordnung von bestimmten Leistungsarten

Das umfangreiche Spektrum und die große Bandbreite möglicher Cloud-Computing-Leistungen macht eine pauschale Zuordnung der jeweiligen Leistungen zu einem gesetzlich definierten Vertragstyp kaum möglich. Vielmehr werden im Regelfall typengemischte Verträge je nach Umfang und Ausprägung der Cloud-Computing-Leistungen vorliegen. Andererseits hat die vertragstypologische Zuordnung der Cloud-Computing-Leistungen zu gesetzlichen Vertragstypen entscheidende Bedeutung für die ohne vertragliche Vereinbarung für ein bestimmtes Thema geltenden gesetzlichen Regelungen, etwa auch für das anwendbare Gewährleistungsrecht.

Vor diesem Hintergrund soll eine beispielhafte Zuordnung der Erscheinungsformen von vergütungspflichtigen Cloud-Computing-Leistungen (vgl. Tabelle 1) zu den gesetzlichen Vertragstypen vorgenommen werden (vgl. Tabelle 3).

Tabelle 3: Zuordnung von Cloud-Computing-Leistungen zu gesetzlichen Vertragstypen

Ebene	Vertragstypologische Einordnung
SaaS	SaaS stellt aus rechtlicher Sicht als zeitlich begrenzter Zugriff auf bereitgestellte Software eine Art des Application Service Providing (ASP) dar. Nach der Rechtsprechung des Bundesgerichtshofs zu ASP wird daher auch bei SaaS häufig eine mietvertragliche Gestaltung vorliegen. Ergänzend vereinbarte Überwachungs- und Betriebsleistungen haben üblicherweise dienstvertraglichen Charakter.
PaaS	Der für PaaS typische, zeitlich begrenzte Zugriff auf eine bereitgestellte Laufzeit- oder Entwicklungsumgebung entspricht häufig ebenfalls dem Wesen eines Mietvertrags. Ergänzend vereinbarte Überwachungs- und Betriebsleistungen haben üblicherweise dienstvertraglichen Charakter.
IaaS	Im Rahmen von IaaS gilt es zu unterscheiden: ■ Die reine Bereitstellung einer Hardware-Umgebung und/oder von Speicherplatz erfolgt wohl regelmäßig auf Basis eines Mietvertrags. ■ Ergänzende Überwachungs- und Betriebsleistungen haben üblicherweise dienstvertraglichen Charakter. ■ Bestimmte Vertragsgestaltungen etwa beim Webhosting können nach Auffassung des Bundesgerichtshofs werkvertraglichen Charakter haben. Dort liegt der Schwerpunkt üblicherweise auf der permanenten Abrufbarkeit der Website und damit einem rechtsgeschäftlichen Erfolg, nicht nur in der Bereitstellung von Webspace.

Soweit Einzelleistungen unentgeltlich zur Verfügung gestellt werden[22] wird wohl das gesetzliche Leitbild des Leihvertrags anwendbar sein. Die Einräumung der bloßen Nutzungsmöglichkeiten ersetzt die sonst erforderliche Besitzverschaffung bei einer Leihe. Oft werden kostenlose Dienste aber nicht isoliert angeboten oder können nicht isoliert in Anspruch genommen werden. Das kann wegen des eingeschränkten Funktionsumfangs des kostenlosen Leistungsanteils[23] der Fall sein oder weil die kostenlose Leistung nur ein Teil eines insgesamt kostenpflichtigen Leistungspaketes ist und sinnvoll nur im Rahmen dieses Gesamtpaketes genutzt werden kann. Dann hat häufig der vergütungspflichtige Vertragsanteil den Vorrang. Im dargestellten Beispiel würde der mietrechtliche Charakter wieder in den Vordergrund rücken.

Häufig sind neben standardisiert angebotenen Cloud-Computing-Leistungen weitere kundenspezifische Leistungen erforderlich, damit der Kunde die Cloud-Computing-Leistungen in seinem betrieblichen und technischen Umfeld überhaupt erst oder besser nutzen kann. Beispiele dafür sind Anbindungen der Cloud-Computing-Leistungen – etwa bei einer Private oder Hybrid Cloud – an die vorhandenen IT-Systeme des Kunden. Dafür notwendige Leistungen können ebenso unterschiedlich sein wie die vorhandenen Systeme der Kunden. Solche Leistungen können daher nicht von vornherein pauschal einem gesetzlichen Vertragstyp zugeordnet werden. Häufig wird es sich um dienst- oder werkvertragliche Leistungen handeln.

Zusammenfassend lässt sich feststellen, dass die Erbringung von laufenden und vergütungspflichtigen Cloud-Computing-Leistungen im Schwerpunkt wohl auf mietvertraglicher Basis erfolgen wird. Jedoch hängt die rechtliche Zuordnung im Einzelfall davon ab, wie die gegenständlichen Cloud-Computing-Leistungen zu definieren und welche sonstigen Leistungen noch mit eingeschlossen sind oder im Zusammenhang mit den Cloud-Computing-Leistungen erbracht werden.

22. z. B. Speicherplatz im Internet oder Web-E-Mail-Dienste
23. z. B. begrenzte Postfachgröße oder Speicherkapazität

2.4.3 Rechtsfolgen von Leistungsstörungen

Bei Leistungsstörungen im Zusammenhang mit der Erbringung von Cloud-Computing-Leistungen können je nach vertraglicher Ausgestaltung im Einzelfall gesetzliche Gewährleistungsrechte bestehen (vgl. Abschnitt 2.6):

- Bei mietvertraglichen Gestaltungen kommen die gesetzlichen Gewährleistungsrechte gemäß der §§ 535 ff BGB zur Anwendung, soweit sie nicht wirksam vertraglich modifiziert sind.
- Bei dienstvertraglichen Gestaltungen existieren keine „klassischen" Gewährleistungsrechte im Sinne von Nacherfüllung oder Minderung.
- Bei werkvertraglichen Gestaltungen kommen die gesetzlichen Gewährleistungsrechte gemäß der §§ 634 ff BGB zur Anwendung, soweit sie nicht vertraglich (individuell vereinbart oder via AGB) wirksam modifiziert sind.
- Bei leihvertraglichen Gestaltungen bestehen Gewährleistungsrechte nur, soweit ein Mangel arglistig verschwiegen wurde (§ 600 BGB). Nach allgemeiner Ansicht umfasst ein daraus resultierender Schadensersatzanspruch auch nur den Ersatz des Vertrauensschadens.

Bei Cloud-Computing-Leistungen liegen für verschiedene Leistungsteile nebeneinander häufig mehrere gesetzliche Vertragstypen vor. Dann ist bereits die Abgrenzung schwierig, welcher Vertragstyp genau für welchen Leistungsbestandteil gilt. In einem Vertrag über Cloud-Computing-Leistungen können gleichzeitig alle angesprochenen gesetzlichen Vertragstypen vorliegen (vgl. Abbildung 15).

Bei Geltung gesetzlichen Mietrechts stellt sich vorab eine Kernfrage: In welchem zeitlichen und funktionalen Umfang hat die bereitzustellende Leistung dem Kunden vertraglich zur Verfügung zu stehen? Es ist bei einem Mietvertrag zwar Pflicht des Anbieters, etwa die im Rahmen von IaaS vereinbarte Infrastruktur dem Kunden in einem zum vertraglichen Gebrauch geeigneten Zustand bereitzustellen und während der Vertragslaufzeit in einem geeigneten Zustand zu halten. Aus dieser gesetzlichen Verpflichtung folgt aber nicht, welche Betriebszeiten und Verfügbarkeiten für diese Infrastruktur vereinbart sind und auch nicht, in welchem Zeitraum auftretende Mängel oder Störungen zu bereinigen oder zu umgehen sind. Ohne entsprechende vertragliche Vereinbarung ist der Anbieter bei mietvertraglicher Einordnung nur verpflichtet, Störungsmeldungen entgegen zu nehmen und zu bearbeiten, wenn der Kunde beweisen kann, dass es sich rechtlich um einen Mangel der Leistung des Anbieters handelt. Diese und weitere Parameter für die Definition der vertraglichen Leistungen können in Service Level Agreements (SLA) vereinbart werden.

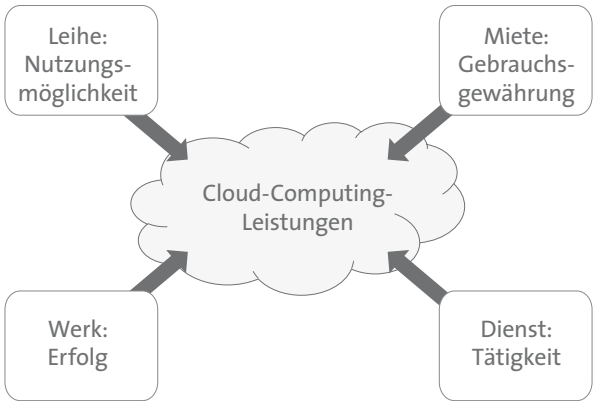


Abbildung 15: Vertragstypen für Cloud-Computing-Leistungen

An diesem Beispiel wird deutlich, dass Service Levels zur Vereinbarung eines einheitlichen Rahmens auch bei Schlechtleistungen für beide Vertragspartner die notwendige Klarheit schaffen können und deshalb für beide Vertragspartner vorteilhaft sind (weitere Einzelheiten vgl. Abschnitt 2.4.4).

2.4.4 Service Level Agreements

SLA beschreiben die geschuldeten Leistungen näher, insbesondere bei miet- oder dienstvertraglichen Gestaltungen. Dort werden qualitative und quantitative Leistungsmerkmale sowie spezifische Folgen bei deren Nichteinhaltung vereinbart. Die Konzeption von Service Level unterliegt dabei mindestens denselben hohen

Anforderungen wie die Leistungsbeschreibung. Zur Bestimmung (Messung) der Service Levels müssen geeignete Key Performance Indicators (KPI) vereinbart werden.

Als KPI im Rahmen von Cloud-Computing-Leistungen kommen insbesondere in Betracht:

- Verfügbarkeit des Systems oder Dienstes in einem bestimmten Messzeitraum,
- Reaktionszeiten auf Mängelmitteilung,
- Umgehungs- oder Beseitigungszeiten bei Mängeln.

Für die konkreten Festlegungen der KPI ergeben sich häufig keine wesentlichen Unterschiede zum „klassischen" Outsourcing. Daher kann oft auf dessen „Best Practices" zurückgegriffen werden, was sich am Beispiel der Systemverfügbarkeit als dem wohl wichtigsten KPI für Cloud-Computing-Leistungen zeigen lässt. Wird etwa eine Systemverfügbarkeit von 99,5 Prozent in einem monatlichen Messzeitraum und eine maximale Ausfalldauer von 4 Stunden vereinbart, dann muss der Cloud-Computing-Anbieter die technischen Voraussetzungen durch eine entsprechende Dimensionierung und Auslegung der Systeminfrastruktur schaffen, um die Erfüllung dieser Vorgaben zu ermöglichen.

Unterschiede zum „klassischen" Outsourcing

Unterschiede zum „klassischen" Outsourcing können sich jedoch für die Überwachung der Einhaltung von Service Levels ergeben. Dem Kunden sind bei „klassischem" Outsourcing sowohl die technischen als auch vielfach die menschlichen Ressourcen bekannt (z. B. nach der vollständigen Ausgliederung eines Betriebsteils). Dort ist es üblich, dem Anbieter die Messung der KPI in Verbindung mit einem entsprechend individuellen SLA-Reporting zu überlassen und sich kundenseitig auf eine bloße Inanspruchnahme der Leistungen ohne eigene IT-Ressourcen zu beschränken. Entsprechend der Natur von Cloud-Computing-Leistungen, Ressourcen gerade nicht dediziert für einen Kunden zur Verfügung zu stellen, wird der Kunde häufig die Überwachung der SLA selbst durchführen oder zumindest steuern müssen.

Ein weiterer Unterschied zeigt sich für Schnittstellen, ebenfalls dargestellt am Beispiel der Systemverfügbarkeit. Dem Kunden kommt es primär auf eine sogenannte End-to-End-Verfügbarkeit an, also vom Server des Anbieters zum Client des Kunden:

- Bei „klassischem" Outsourcing wird dies häufig dadurch gelöst, dass der Outsourcing-Anbieter auch die Netzwerkverbindungen bereit stellt oder verantwortet.
- Im Gegensatz dazu bleibt bei Cloud Computing, etwa bei SaaS, die Bereitstellung der Internetverbindung in der Verantwortung des Kunden. Gerade die Performance der Internetverbindung, also deren Dimensionierung, ist jedoch entscheidend für die Verfügbarkeit und die Antwortzeiten einer durch SaaS genutzten Anwendung. Dieses Thema kann durch den Kunden auch nicht über ein SLA mit dem Cloud-Computing-Anbieter gelöst werden, sondern nur durch eine entsprechende Vereinbarung mit seinem Netzbetreiber (vgl. Abbildung 12).

Unabhängig davon sind in einem SLA auch geeignete und angemessene Folgen für die Unterschreitung vereinbarter KPI zu vereinbaren. Solche Folgen können definierte Minderungen der Vergütung oder pauschalierter Schadensersatz oder Vertragsstrafen sein, wobei Letztere gesetzlich auf sonstige Ansprüche anzurechnen sind. Für nachhaltige und gleichzeitig schwerwiegende Verstöße kommen auch Sonderkündigungsrechte in Betracht. Typischerweise werden in den SLA die Folgen von Unterschreitungen der vereinbarten Leistungsparameter abschließend geregelt, also weitere denkbare Ansprüche wegen unzureichender Leistung ausgeschlossen. So kann aus Sicht der Vertragspartner eine angemessene und interessengerechte Regelung erfolgen. Für den Kunden ist in einem SLA vor allem sein vorrangiges Interesse an einer vertragsgemäßen Leistung zu berücksichtigen.

2.4.5 Zuordnung von Cloud-Computing-Leistungen in organisatorischer Hinsicht

Neben leistungsinhaltlichen Kriterien lassen sich Cloud-Computing-Leistungen auch unter Betriebs-, Eigentums- oder Organisationsaspekten unterscheiden. Die vertragstypologische Einordnung ist jedoch unabhängig von der im Einzelfall gewählten Organisationsform der Cloud (vgl. Tabelle 2 und Abbildung 16).

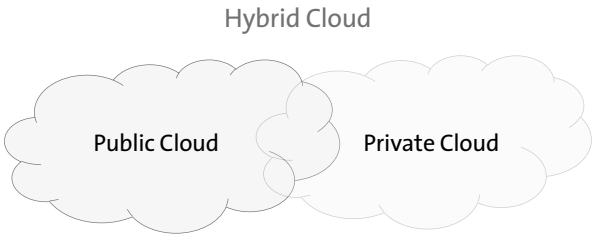


Abbildung 16: Public, Private und Hybrid Cloud

Auch wenn diese Organisationsformen die vertragstypologische Einordnung nicht beeinflussen, so haben sie doch Auswirkungen sowohl auf die praktische Nutzbarkeit der Cloud-Computing-Leistungen im Einzelfall als auch für mögliche rechtliche Hindernisse.

Cloud-Computing-Leistungen der Ebenen SaaS, PaaS und IaaS legen oft den organisatorischen Schwerpunkt in einer Public Cloud nahe, da die parallele Nutzung der jeweiligen Ressourcen durch mehrere Kunden im Vordergrund steht. Eine Public Cloud zeichnet sich wiederum dadurch aus, dass sie offen und auch international zugänglich ist. Das erhöht die gewünschte Flexibilität der Leistungserbringung, bedeutet aber zusätzliche rechtliche Anforderungen und Fragen. Dies gilt etwa für den Schutz personenbezogener Daten oder mit regulatorischen Anforderungen zusammenhängende Fragen, wie z. B. Kontrollmöglichkeiten im Rahmen der IT-Sicherheitspflichten. Da es dem Wesen einer Private Cloud entspricht, auf einen organisatorisch und auch technisch abgeschlossenen Unternehmensbereich beschränkt zu sein, lassen sich diese rechtlichen und regulatorischen Fragen besser klären. Daraus ergeben sich jedoch vielfach Probleme für den praktischen Nutzen der Cloud-Computing-Leistungen, insbesondere was Flexibilität, Skaleneffekte und Kosteneinsparungen betrifft.

Ein möglicher Ausweg könnte daher in einer geeigneten Kombination der Vorteile aus beiden Organisationsformen im Rahmen einer Hybrid Cloud liegen.

2.4.6 Individualleistungen und Cloud Computing

Cloud-Computing-Leistungen setzen ein hohes Maß an Standardisierung voraus, um das mit ihnen hauptsächlich verfolgte Ziel zu erreichen, durch flexible und skalierbare Leistungserbringung „on demand“ Kostenvorteile zu realisieren und dadurch entsprechend attraktiv zu sein. Dies lässt sich durch den Einsatz von Virtualisierungs- und Webtechnologien aus technischer Sicht realisieren. Gleichzeitig setzt dieses Konzept jedoch voraus, dass der Kunde die betreffende Leistung in der standardisiert angebotenen Form nutzen kann. Benötigt der Kunde dagegen etwa zusätzlich den Betrieb von selbst entwickelten Anwendungen oder Speziallösungen, stößt ein idealtypisches Cloud-Computing-Modell an seine Grenzen.

In den unterschiedlichen Konstellationen können auch folgende Umstände eine differenzierte Betrachtung erforderlich machen:

- Betreibt der Cloud-Computing-Anbieter eigens entwickelte Anwendungen oder Speziallösungen des Kunden werden sich in der Regel die Synergie- und Skaleneffekte reduzieren, was zu einer Erhöhung der Kosten führt. Selbst wenn sich ein solcher Betrieb im Rahmen eines vollständigen Outsourcings für den Kunden noch rechnen mag, wird der Support und die Administration in aller Regel beim Kunden verbleiben müssen. Dies läuft dem Konzept eines vollständigen Outsourcings durch Cloud Computing zuwider und bedeutet zusätzliche Aufwendungen für den Kunden, da er eine Support-Organisation aufrechterhalten muss.
- Etwaige Notwendigkeiten für den Kunden, die Einhaltung der SLA im Rahmen von Cloud Computing selbst

zu überwachen und selbst für den Internet- bzw. sonstigen Netzwerkzugang zu sorgen, können ebenfalls zusätzliche Kosten für den Kunden bedeuten.

Solche Überlegungen werden daher im Rahmen der Sourcing-Strategie des Kunden zu betrachten sein und können dazu führen, dass derjenige Cloud-Computing-Anbieter den Vorzug erhält, der in der Lage ist, ein über die reinen Cloud-Computing-Leistungen hinausgehendes Leistungsportfolio abzudecken und anzubieten.

Auch eine gewünschte Anbindung von vorhandenen IT-Systemen des Kunden an die Cloud-Computing-Leistungen wird sich häufig nicht mit standardisierten Leistungsangeboten abdecken lassen. Dafür sind die spezifischen IT-Umgebungen der Kunden und ihre betrieblichen Anforderungen zu vielgestaltig. Umso mehr werden am Markt die Anbieter entsprechende Vorteile haben, die auch solche kundenspezifischen Leistungen im Zusammenhang mit Cloud Computing realisieren können.

2.5 Vertragsänderungen

Vertragsänderungen (Change Requests) beim Cloud Computing können sowohl den Leistungsinhalt (z. B. Bereitstellung neuer Software-Funktionen) als auch den Leistungsumfang (z. B. weitere Nutzer, Bereitstellung zusätzlicher Speicherkapazität) betreffen.

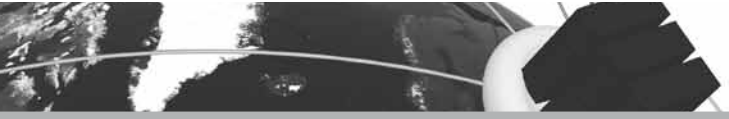
Bestimmte Erweiterungen und Anpassungen der vereinbarten Leistungen können bereits im Vorfeld vertraglich geregelt werden. Typischerweise werden für Cloud-Computing-Leistungen dazu Regelungen für die charakteristische Flexibilität und Skalierbarkeit vereinbart. Dazu zählen beispielsweise die Preise für zusätzliche Nutzer oder auch für zusätzliche Speicherkapazität.

Darüber hinaus kann ein Vertragspartner den Wunsch oder Bedarf nach anderen oder geänderten Leistungen oder Arten der Leistungserbringung haben.[24] Für diese Situationen und für nicht vorhersehbare Leistungsänderungen empfiehlt es sich, ein formales Verfahren (Change-Request-Verfahren) zu definieren. Ein Change-Request-Verfahren sollte zumindest folgende Regelungen enthalten:

- Beide Vertragspartner können Änderungen (Change Requests) des vereinbarten Vertragsumfangs vorschlagen.
- Die gewünschte Änderung ist zu beschreiben und zu begründen. Die Folgen der Änderung, insbesondere für Preis, Termine und Qualität, sind als Entscheidungsgrundlage aufzuzeigen.
- Berechtigte des Auftraggebers und des Auftragnehmers entscheiden gemeinsam, unter Berücksichtigung der Folgen der Änderung, ob die Änderung durchgeführt wird und dokumentieren die Entscheidung als Vertragsergänzung.
- Vor einer Entscheidung über eine Änderungsanforderung werden keine Änderungen vorgenommen, sondern der bestehende Vertrag weiter durchgeführt.
- Bei erheblichem Aufwand für die Prüfung eines Änderungsvorschlages ist für die Prüfung selbst ein Change-Request-Verfahren durchzuführen, in dem auch über eine Unterbrechung der weiteren Leistungserbringung während der Prüfungsarbeiten entschieden wird.

Unabhängig davon, welches Verfahren für Änderungswünsche und die Durchführung von Vertragsänderungen vereinbart ist, ist das vereinbarte Verfahren umzusetzen und ausnahmslos anzuwenden und dokumentiert durchzuführen. Andernfalls wird früher oder später unklar, welche Leistungen aktuell genau vereinbart sind. Diese Unklarheit bietet allenfalls überflüssigen Stoff für Diskussionen über unterschiedliche Auffassungen. Das liegt weder im Interesse der Vertragspartner, noch einer möglichst guten Leistungserbringung und Vertragsdurchführung.

24. etwa andere Größenordnung der Leistungen, Ergänzung und Streichung von Leistungen



2.6 Gewährleistung und Haftung

Gewährleistungs- und Haftungsfragen für Cloud Computing lassen sich mit teilweise über 100 Jahre alten gesetzlichen Regelungen allenfalls teilweise abschließend beantworten. Daher sollten vertragliche Regelungen nicht nur genau die Art und den Umfang der geschuldeten Leistungen beschreiben, sondern auch entsprechende Regelungen für etwa dahinter zurückbleibende Leistungen beinhalten.

Für nicht vertragsgemäß erbrachte Leistungen existieren nur bei bestimmten gesetzlich vordefinierten Vertragstypen gesetzliche Regelungen. Die Frage, welchem vordefinierten gesetzlichen Vertragstyp eine bestimmte Leistung zuzuordnen ist, entscheidet darüber, welche gesetzlichen Regelungen bei mangelhafter Leistungserbringung greifen. Allerdings führen diese gesetzlichen Regelungen bei Verträgen über Cloud-Leistungen häufig nicht zu praktikablen Ergebnissen. Darüber hinaus kann durch Änderung der Leistungen während der Vertragsdurchführung oder ihres Schwerpunktes auch eine Änderung der Zuordnung zu einem gesetzlich vordefinierten Vertragstyp erfolgen (etwa bei unterschiedlichen „on demand"-Leistungen).

Wie im Abschnitt 2.4.2 dargestellt, enthalten Leistungen im Bereich Cloud Computing dienstvertragliche, werkvertragliche und mietvertragliche Elemente. Im Folgenden werden die gesetzlichen Gewährleistungsvorschriften für diese Leistungselemente im Überblick dargestellt. Schon die Unterscheidung zwischen solchen Elementen erscheint in der Praxis als wenig brauchbar. Die gesetzlichen Gewährleistungsrechte werden den Interessen der Vertragspartner zudem häufig nicht gerecht. Vereinbarte Service Level können in praxistauglicher Weise die vereinbarten Leistungen beschreiben und die Folgen einer Unterschreitung der Leistungsanforderungen regeln. Daneben sollten im Vertrag auch Haftungsfragen angemessen geregelt werden.

2.6.1 Gewährleistung bei mietvertraglichen Leistungselementen

Bei mietvertraglichen Leistungselementen hat der Anbieter dem Kunden den Gebrauch bestimmter Hardware oder Software für die Mietdauer gegen Vergütung zu gewähren. Dafür ist kein Besitz der Mietgegenstände durch den Kunden erforderlich. Es genügt vielmehr, dass er die Mietgegenstände benutzen kann. Für viele Cloud-Computing-Leistungen liegt eine rechtliche Einordnung als mietvertragliches Leistungselement nahe (vgl. Tabelle 3). Der Bundesgerichtshof hat für Application Service Providing entschieden, dass es sich in der damals konkret vorliegenden Ausgestaltung um eine mietvertragliche Leistung handelte. Das gilt auch für die laufende Bereitstellung von Hardware oder Speicherplatz.

Für Mietverträge existieren spezifische gesetzliche Gewährleistungsvorschriften. Diese sehen eine Minderung der Vergütung bei Mängeln vor, die eine Nutzung der Leistungen durch den Kunden beeinträchtigen. Unter bestimmten Voraussetzungen wäre der Kunde gesetzlich auch zur Selbstvornahme einer Mängelbeseitigung sowie zum Ersatz dafür notwendiger Aufwendungen berechtigt, was bei Cloud-Computing-Leistungen aber schon wegen fehlenden Zugriffs auf die dazu notwendige Infrastruktur kaum praktikabel erscheint. Unter bestimmten Voraussetzungen kann der Kunde bei Mängeln der Leistungen auch Schadensersatz verlangen. Wie im Dienst- und Werkvertragsrecht gilt allerdings auch hier, dass der Kunde so gerade nicht die von ihm beauftragte Leistung erhält.

Im Mietrecht sind viele praktisch wichtige Fragen gesetzlich nicht geregelt. Dazu gehören etwa:

- Wie rasch ist ein auftretender Mangel durch den Anbieter zu beseitigen?
- Welche Einschränkungen der Verfügbarkeit von Leistungen sind akzeptabel?
- Wie berechnen sich etwaige Ansprüche des Kunden bei Einschränkungen von Leistungen?

Ohne vertragliche Regelungen sind also selbst dann längere Diskussionen vorprogrammiert, wenn sich die Vertragspartner darüber einig sind, dass

Leistungseinschränkungen vorlagen. Das wird den praktischen Bedürfnissen kaum gerecht.

2.6.2 Gesetzliche Gewährleistung bei dienstvertraglichen Elementen

Bei dienstvertraglichen Leistungselementen schuldet der Anbieter ein Tätigwerden nach anerkannten Regeln, aber keinen definierten Leistungserfolg. Beispiele für dienstvertragliche Leistungen sind etwa Beratung und Unterstützung. Dienstvertragliche Leistungselemente werden häufig nach Aufwand vergütet.

Gesetzlich sind für dienstvertragliche Leistungselemente keine spezifischen Gewährleistungsvorschriften vorgesehen. Zwar kann ein Kunde bei schuldhaften Pflichtverletzungen des Dienstleisters grundsätzlich Schadensersatz verlangen. Dafür muss er aber zunächst die Pflichtverletzung des Dienstleisters beweisen, der sich grundsätzlich durch fehlendes Verschulden zu entlasten hat. Bereits dies verursacht in der Praxis erhebliche Schwierigkeiten für beide Vertragspartner und bis zur Klärung etwa unzureichender Leistungen und daraus möglicherweise folgender Ansprüche vergehen nicht selten Monate. Schon dieser Zeitaspekt ist mit Grundgedanken des Cloud Computing kaum vereinbar.

Daneben erhält der Kunde auf diesem Wege auch nicht die von ihm benötigte ordnungsgemäße Dienstleistung, sondern allenfalls Schadensersatz in Geld.

2.6.3 Gesetzliche Gewährleistung bei werkvertraglichen Elementen

Eine werkvertragliche Charakteristik eines Leistungselements setzt voraus, dass zwischen Kunde und Anbieter ein – typischerweise im Vorfeld – definierter Leistungserfolg vereinbart ist. Sind nicht alle Elemente eines solchen Leistungserfolgs im Vorfeld vereinbart, hat der Anbieter die Leistung grundsätzlich geeignet für den vertraglichen Verwendungszweck „nach mittlerer Art und Güte“ zu erbringen. Beispiel für ein werkvertragliches Leistungselement ist Webhosting, bei dem der Anbieter – soweit nicht anders vereinbart – die Abrufbarkeit der Website als Erfolg schuldet.

Gesetzlich gibt es spezifische Gewährleistungsregelungen für Werkverträge. Die Geltung dieser Regelungen beginnt grundsätzlich mit der Abnahme der Leistungen durch den Kunden, die bei Cloud Computing aber in der Regel kaum erfolgen wird. Bei mangelhaften Leistungen hat der Kunde gesetzlich ein Recht auf Nacherfüllung durch Nachbesserung oder Neulieferung nach Wahl des Anbieters. Allerdings wird eine solche Nacherfüllung bei Cloud-Computing-Leistungen schon aufgrund des Zeitablaufs häufig kaum sinnvoll sein.

Unter bestimmten Voraussetzungen hat der Kunde gesetzlich auch ein Recht zur Selbstvornahme einer Mängelbeseitigung. Dies ist bei Cloud-Computing-Leistungen aber wegen fehlenden Zugriffs des Kunden auf die dafür benötigte Infrastruktur noch weniger praktikabel.

Bei Fehlschlagen einer Nacherfüllung kann der Kunde unter bestimmten gesetzlichen Voraussetzungen vom Vertrag zurücktreten, also die Rückabwicklung des Vertrages verlangen. Ob dieses, auf einen einmaligen Leistungsaustausch gerichtete Instrument für eine dauerhafte Leistungsbeziehung wie Cloud Computing überhaupt anwendbar ist, ist allerdings fraglich. Bei laufenden Leistungen lassen erst später auftretende Störungen bereits erbrachte Leistungen unberührt, weshalb ein Rücktritt für die bereits mangelfrei erbrachten Leistungen unangemessen wäre. In diesen Fällen wäre anstelle eines Rücktritts wohl eine Kündigung angemessen. Gesetzlich hätte der Kunde alternativ zu einem Rücktritt nach Fehlschlagen der Nacherfüllung ein Minderungsrecht für die Vergütung mangelhafter Leistungen. Die Bemessung einer solchen Minderung dürfte selbst bei anerkannten Leistungsmängeln von Cloud-Computing-Leistungen problematisch sein. Bei verschuldeten Mängeln kann auch ein Schadens- oder Aufwendungsersatzanspruch des Kunden gegeben sein, der ihm aber – wie bei dienstvertraglichen Leistungselementen – gerade nicht die von ihm beauftragten Leistungen verschafft.

Es erscheint daher insgesamt fraglich, ob die gesetzlichen Gewährleistungsregelungen bei werkvertraglichen Leistungselementen von Cloud Computing den praktischen Bedürfnissen der Vertragspartner überhaupt gerecht werden können.

2.6.4 Gewährleistung bei leihvertraglichen Leistungselementen

Bei leihvertraglichen Leistungselementen wird dem Kunden die Nutzung bestimmter Hardware oder Software für die Leihdauer ohne Vergütung gewährt. Dafür ist kein Besitz der Leihgegenstände durch den Kunden erforderlich.

Für Leihverträge bestehen gesetzliche Gewährleistungsvorschriften. Danach haftet der Anbieter nur für grobe Fahrlässigkeit und Vorsatz sowie für arglistiges Verschweigen eines Mangels. Der Kunde hat wegen Unentgeltlichkeit der Leistung keine Ansprüche auf Beseitigung von Mängeln oder eine Reduzierung von Vergütung, die ja gar nicht zu leisten ist.

Für den Kunden sind solche kostenlosen Leistungen also üblicherweise nur im Rahmen ihrer gegebenen Funktionalität und Verfügbarkeit nutzbar. Wegen etwaigen Einschränkungen oder Fehlfunktionen hat der Kunde unter normalen Umständen keine Ansprüche.

2.6.5 Service Level als möglicher Lösungsweg

Die gesetzlichen Gewährleistungsregeln unterscheiden sich je nach Art des betroffenen Leistungselements. In der Praxis besteht also zunächst die Schwierigkeit herauszufinden, welches oder welche Leistungselemente von einer Leistungseinschränkung betroffen sind und welche gesetzlichen Regelungen dann überhaupt anwendbar sein können (vgl. Abbildung 17).

Aber auch unabhängig von diesen Abgrenzungsschwierigkeiten werden die gesetzlichen Gewährleistungsregelungen den praktischen Bedürfnissen der Vertragspartner nur selten gerecht. Teilweise sind die gesetzlichen Ansprüche in der Praxis gar nicht umzusetzen, teilweise gehen sie an den Bedürfnissen des Kunden vorbei.

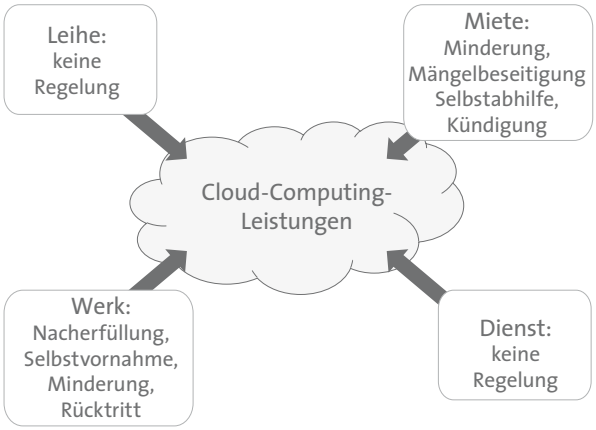


Abbildung 17: Gesetzliche Gewährleistung für Vertragstypen

Es empfiehlt sich daher, vertraglich nicht nur die geschuldeten Leistungen detailliert zu regeln, sondern auch die Folgen etwaiger Leistungseinschränkungen. Zunächst lässt sich dadurch klar bestimmen, welche Leistungen in welcher Art und Weise mit welchen Charakteristiken überhaupt vereinbart sind. Durch entsprechende vertragliche Regelungen lässt sich so für beide Vertragspartner auch eine verlässliche Grundlage für die Folgen etwaiger Leistungseinschränkungen und ihre Bereinigung schaffen.

Üblicherweise sehen Service Level für die Unterschreitung vereinbarter Kriterien auch in ihrer Höhe definierte Konsequenzen vor (etwa Bonus- und Malusregelungen). Regelungen für Verfügbarkeiten und Reaktionszeiten bei etwaigen Störungen sind bereits bei Verträgen über Outsourcing und Application Service Providing nicht unüblich. Typischerweise werden dabei für die Vertragsdurchführung wichtige Leistungsindikatoren und deren Messung ebenso vertraglich definiert, wie die Höhe einer etwaigen Konsequenz bei Über- und Unterschreitungen. Für „worst case“-Szenarien werden teilweise auch Regelungen über eine Vertragsbeendigung (etwa Kündigungsrechte) vereinbart, die üblicherweise von einer länger andauernden

und recht erheblichen Unterschreitung vereinbarter Leistungsindikatoren aus Gründen abhängen, die durch den Anbieter zu verantworten sind.

Auch wenn es rechtlich untypisch erscheinen mag, kann so ein klarer und einheitlicher Rechtsrahmen für etwaige Leistungseinschränkungen geschaffen werden, in dem die Leistungsqualität anhand Verfügbarkeiten und Reaktionszeiten nachvollziehbar gemessen wird.

Es empfiehlt sich daher, entsprechend detailliert die zu vereinbarenden Leistungsindikatoren und etwaige Konsequenzen bei deren Über- oder Unterschreitung im Vertrag festzulegen.

2.6.6 Haftung

Gesetzlich ist nach deutschem Recht eine zwingende Haftung für Vorsatz vorgesehen, die vertraglich nicht abgeändert werden kann. Üblich sind bei IT-Leistungen indes Vereinbarungen für Haftungsbeträge bei fahrlässig verursachten Schäden. Ebenso wie der Kunde ein Interesse an Ersatz solcher Schäden hat, hat der Anbieter ein nachvollziehbares Interesse daran, auf dem Wege der Haftung nicht das Geschäftsrisiko des Kunden zu übernehmen. Haftungsbeschränkungen in Allgemeinen Geschäftsbedingungen sind nur in bestimmten Grenzen rechtlich wirksam. Individuell vereinbarte Haftungsbeschränkungen sind in weitem Rahmen zulässig. Nicht selten werden Haftungsbeträge als Prozentsätze der vertraglichen Vergütung festgelegt.

2.7 Nutzungsrechte

Im Folgenden werden die Fragen der Erforderlichkeit sowie der Art und Weise der Einräumung von Nutzungsrechten für einzusetzende Software – ausgehend vom deutschen Urheberrechtsgesetz (UrhG) – dargestellt. Daneben können auch patentrechtliche Aspekte eine Rolle spielen.

2.7.1 Urheberrechte an Software

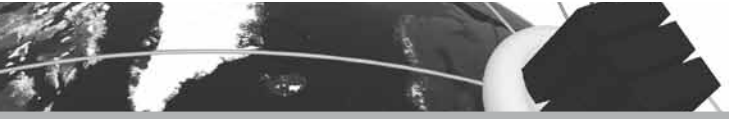
Nach deutschem Urheberrecht sind Computerprogramme alle Programme in jedem Entwicklungsstand, einschließlich des Entwurfsmaterials (§ 69a Abs. 1 UrhG). Sie sind als Computerprogramme geschützt, wenn sie individuelle Werke sind, die das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind (§ 69a Abs. 3 UrhG). Zur Bestimmung ihrer Schutzfähigkeit sind keine anderen Kriterien anzuwenden, insbesondere nicht qualitative oder ästhetische.

Unterschieden wird zwischen einfachen und ausschließlichen Rechten (§ 31 UrhG). Das einfache Nutzungsrecht berechtigt seine Inhaber, das Werk auf die erlaubte Art zu nutzen, ohne eine Nutzung durch andere auszuschließen. Demgegenüber berechtigt das ausschließliche Nutzungsrecht seinen Inhaber, das Werk unter Ausschluss aller anderen Personen auf die ihm erlaubte Art zu nutzen und Dritten einfache Nutzungsrechte einzuräumen.

Welche Rechte für die Leistungserbringung des Cloud-Computing-Anbieters benötigt werden, hängt von der konkreten Art des Nutzungsbedarfes ab, der sich aus den zu erbringenden Leistungen ergibt.

Die erlaubte Art der Nutzung ist daher inhaltlich, zeitlich und räumlich zwischen dem Hersteller oder Anbieter der einzusetzenden Software und dem Cloud-Computing-Anbieter sowie zwischen dem Cloud-Computing-Anbieter und dem Kunden festzulegen:

- Inhaltliche Festlegungen
  Regelungsgegenstand ist zum einen, das „Wie“ der Nutzung, also die Ausprägung der Art und Weise, in welcher Form die Software genutzt oder eingesetzt wird. Des Weiteren ist festzulegen, „Wer“ die Software nutzen darf. Hier ist wiederum zu unterscheiden: Auf der einen Seite kann eine Nutzung durch den Kunden des Cloud-Computing-Anbieters erfolgen und auf der anderen Seite durch Subauftragnehmer, die durch den Cloud-Computing-Anbieter in die Leistungserbringung eingebunden werden.
- Zeitliche Festlegung
  Eine vertragliche Vereinbarung ist auch für den



zeitlichen Umfang der Nutzungsberechtigung zu treffen.

- Räumliche Festlegung
  Letztlich ist auch die räumliche – also geographische – Festlegung des Nutzungsrechtes an der Software erforderlich, etwa in Deutschland, Europa oder weltweit.

2.7.2 Rechteeinräumung nach Art der Leistung

Nachfolgend wird für die verschiedenen Arten des Cloud Computing dargestellt, ob und welche urheberrechtlich relevanten Vorgänge bei der Nutzung der Leistung durch den Kunden stattfinden und daher eine Nutzungsrechts-Einräumung erfordern. Dabei wird, soweit nicht explizit eine andere Situation dargestellt wird, davon ausgegangen, dass alle Abläufe mit Ausnahme der Anzeige und der Übertragung von Daten des Kunden ausschließlich auf der Infrastruktur des Anbieters stattfinden. Der Kunde greift auf „die Cloud" nur über Web-Browser oder eine Client-Software zu.

Ob und inwiefern dem Kunden eigene Nutzungsrechte eingeräumt werden müssen, ist insbesondere bedeutsam für Folgefragen:

- Welche Nutzungsrechte benötigt der Anbieter an der Software, die er im Rahmen des Cloud Computing dem Kunden bereitstellt?
- Verstößt ein Kunde gegen das Urheberrecht, wenn der Anbieter seinerseits nicht die erforderlichen Nutzungsrechte für die Software bereitstellen kann?

Für alle Arten von Cloud Computing gilt:

Der Anbieter muss für ausreichende Nutzungsrechte an der von ihm eingesetzten Software sorgen, wobei er insbesondere berechtigt sein muss, die Software für den Einsatz im Rahmen des Cloud Computing für alle Länder, in denen die Cloud eingesetzt wird, und mindestens für die Dauer seines Vertragsverhältnisses zu Nutzern der Cloud zu verwenden. Dazu gehört insbesondere ein Recht zur Vervielfältigung der Software (§ 69c Nr. 1 UrhG).

Im Übrigen ist zu unterscheiden:

- IaaS
  Für den Anbieter dürften weitergehende Rechte, insbesondere ein Recht zur Einräumung von einfachen Nutzungsrechten (an Kunden), zur Vermietung oder zum öffentlich zugänglich machen, nicht erforderlich sein, da IaaS lediglich die Bereitstellung von Rechenleistung und Speicherplatz umfasst. Zwar greift der Kunde durch deren Nutzung „mittelbar" auf die zur Errichtung der Cloud erforderliche Software des Anbieters zu, der Kunde nimmt aber keine Vervielfältigungshandlungen vor. Der Kunde hat keinen Einfluss auf die systemtechnische Realisierung der Cloud und nutzt im Übrigen auch nur das Ergebnis der im Hintergrund laufenden und für ihn nicht sichtbaren Software. Das sind etwa der Speicherplatz und die in der Regel über eine Virtualisierungssoftware bereitgestellte Rechenkapazität, nicht aber die Software selbst. Urheberrechtliche Nutzungsrechte für den Kunden selbst sind daher bei IaaS nicht erforderlich.
- PaaS
  Der Anbieter des Cloud Computing muss berechtigt sein, die von ihm in der „Cloud" vorhandene Entwicklungsumgebung im Rahmen des Cloud Computings zugänglich zu machen. Ein urheberrechtliches Vermietungsrecht (§ 69c Nr. 3 UrhG) dürfte allerdings nicht erforderlich sein, da für eine derartige „Vermietung" nach überwiegender Ansicht eine körperliche Überlassung des Vervielfältigungsstücks erforderlich wäre. Noch nicht abschließend geklärt ist, inwiefern das Anbieten von Cloud-Computing-Leistungen ein öffentliches Zugänglichmachen von Software (§ 69c Nr. 4 UrhG) bedeutet. In der Literatur wird insbesondere im Zusammenhang mit ASP teilweise darauf abgestellt, dass ein öffentliches Zugänglichmachen nur vorliegt, wenn nicht bloß Grafikdaten (etwa Ein- und Ausgabedaten), sondern auch urheberrechtlich geschützte Programmteile übertragen werden. Für den Kunden stellt sich die Situation wie folgt dar: Wird dem Kunden eine Entwicklungsplattform bereitgestellt, erhält er neben der Nutzungsmöglichkeit von Rechenleistung und Speicherplatz zusätzlich Zugriff auf eine vom Anbieter zur Vergütung gestellte Softwareumgebung. Noch nicht abschließend geklärt ist,

ob der Kunde zur Nutzung dieser Softwareumgebung ein urheberrechtliches Nutzungsrecht gem. § 69c Nr. 1 UrhG benötigt. In der Literatur wird vereinzelt vertreten, dass die zur Verfügung gestellte Software über den Browser „gestreamt" wird, wodurch es im Browser-Cache und im Arbeitsspeicher des Anwenders zu Vervielfältigungen kommt. Die Folge wäre, dass der Kunde auch ein eigenes Nutzungsrecht benötigen würde. Allerdings lässt diese Ansicht außer Acht, dass der Browser lediglich ein Abbild des Ergebnisses der Softwarenutzung anzeigt, der Softwarecode aber in aller Regel gerade nicht in den Browser-Cache oder den Arbeitsspeicher des Computers des Anwenders vervielfältig wird. Etwas anderes kann nur dann vorliegen, wenn entweder über eine gesonderte Client-Software oder eine im Browser selbst laufende Software (z. B. ein Applet) eine Vervielfältigung der Entwicklungssoftware oder von Teilen dieser Software erfolgt. In der Regel aber gilt: Mangels Vervielfältigung benötigt der Kunde einer Cloud für PaaS kein eigenes urheberrechtliches Nutzungsrecht.

- SaaS
  Bei SaaS gilt die Darstellung für PaaS. In der Regel wird es an Vervielfältigungshandlungen des Nutzers fehlen, so dass dieser kein urheberrechtliches Nutzungsrecht benötigt.

2.7.3 Softwarebeistellungen des Kunden

Sofern der Kunde dem Cloud-Computing-Anbieter zur Erbringung der vertraglich vereinbarten Leistungen Software beistellen soll, bedarf es für diese Software ebenfalls der Einräumung entsprechender Rechte. Diese Rechteeinräumung richtet sich nach den Ausführungen im Abschnitt 2.7.1 und zwar unabhängig davon, ob der Kunde selbst Hersteller der Software oder Nutzungsberechtigter auf Grundlage eingeräumter Rechte ist.

2.7.4 Absicherung für den Ausfall des Anbieters

- Insolvenz des Anbieters
  Gerät der Anbieter in die Insolvenz, bleibt das Vertragsverhältnis mit dem Kunden hiervon zunächst unberührt. Nach der deutschen Insolvenzordnung kann der Insolvenzverwalter jedoch, soweit man von einem Miet- oder Werkvertrag ausgeht, die weitere Erfüllung des Vertrages ablehnen. Ausnahmen davon gelten, wenn der Anbieter die Software finanziert und zur Sicherheit an seinen Kreditgeber übertragen hat. Daten und Software des Kunden, die im Rahmen der Vertragsdurchführung in die Cloud übertragen wurden, kann der Kunde auch bei einer Vertragsbeendigung vom Insolvenzverwalter herausverlangen (sog. Recht auf Aussonderung). Sitzt der Anbieter im Ausland, gelten für die Insolvenz die jeweiligen Regelungen am Sitz des Anbieters. Für die Frage der Herausgabe von Daten sind zusätzlich die Bestimmungen des Landes zu beachten, in dem sich die Daten tatsächlich befinden.
- Ausfall des Anbieters
  Ist der Anbieter durch tatsächliche oder rechtliche Umstände, die nicht vom Kunden zu vertreten sind, nicht mehr zur Leistungserbringung im Stande, steht dem Kunden neben Gewährleistungsrechten und Ansprüchen aus Service Level Agreements nach deutschem Recht auch ein außerordentliches Recht zur Kündigung zu. Durch eine Kündigung enden allerdings auch die Rechte der Kunden hinsichtlich der Cloud. Zur Vermeidung von Streitigkeiten ist es zweckmäßig, für den Fall einer Vertragsbeendigung, gleich aus welchem Grund, das Schicksal der in der Cloud gespeicherten Daten und Software des Kunden zu regeln.
- Absicherungsmöglichkeiten des Kunden
  Dem Kunden bleibt jederzeit die Möglichkeit, die Daten in der Cloud während der Vertragsbeziehung auf eigener Infrastruktur zu sichern. Ist dies

möglicherweise wegen der Menge der Daten oder der Häufigkeit der Aktualisierung nicht zweckmäßig, kommt zudem in Betracht, mit dem Anbieter eine ausdrückliche Vereinbarung über Art und Häufigkeit der Datensicherung zu treffen, gegebenenfalls kombiniert mit einer Pflicht zur regelmäßigen Herausgabe der gesicherten Daten.

2.8 Governance, Audit-Rechte

Den Kunden treffen Sorgfaltspflichten aus den verschiedensten Bereichen, die eine uneingeschränkte Einhaltung aller gültigen Gesetze und Regeln (Compliance) im Unternehmen gewährleisten sollen. Die Verpflichtung zu dieser Einhaltung kann meist nicht vollständig delegiert werden, sondern muss zumindest durch organisatorische Vorkehrungen des Unternehmens gewährleistet werden. Die Sorgfaltspflichten müssen zunächst, sofern nicht bereits erfolgt, identifiziert werden. Dann muss genau geprüft werden, ob und in welchem Umfang der Kunde bestimmte Steuerungs- und Einflussmöglichkeiten benötigt, um seinen eigenen gesetzlichen Pflichten nachkommen zu können.

Gesetzliche Sorgfaltspflichten ergeben sich oft auch aus branchenspezifischen Sondergesetzen. Dazu zählen beispielsweise § 11 Bundesdatenschutzgesetz für personenbezogene Daten (vgl. Kapitel 3), § 238 Abs. 1 Satz 2 Handelsgesetzbuch für die Grundsätze ordnungsgemäßer Buchführung sowie die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) durch die Finanzverwaltung, § 64a Versicherungsaufsichtsgesetz für die Geschäftsorganisation von Versicherungsunternehmen, die umfangreichen Sozialdatenschutzregelungen bei Sozialleistungsträgern, § 147 Abgabenordnung für die Aufbewahrungspflichten für Geschäftsunterlagen; § 25a KWG, SOX; KontraG etc. Für bestimmte personenbezogene oder buchhalterische Daten können die gesetzlichen Sorgfaltspflichten dazu führen, dass ein Datentransfer in eine Public Cloud jedenfalls nicht möglich wäre, wenn dazu nicht besondere Maßnahmen ergriffen werden.

Dazu gehört bei der Verarbeitung personenbezogenen Daten im Auftrag des Kunden stets auch eine schriftliche Vereinbarung mit den gesetzlich geforderten Mindestinhalten (§ 11 Abs. 2 Bundesdatenschutzgesetz).

Zu gewährleisten ist insbesondere, dass der Kunde seine Pflichten etwa zur Auditierung gemäß den deutschen Datenschutzvorgaben einhalten kann. Der Kunde ist verpflichtet, selbst dafür Sorge zu tragen, dass er Kenntnis davon hat beziehungsweise sich verschaffen kann, wo seine Daten gespeichert sind. Beispielsweise mit einem allgemeinen Versprechen, dass der SaaS-Anbieter im Rahmen von Cloud-Computing-Leistungen alle gesetzlichen Regeln des Datenschutzes etc. einhalten werde, kann der Kunde seine Sorgfalts- und Überwachungsverantwortung nicht einhalten, falls dem SaaS-Anbieter eine Weitergabe dieser Zusage an den IaaS-Anbieter nicht gelingt. Oder auch eine vertragliche Verpflichtung des SaaS-Anbieters, er werde dem Kunden auf Anfrage einen Audit-Zugang beim IaaS-Anbieter verschaffen, ist ohne Zustimmung des IaaS-Anbieters wegen des Verbots eines Vertrags zu Lasten Dritter nicht wirksam. Im Zweifel empfiehlt es sich, neben dem Vertrag mit dem SaaS-Anbieter, einen Vertrag zur Auditgewährung direkt mit dem IaaS-Anbieter abzuschließen (vgl. Abbildung 18).

An dieser Stelle soll auch darauf hingewiesen werden, dass gesetzliche Vorschriften der Exportkontrolle auch dann eingreifen können, wenn eine Software gar nicht physisch exportiert wird, sondern durch Cloud Computing deren Nutzung im Ausland ermöglicht wird. Software, die Exportrestriktionen unterliegt (z.B. Dual Use Software) darf daher grundsätzlich nicht – zumindest nicht ohne Zustimmung des Bundesamts für Ausfuhrkontrolle – in einer Public Cloud zur Verfügung gestellt werden. Denn die Exportrestriktionen, die zum einen die Ausfuhrbeschränkung für bestimmte Länder und darüber hinaus auch eine Nutzungsuntersagung für bestimmte Länder (Verbot des Know-how-Transfers) enthalten, können in einer Public Cloud in der Regel nicht gewährleistet werden.

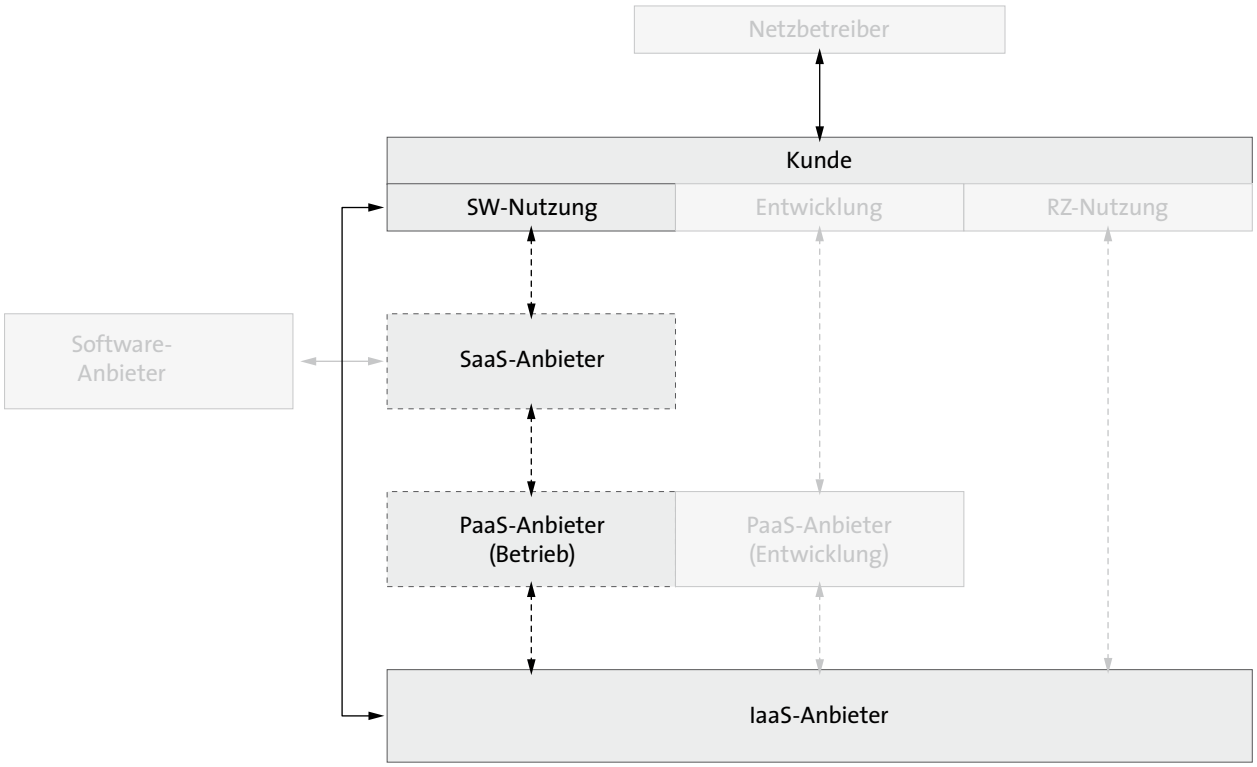


Abbildung 18: Direkter Vertrag für Auditierung

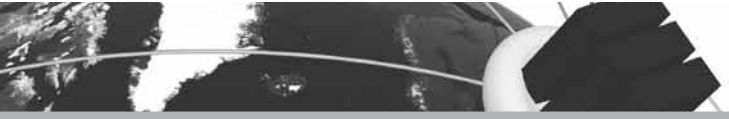
Zu den gesetzlichen Sorgfaltspflichten kommen noch die kundeninternen Vorgaben, wie Konzernregeln, Ethik- und Compliance-Regelungen hinzu, für deren Einhaltung Sorge getragen werden muss – speziell in international agierenden Konzernen und deren unterschiedlichen Abhängigkeiten.

Auch aus wirtschaftlichen Interessen kann für den Kunden ein Bedarf an Steuerungsrechten entstehen. Solche Interessen betreffen beispielsweise den besonders sorgfältigen Umgang mit sensiblen Daten und Geschäftsgeheimnissen, die nicht von einem Auftragsdatenverarbeitungs-Audit für personenbezogene Daten erfasst werden.

Als Steuerungs- und Einflussmaßnahmen kommen beispielsweise die Vereinbarung von Weisungsrechten, Kontroll-/Auditrechten, Mitbestimmungsrechten oder Reportingpflichten des Anbieters in Betracht. Eine zielführende Auswahl der Steuerungs- und Einflussmöglichkeiten setzt zudem voraus, dass der Kunde das konkrete IT-Risiko bewerten kann. Hierfür bedarf es einer großen Transparenz der Leistungen, die vom Anbieter für den Kunden vereinbarungsgemäß erbracht werden sollen. Die Einräumung von Steuerungs- und Einflussmöglichkeiten sollte nicht pauschal umfassend, sondern eher sparsam und konkret erfolgen. Sie sollte auch berücksichtigen, welche Steuerungs- und Einflussmöglichkeiten später auch tatsächlich genutzt werden oder zwingend sind, etwa weil gesetzlich vorgeschrieben.

2.9 Vergütung

Idealisierend wird in theoretischen Darstellungen von Cloud Computing die Vergütung als rein nutzungsabhängig beschrieben. Dieses Vergütungsmodell wird allerdings in vielen Fällen den Bedürfnissen und Interessen der beiden Vertragspartner in der Praxis nicht entsprechen. Nachfolgend werden daher verschiedene Vergütungs-



und Abrechnungsmodelle für die praktische Umsetzung angesprochen.

2.9.1 Vergütungsmodelle

Für die Abrechnung der durch den Anbieter erbrachten Cloud-Computing-Leistungen bieten sich eine ganze Reihe unterschiedlicher Vergütungsmodelle an, die auch bedarfsgerecht und individuell mit einander kombiniert werden können.

- Fixpreis / Flatfees
  Die einfachste Art der Abrechnung ist das Fixpreis- bzw. Flatfee-Modell. Hierbei wird gegen eine feste Zahlung pro Abrechungseinheit – typischerweise eine Zeiteinheit wie Monat, Quartal oder Jahr – eine von genutzten Volumina unabhängige Vergütung zwischen Anbieter und Kunde vereinbart. Den Vorteilen der einfachen Abrechnung und Sicherheit in der Cashflow-Berechnung steht das kalkulatorische Risiko gegenüber, dass Nutzer mehr Leistungen abrufen, als der Anbieter kalkuliert hatte. Um diesem Risiko vorzubeugen müsste der Anbieter von vornherein einen Aufschlag auf die Vergütung für das tatsächlich erwartete Nutzungsvolumen vornehmen. Dadurch erhöhte Preise würden aber auch dem Interesse des Kunden zuwider laufen.
- Pay per Use
  Anders als beim Fixpreis- bzw. Flatfee-Modell zahlt der Kunde bei Pay per Use nur die tatsächlich abgerufenen Leistungen. Damit entfällt das oben benannte kalkulatorische Risiko, gleichzeitig aber auch der Vorteil einer sicheren Cashflow-Berechnung.
- Mischmodelle
  Es liegt auf der Hand, dass beide zuvor dargestellten Modelle, also Fixpreis- bzw. Flatfee sowie Pay per Use auch bedarfsgerecht miteinander kombiniert werden können. Dies führt in der Regel zu einer fixen Basiszahlung pro Abrechnungszeitraum, ergänzt durch eine von der tatsächlichen Nutzung abhängige flexible Vergütung. Diese kann auch derart definiert werden, dass erst ab dem Überschreiten einer zuvor bestimmten Nutzungsmenge eine ergänzende variable Vergütung fällig wird. Damit kann ein guter Ausgleich zwischen den Risiken und Vorteilen der zuvor dargestellten Vergütungsmodelle erreicht werden.
- Rechnungsbegleitende Dokumentation
  Im Zusammenhang mit der Frage nach dem passenden Vergütungsmodell ist auch der Aspekt der rechnungsbegleitenden Dokumentation zu beachten. Bei den Fixpreis- bzw. Flatfee-Modellen ist die Rechnungslegung erkennbar einfach, da nur der für den jeweiligen Abrechungszeitraum fällige fixe Betrag auszuweisen ist. Komplexer wird die Abrechnung bei Pay per Use und Mischmodellen, da hier detailliert ausgewiesen werden muss, welche abrechnungsfähigen Leistungen innerhalb der jeweiligen Abrechungsperiode in Anspruch genommen wurden. Dies muss also gemessen und nachvollziehbar dokumentiert werden, was mit zusätzlichen Aufwendungen beim Anbieter verbunden sein wird.

2.9.2 Preisanpassung

Im Rahmen der Vergütung ist unabhängig von dem gewählten Vergütungsmodell das Thema der Anpassung der Vergütung zu berücksichtigen.

- Notwendigkeit der Anpassung wegen Vertragslaufzeiten
  Bei länger währenden Vertragsverhältnissen empfiehlt es sich, eine Preisanpassung vertraglich zu vereinbaren, um den sich verändernden Marktsituationen Rechnung zu tragen. Eine Möglichkeit besteht in der Vereinbarung, die Preise jährlich um einen zuvor festgelegten Prozentsatz anzupassen. Um den Bedürfnissen des Nutzers angemessen Rechnung zu tragen, kann eine solche Preisanpassung auch mit einem Kündigungsrecht verbunden werden. Dieses Kündigungsrecht ‚diszipliniert' dann den Anbieter, mit Preisanpassungen vorsichtig umzugehen. Eine derartige Klausel ist zwar komfortabel für den Anbieter, berücksichtigt jedoch eventuell sinkende Preise nicht. Da der Kunde wiederum von zukünftig fallenden Marktpreisen profitieren möchte, können diese

unterschiedlichen Interessen z. B. durch eine Benchmark-Vereinbarung in Einklang gebracht werden. Im Rahmen eines sog. Preis-Benchmarkings werden vergleichbare Leistungen und Preise verschiedener zuvor festgelegter Anbieter in festgelegten Regionen (sog. Peer Group) einem Preisvergleich unterzogen. Die Ergebnisse dieses Preisvergleiches können dann für die Preisanpassung herangezogen werden, entweder durch eine gesonderte Umsetzungsvereinbarung oder unmittelbar.

- Preisgleitklauseln
  Vertragsregelungen, die eine automatische Preisanpassung abhängig von Preisindices vorsehen, sind nur unter bestimmten Voraussetzungen zulässig. Dies gilt es bei der Gestaltung solcher Regelungen zu beachten.

2.9.3 Abrechnungsmodelle

- Vorauszahlung
  Um eine Belastung mit dem Bonitätsrisiko der Kunden zu reduzieren, empfiehlt es sich für den Anbieter bei einer Fixed Fee eine Vorkasse zu vereinbaren. Bei einer Fixed Fee und einer variablen Vergütung sowie in den Fällen einer Vergütung „Pay Per Use“ sollte eine angemessene Abschlagzahlung vereinbart werden.
- Nachträgliche Abrechnung
  Durch eine nachträgliche Abrechnung wird das Bonitätsrisiko des Kunden auf den Anbieter verlagert. Die vertraglich geschuldeten Cloud-Computing-Leistungen sind dann bereits erbracht und können bei ausbleibender Vergütungszahlung auch nicht mehr zurückgeholt werden.

2.10 Vertragsbeziehungen und Subunternehmer

In der Vertragsgestaltung für Cloud-Computing-Leistungen kommt dem Thema „Subunternehmer“ eine besondere Bedeutung zu.

Auch wenn der Kunde nur einen Anbieter von Cloud-Computing-Leistungen als Vertragspartner hat, wird dieser Anbieter häufig einzelne oder mehrere Leistungen seinerseits von Dritten beziehen. Aus Sicht des Kunden sind diese Dritten die Subunternehmer seines Vertragspartners.

Die Abbildung 19 zeigt schematisch mögliche Vertragsbeziehungen im Fall einer „Public Cloud“.

Der Netzbetreiber (Provider) stellt Kunden einen Zugang zu einem Netz (in der Regel dem Internet) zur Nutzung von Cloud-Computing-Leistungen bereit.

Kunden von Cloud-Computing-Leistungen können drei Gruppen zugeordnet werden:

- Software-(SW-)Nutzung im Rahmen von SaaS,
- Nutzung einer Entwicklungs- oder Betriebs-Plattform im Rahmen von PaaS,
- Rechenzentrums-(RZ-)Nutzung im Rahmen von IaaS.

Der Software-Anbieter liefert dem SaaS-Anbieter die Software zur Bereitstellung von SaaS, sofern der SaaS-Anbieter nicht selber Hersteller der Software ist.

Der SaaS-Anbieter stellt Kunden die Software zur Nutzung im Rahmen von Cloud Computing bereit. Er verfügt seinerseits über die Nutzungsmöglichkeiten von „Plattform“- und (RZ-)Infrastruktur-Leistungen.

Der PaaS-Anbieter kann zwei unterschiedliche „Systeme“ bereitstellen:

- ein „Laufzeitsystem“ für den SaaS-Betrieb (z.B. Verwaltung der Zugangsdaten und Ermittlung von Abrechnungsdaten)
- eine „Entwicklungsumgebung“ (z.B. um Software „Cloud-fähig“ zu machen).

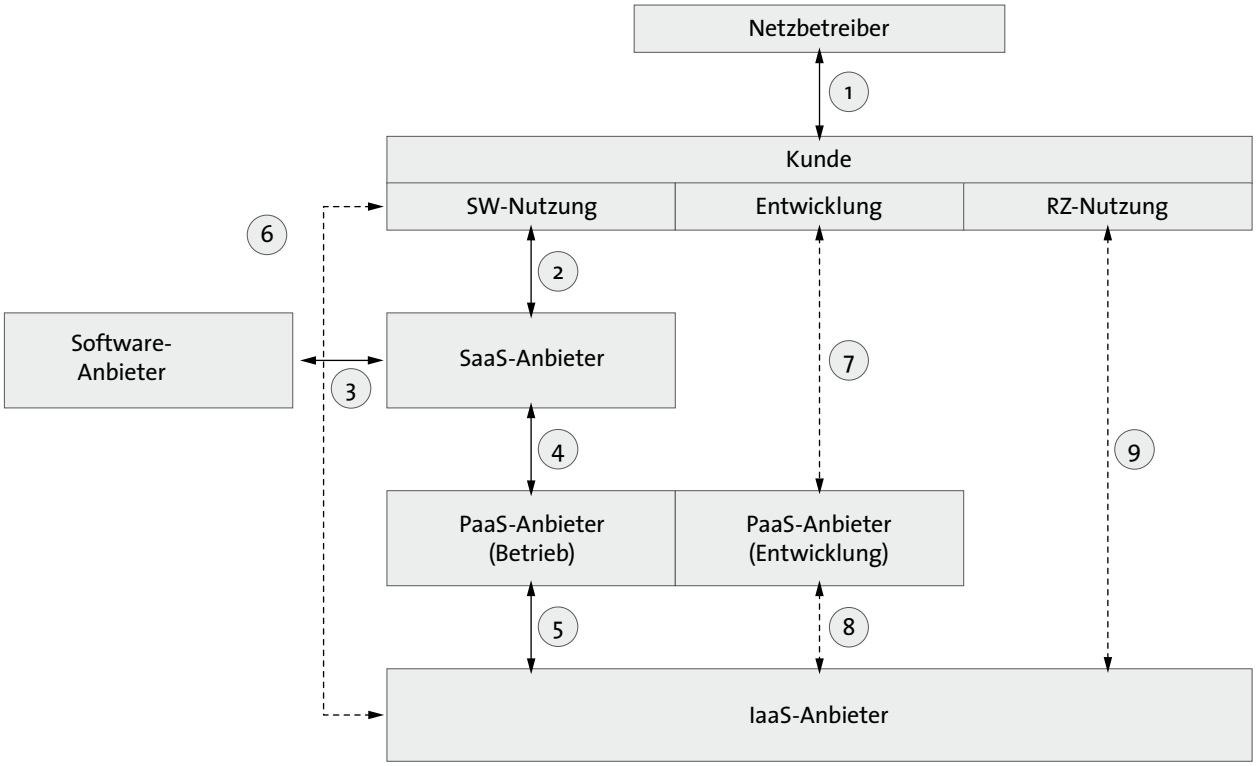


Abbildung 19: Mögliche Vertragsbeziehungen bei Cloud Computing

Der IaaS-Anbieter stellt RZ-(Infrastruktur-)Leistungen bereit.

Nachfolgend werden die in der Abbildung 19 dargestellten Vertragsbeziehungen kurz erläutert:

1 Der Vertrag zwischen Kunde und Netzbetreiber ist unabhängig vom Vertrag des Kunden mit dem SaaS-Anbieter. Für die Einhaltung eines bestimmten „Service-Levels“ (vgl. Abschnitt 2.4) bei der Nutzung von Cloud Computing müssen in zwei voneinander unabhängigen Verträgen entsprechende Vereinbarungen getroffen werden.

2 Vertrag zur Nutzung von SaaS In den meisten Fällen wird der Kunde einen „Generalunternehmer“-Vertrag mit dem SaaS-Anbieter schließen (siehe 2.2.3.). In der Vertragsgestaltung für Cloud-Computing-Leistungen kommt damit dem Thema „Subunternehmer“ eine besondere Bedeutung zu. Auch wenn der Kunde nur einen Anbieter von Cloud-Computing-Leistungen als Vertragspartner hat, wird dieser Anbieter oft mehrere Leistungen seinerseits von Dritten beziehen. Aus Sicht des Kunden sind diese Dritten die Subunternehmer seines Vertragspartners. In der Praxis wird daher häufig etwa die in Abbildung 19 dargestellte Vertragskette (2)↔(4)↔(5) vorliegen:Die Themen, die aus einer Vertragskette resultieren, sind vielfältig. Der Kunde hat meistens keine Möglichkeit, seine speziellen Anforderungen – etwa im Bereich der „Service Level“ – direkt mit einem Subunternehmer vertraglich zu regeln, hier etwa dem Plattform- und dem Infrastruktur-Anbieter. Er kann nur auf eine konsistente Vereinbarung solcher Anforderungen in der gesamten Vertragskette dringen. Auch Regelungen, die sich beispielsweise aus Vertraulichkeitserfordernissen oder Datenschutzgesetzen ergeben, müssen über drei Vertragsstufen konsistent sein. Wenn der Kunde alle erforderlichen Regelungen mit dem Anbieter als seinem Vertragspartner trifft, hat er noch keine Sicherheit, dass diese Inhalte durch entsprechende Regelungen in den weiteren Verträgen der Kette abgebildet sind. In der Regel werden dem

Kunden die Subunternehmerverträge nicht offen gelegt. Der Kunde hat meistens auch nur eingeschränkte oder keine Möglichkeiten, in seinem Vertrag mit dem SaaS-Anbieter Einfluss auf die Vertragsinhalte für Plattform- oder Infrastruktur-Leistungen von Subunternehmern des Anbieters zu nehmen. Er wird daher Wert darauf legen, dass ihm zumindest die Subunternehmer des Anbieters benannt werden (Vertrauenswürdigkeit). Für einen möglichen Wechsel eines Subunternehmers kommt ein Zustimmungserfordernis des Kunden mit entsprechender Zustimmungspflicht in Betracht, wenn der Wechsel des Subunternehmers für den Kunden keine wesentlichen Nachteile bedeutet. Als letzte Möglichkeit ist bei berechtigter Ablehnung eines neuen Subunternehmers durch den Kunden ein Sonderkündigungsrecht denkbar.

3 Der SaaS-Anbieter benötigt vom Software-Anbieter (soweit diese nicht identisch sind) ein Nutzungsrecht an der Software (vgl. Abschnitt 2.7), die ihm die Erbringung der Cloud-Computing-Leistungen ermöglicht. Häufig ist ein entsprechendes Nutzungsrecht erforderlich für eine „unbegrenzte" Anzahl von Kunden, die jeweils wiederum „beliebig" viele Nutzer haben können. Die meisten bestehenden Software-Überlassungsverträge enthalten diese Berechtigung nicht, müssen also um entsprechende Regelungen erweitert werden. Darüber hinaus benötigt der SaaS-Anbieter häufig das Recht, die Software auf „beliebig" vielen Servern zu installieren und dies möglicherweise weltweit.

4 In diesem Vertrag zwischen SaaS-Anbieter und PaaS-Anbieter wird die Nutzung des „Laufzeitsystems" der „Plattform" für den Betrieb geregelt. Dazu zählen bei der oben beschriebenen Vertragskette auch „durchgereichte" Regelungen zur Nutzung der Infrastruktur.

5 Der Zugang zur Infrastruktur wird in der Regel über einen Vertrag zwischen PaaS-Anbieter und IaaS-Anbieter geregelt.

6 Bei der Verarbeitung personenbezogener Daten und/oder „unternehmenskritischer Daten" (z.B. steuerrelevante Daten) hat der Kunde regelmäßig einen Bedarf, dass der Zugriff auf seine Daten in jedem Fall gesichert ist, etwa auch bei Insolvenz eines Subunternehmers (vgl. Abschnitt 2.7.4). Gleiches gilt auch für Prüfungsrechte des Datenschutzbeauftragten (vgl. Abschnitt 2.8) für die Verarbeitung personenbezogener Daten durch Cloud Computing. Das kann ein (zusätzliches) Vertragsverhältnis zwischen dem Kunden und dem IaaS-Anbieter erforderlich machen, wenn der Zugriff oder Zugang nicht auf andere Weise gesichert werden kann.

7 Der Vertrag mit dem PaaS-Anbieter für die Nutzung der „Plattform" als Entwicklungssystem kommt in Betracht sowohl für einen (Entwicklungs-)Kunden, der Entwicklungsspitzen abfedern will, als auch für einen SaaS-Anbieter, der seine Software als Cloud-Computing-Leistung anbieten möchte.

8 Auch für Entwicklungszwecke wird der Zugang zur Infrastruktur in der Regel über einen (Subunternehmer-)Vertrag zwischen PaaS-Anbieter und IaaS-Anbieter geregelt.

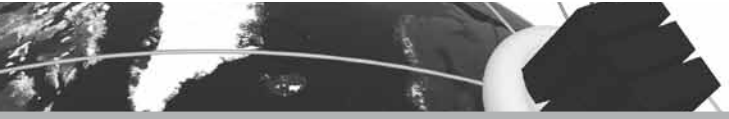
9 Ein Vertrag zwischen Kunde und IaaS-Anbieter kann die Nutzung (nur) von Rechenzentrums-Leistungen im Rahmen von Cloud Computing regeln, etwa als Kapazitätserweiterung des Rechenzentrums eines Kunden.

Die Vertragsbeziehungen und Konstellationen können bei Cloud Computing also durchaus vielgestaltig sein. Von besonderer Bedeutung ist es dabei für die Beteiligten, auf konsistente und durchgängige Vereinbarungsinhalte zu achten, die für alle Glieder einer Vertragskette gelten sollen.

2.11 Notfall-Management

Für Cloud Computing sollten ebenfalls die auch für andere von Dritten bezogenen IT-Leistungen üblichen Vorkehrungen für ein Notfall-Management vereinbart werden. Dies kann durch entsprechende Regelungen in einem Service Level Agreement erfolgen, etwa für Reaktionszeiten und Wiederanlaufzeiten.

Solche Regelungen müssen bei Cloud-Computing-Leistungen – wie bei anderen externen IT-Leistungen auch – nicht selten über mehrere Vertragsstufen vom Kunden bis zu Subunternehmern, etwa für die Infrastruktur,



„durchgereicht“ werden. Im Notfall hat der Nutzer in der Regel jedoch keinen direkten Zugriff auf Subunternehmer des Anbieters, etwa einen Betreiber der Infrastruktur. Für den „Notfall“ sollten daher bei Cloud-Computing, wie auch bei allen anderen Arten des IT-Betriebes, bei Bedarf immer eine „Ersatzlösung“ zur – ggf. eingeschränkten – Aufrechterhaltung der Arbeitsfähigkeit des Betriebes bereitstehen.

Das Risiko eines Betriebsausfalls durch Störungen im IT-Bereich ist unabhängig von der Art der IT-Organisation (eigenes Rechenzentrum, Outsourcing oder Cloud Computing). Solche Risiken sind immer durch ein entsprechendes Notfall-Management zu begrenzen. Dafür empfiehlt es sich, stets eine sogenannte „Business Impact Analyse“ (BIA, siehe BSI-Standard 100-4) durchzuführen.

Werden im Cloud Computing besonders schützenswerte Daten, etwa personenbezogene Daten oder steuerrelevante Daten, verarbeitet und gespeichert, sollten für diese Daten – unabhängig von allen vertraglichen Regelungen –- entsprechende Vorkehrungen gegen mögliche Ausfälle getroffen werden. Dazu kann etwa eine „Sicherheitskopie“ zusätzlich außerhalb der „Cloud“ gespeichert werden oder eine redundante und regional verteilte Datenhaltung vereinbart werden. Rechtlich und praktisch kann nur durch – möglicherweise parallele – Speicherung der Datenbestände im eigenen Unternehmen auch bei einer Insolvenz eines Subunternehmers sichergestellt werden, dass der Kunde im Notfall den uneingeschränkten Zugriff auf seine Daten behält.

Unabhängig von den konkret vereinbarten und praktisch umgesetzten Maßnahmen zur Notfallvorsorge sind natürlich auch Cloud-Computing-Leistungen – wie andere IT-Leistungen auch – jeweils Gegenstand der betrieblichen Notfallvorsorge und -planung.

2.12 Vertragsbeendigung

Voraussetzung für einen Anbieterwechsel ist die Beendigung des Vertrages, beispielsweise durch Zeitablauf oder Kündigung.

2.12.1 Fallgruppen der Kündigung

Im Zusammenhang mit Kündigungsrechten und –fristen ist zwischen verschiedenen Fallgruppen zu unterscheiden:

- Ordentliche Kündigung
  Im Rahmen einer ordentlichen Kündigung kann der Kunde den Vertrag nach vorheriger schriftlicher Mitteilung an den Anbieter wie zuvor vereinbart durch einseitige Willenserklärung beenden. Soweit im Vertrag weitere Rechte und Pflichten festgelegt wurden (z. B. Termination Fee, Abschlagszahlungen, Kostenersatz, Verkauf/Übergabe von Assets, Übertragung von Rechten, wie Softwarelizenzen, Patente etc.), finden diese mit Vertragsbeendigung Anwendung.
- Kündigung aus wichtigem Grund
  Bei Vorliegen eines wichtigen Grundes kann jede Partei nach Mitteilung schriftlich den Vertrag kündigen. Im Falle der Verletzung vertraglicher Pflichten hat die kündigende Partei der anderen Partei in der Regel keine Kosten zu ersetzen. Die Partei, die sich auf die Kündigung aus wichtigem Grund beruft, muss der anderen Partei (in der Regel schriftlich) ausreichend detailliert und – sofern nicht vertraglich geregelt – mit angemessener Frist die Vertragsverletzung und die Möglichkeit einer Kündigung aus wichtigem Grund mitteilen. Dabei ist regelmäßig eine angemessene „Wiedergutmachungsfrist“ zu setzen, nach deren ergebnislosem Ablauf der Vertrag außerordentlich gekündigt wird. In der Praxis sollte vor der Kündigung eines Cloud-Computing-Vertrages aus wichtigem Grund geprüft werden, welche Alternativen dem Kunden tatsächlich offenstehen, ohne die vereinbarten IT-Leistungen zu verlieren.
- Kündigung wegen höherer Gewalt
  Regelmäßig haften Anbieter und Kunde nicht für die Nichterfüllung oder Verzögerung bei der Erfüllung ihrer jeweiligen Verpflichtungen, soweit der Verzug oder die Nichtleistung direkt oder indirekt auf ein Ereignis außerhalb der zumutbaren Kontrolle der jeweiligen Partei zurückzuführen ist und nicht durch kommerziell verhältnismäßige Vorsichtsmaßnahmen, alternative Quellen oder Workarounds verhindert werden kann. Solange diese höhere Gewalt andauert,

steht der leistungsempfangenden Partei regelmäßig ein Kündigungsrecht zu.

2.12.2 Empfehlungen zum Exit

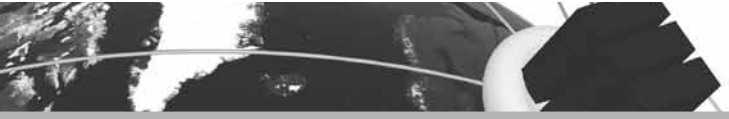
Die Ausführungen im Abschnitt 2.12 zeigen die Notwendigkeit, Exit-Management und Exit-Support von Anfang an vertraglich zu regeln. Gerade bei Cloud-Services ist es unverzichtbar, Rechte und Pflichten, technische Rahmenbedingungen und Zeitablauf nicht nur in Grundzügen zu regeln.

Idealerweise wird bereits im Vertrag vereinbart, welche Leistungen nach einer Vertragsbeendigung in welchem zeitlichen Rahmen und zu welchem Preis zu erbringen sind. Zudem ist vertraglich zu regeln, welche Partei für welche Schritte und Maßnahmen verantwortlich ist (Exit Responsibility Matrix). Die zu übergebenden Maschinen und zu übertragenden Miet-, Pacht-, Lizenz- und anderen Verträge sollten im Einzelnen aufgeführt werden. Insoweit ist zu prüfen, unter welchen Voraussetzungen diese Verträge auf den Kunden oder auf den von ihm gewählten neuen Anbieter übertragen werden können. Die Problematik des Betriebsübergangs (§ 613a BGB) ist gegebenenfalls auch bei Cloud-Services zu beachten.

Die Erfahrung zeigt, dass bei Vertragsschluss getroffene Regelungen über Exit-Management und Exit-Support in der Regel nicht alle Eventualitäten vorhersehen. Aus diesem Grund sollten entweder ein Kontingent von Projekttagen für noch nicht bekannte, aber zur Umsetzung der Kündigung notwendige, Maßnahmen geplant und kalkuliert oder zumindest Tagessätze für Unterstützungsleistungen vereinbart werden. Dies gilt insbesondere für die unverzichtbare Zusammenarbeit zwischen dem ursprünglichen und dem neuen Anbieter.

Ein stringentes Projekt- und Vertragsmanagement ist den Vertragsparteien bereits im Vorfeld von Kündigungen dringend zu empfehlen. Vertragsbeendigungen bzw. die Übertragung von laufenden Projekten auf einen neuen Anbieter erfordern regelmäßig eine zügige Bearbeitung. Service und Qualität müssen trotz widersprechender Interessen sowie Spannungen zwischen den Projektteams uneingeschränkt und unterbrechungsfrei aufrecht erhalten werden. Das Potential für Auseinandersetzungen ist in dieser Phase des Projekts enorm.

Das Ende des Exit-Supports und dessen erfolgreicher Abschluss sollte anhand einer im Vorfeld vereinbarten Checkliste geprüft und bestätigt werden.



3 Cloud Computing und Datenschutz

- Der Begriff Datenschutz bezieht sich im deutschen Recht im Wesentlichen auf personenbezogene Daten.
- Bevor personenbezogene Daten in einer Cloud-Lösung verarbeitet werden können, müssen die Voraussetzungen, die der Datenschutz dafür auferlegt, genau geprüft werden.
- Mit der dedizierten Einwilligung des Betroffenen können personenbezogene Daten in jeder Cloud-Variante verarbeitet werden.
- Die konzernweite Verarbeitung personenbezogener Daten wird national und in der EU durch Binding Corporate Rules und in Drittländern durch EU-Standardvereinbarungen vereinfacht.
- Bei der Verlagerung von personenbezogenen Daten in die USA kann die Safe-Harbor-Vereinbarung zwischen der EU und den USA genutzt werden.
- Betreiben Subunternehmer oder sonstige Dritte die Cloud, sind grundsätzlich die Bestimmungen der Auftragsdatenverarbeitung zu beachten.
- Die deutschen Aufsichtsbehörden wollen die Verantwortlichkeit für die Einhaltung von Datenschutzregeln allen an der Verarbeitung in der Cloud Beteiligten im Sinne einer „Joint Controllership“ auferlegen.
- Die Private Cloud innerhalb der EU ist zurzeit die datenschutzfreundlichste Variante des Cloud Computing.
- Die konsequente Berücksichtigung von Datenschutzgrundsätzen bei der Entwicklung neuer Cloud-Lösungen wird die Vorgabe der Zukunft sein: „Datenschutz per Software-Design“ einschließlich Verschlüsselung.

3.1 Relevanz des Datenschutzes

Datenschutz kann beim Einsatz von Cloud Computing in zwei Dimensionen Relevanz erlangen. In einer ersten Begutachtung ist festzustellen, welche Art von Daten in die Cloud-Lösung eingebracht werden. Die entsprechende Dimension der Schutzwürdigkeit reicht von „unbedeutend“ wie für allgemein verfügbare Wetterdaten bis zu „besonders hoch“ wie für individuelle Arztdiagnosen.

Die zweite Dimension ist das territoriale Schutzniveau, das in den Staaten herrscht, in denen die vorgenannten Daten in eine Cloud-Lösung eingebracht werden. Somit können nationale Bestimmungen vorsehen, dass nach deren Einstufung besonders schützenswerte Daten in bestimmte Territorien nicht oder nur unter besonderen Vorraussetzungen verbracht werden dürfen. Aus deutscher Sicht ergeben sich bei Anwendung nationaler Regelungen nur geringe Einschränkungen im EU-Raum, deutliche jedoch hinsichtlich der USA und sonstiger Drittstaaten.

3.2 Anwendbares Datenschutzrecht

Zur Beantwortung der Frage, welche gesetzlichen Regelungen zum Schutz der verarbeiteten Daten bestehen und anwendbar sind, ist die Feststellung erforderlich, wo die entsprechenden Daten verarbeitet werden und ggf. aus welcher Rechtsordnung diese Daten stammen.

Dementsprechend lässt sich bei dieser Thematik keine generelle Aussage treffen: Bei einer Private-Cloud-Lösung, die aus Deutschland stammende Daten ausschließlich auf in Deutschland betriebenen Rechnern und Speichersystemen enthält, ist lediglich deutsches Recht zu beachten. Werden dem gegenüber in einer Public Cloud Daten aus unterschiedlichen Staaten auf Rechnern und Speichersystemen in unterschiedlichen Ländern gehalten, sind in der Regel auch internationale bzw. verschiedene nationale Rechtsnormen zu beachten. Soweit die territoriale Verbreitung der Daten und Rechnersysteme sich auf die Staaten der europäischen Gemeinschaft beschränkt, sind neben dem nationalen Recht auch EU-Verordnungen und Richtlinien einschlägig. Dies führt zwangsläufig zu einer sehr differenzierten Betrachtung der Cloud-Computing-Lösungen unter datenschutzrechtlichen Aspekten.

Da dieser Leitfaden Anbieter und Nutzer von Cloud-Computing-Lösungen in Deutschland adressiert, betrachten die nachfolgenden Ausführungen die datenschutzrechtlichen Anforderungen aus dem Blickwinkel des dem deutschen Recht unterworfenen Lesers.

3.2.1 Der Begriff Datenschutz

Die im Rahmen des Cloud Computing verarbeiteten Daten können vielfältig sein (vgl. Abbildung 20): Sie umfassen allgemeine Daten inklusive Wirtschaftsdaten wie Statistiken, Bilanzen, Konstruktions- und Produktionsdaten oder Verkaufszahlen. Derartige Daten können für die rechtmäßigen Autoren der Daten, z.B. Industrieunternehmen, von sehr hoher Bedeutung sein. Sie sind daher als vertraulich und ggf. auch als geheim einzustufen. Dementsprechend sind diese Daten von den Verantwortlichen der jeweiligen Unternehmen vor fremdem Zugriff zu schützen. Hier gelten die allgemeinen gesellschaftsrechtlichen Regelungen des Aktien- und des GmbH-Gesetzes. Danach haben Geschäftsführer bzw. Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen gewissenhaften Geschäftsleiters anzuwenden (vgl. § 43 GmbHG und § 93 AktG). Im Vordergrund steht hierbei somit ein allgemeiner Datenschutz im Sinne von Datensicherheit.

Gleichermaßen haben die Verantwortlichen sicherzustellen, dass die handels- und die steuerrechtlichen Bestimmungen eingehalten werden. Im Vordergrund stehen dabei die Pflicht zur Archivierung unveränderbarer Geschäftsdaten und deren gezielte Auffindbarkeit im Prüfungsfalle. Diese Pflichten ergeben sich zum Beispiel aus dem Handelsgesetzbuch (§ 257 HGB) oder der Abgabenordnung (§ 147 AO) sowie deren nachgelagerten Ausführungsbestimmungen wie die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“ des Bundesministeriums der Finanzen.

3.2.2 Datenschutz im engeren Sinne

Eine Untermenge der allgemeinen Daten sind die persönlichen Daten, z.B. Telefongespräche oder E-Mails, die durch das Telekommunikationsgesetz (TKG), geschützt sind, und die personenbezogenen Daten. Letztere werden in § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) wie folgt definiert: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“ Diese Daten unterliegen nach deutschem Sprachgebrauch dem Datenschutz im engeren Sinne. Insbesondere diesen Daten widmen sich die nachfolgenden Ausführungen.

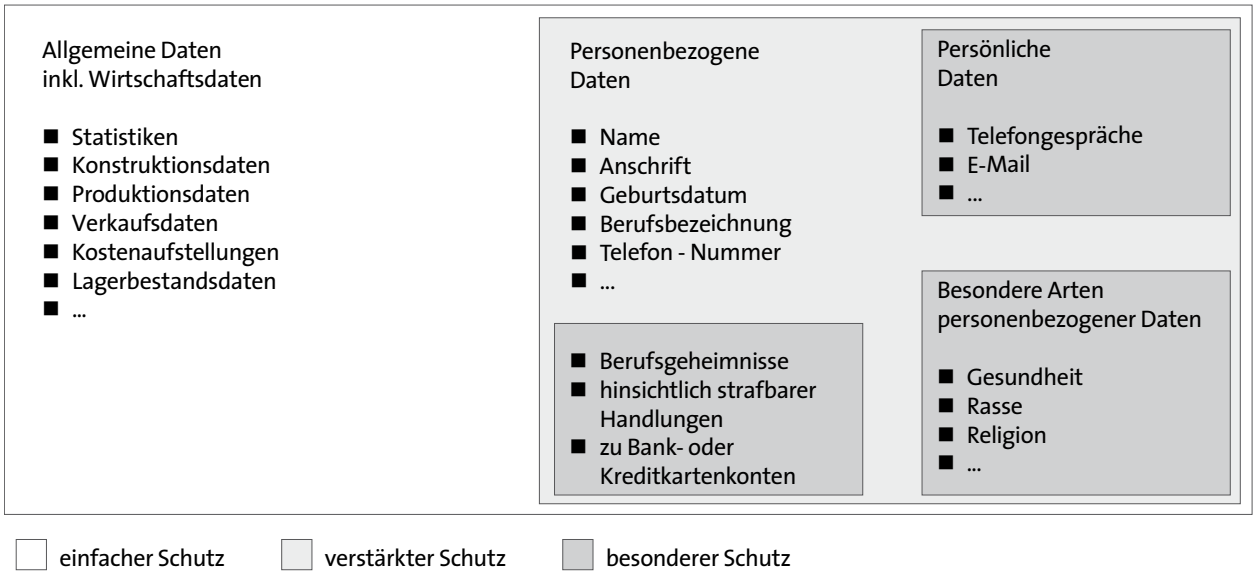


Abbildung 20: Kategorien von Daten und Datenschutz

3.2.3 Weitere Begriffsbestimmungen

Die Regelungen des BDSG zu personenbezogenen Daten sind subsidiär, sofern spezifische Rechtsnormen Bestimmungen zum Datenschutz enthalten. Dies ist zum Beispiel der Fall, wenn derartige Daten zur Bereitstellung von Telemedien in einer Cloud eingestellt sind. Dementsprechend ist der § 12 Telemediengesetz (TMG) anwendbar.

Als Normadressat muss die „verantwortliche Stelle" die datenschutzrechtlichen Bestimmungen beachten. Dabei handelt es sich nach § 3 Abs. 7 BDSG um „jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt". Auf Grund der vielfältigen Einzelaktivitäten, die unter dem Begriff „Verarbeiten" zu subsumieren sind und von speichern über verändern bis zu löschen reichen (vgl. Abbildung 21), bedarf es detaillierter Prüfungen der Maßnahmen in der Cloud, um festzustellen, ob die datenschutzrechtlichen Bestimmungen einschlägig sind. Das Gesetz knüpft teilweise unterschiedliche Rechtsfolgen und Anforderungen an die jeweiligen Aktivitäten.

Abbildung 21: Definition der Datenverarbeitung nach § 3 BDSG

3.2.4 Einwilligung

Im deutschen Datenschutzrecht gilt der Grundsatz des „Verbots mit Erlaubnisvorbehalt". Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist daher nach § 4 BDSG verboten, sofern nicht eine spezielle Erlaubnis durch Rechtsnorm oder die vorherige Einverständniserklärung des Betroffenen erteilt ist.

Die datenschutzrechtlichen Restriktionen können in der überwiegenden Mehrzahl der Anwendungsfälle mittels Einwilligung aufgehoben werden. Erforderlich ist jedoch, dass der Betroffene den detaillierten Sachverhalt der Datenverarbeitung kennt und die Einwilligung freiwillig, d.h. ohne sozialen oder wirtschaftlichen Druck, erteilt.

Ergänzend ist allerdings festzuhalten, dass eine einmal gegebene Einwilligung nicht bedeutet, dass mit den erhobenen personenbezogenen Daten nach Belieben verfahren werden kann. Selbstverständlich dürfen Daten nur im Rahmen der gegebenen Erklärungen und Hinweise (zweckgebunden) verarbeitet werden – auch in einer Cloud. Es kann jedoch je nach Cloud-Typ und Geschäftsmodell schwierig sein, diesen Rahmen im Voraus fest zu legen. Bei hinreichend definierten Private Clouds sind Umfang und Lokation der Verarbeitung begrenzbar. In Public Clouds kann weder vorhergesagt werden, wo und wann genau die Daten verarbeitet werden, noch wie viele Verarbeiter die Wolke letztlich bilden.

Schließlich ist darauf hinzuweisen, dass Einwilligungen widerruflich sind und in den Systemen diese Möglichkeit als Option berücksichtigt werden sollten.

3.3 Datenschutzrechtliche Einordnung der Private Cloud

Die eigene Private Cloud wirft zunächst keine besonderen Probleme auf – soweit die Einspeisung von personenbezogenen Daten in eine Cloud auf deutschem Territorium stattfindet und die sogenannte verantwortliche Stelle ihren Sitz bzw. ihre Niederlassung in Deutschland hat. Dabei sind insbesondere die einschlägigen deutschen Vorschriften zu beachten: Je nach Leistungsangebot auf den drei Service-Ebenen und den betroffenen Daten (vgl. Abbildung 22) können diese von BDSG und TKG über SGB X und StGB (z.B. § 203: Verletzung von Privatgeheimnissen) bis hin zu KWG und Abgabenordnung (AO) zur Anwendung kommen.

Das deutsche Datenschutzrecht sieht allerdings kein Konzernprivileg vor. Werden daher in der eigenen Private Cloud Service-Leistungen von verbundenen Unternehmen (z.B. Schwester- oder Tochtergesellschaften) einbezogen, sind mit diesen rechtlich selbstständigen Einheiten spezifische Regelungen zu treffen.

3.3.1 Corporate Binding Rules

Mit konzerninternen Vorgaben und Richtlinien können Unternehmen sicherstellen, dass in allen rechtlich selbständigen Einheiten des Konzerns das gleiche Datenschutzniveau besteht. Dabei handelt es sich um freiwillige Selbstverpflichtungen der Unternehmen, die aber gegenüber den Mitarbeitern wie Dienstanweisungen durchgesetzt werden können. Derartige Binding Rules sind nicht nur in Deutschland einzusetzen, sondern auch in der EU, da auf Grund der EU-Datenschutzrichtlinie 95/46 aus dem Jahre 1995 von einem gleichartigen Schutzniveau in den EU-Mitgliedsstaaten und den zusätzlichen Staaten des Europäischen Wirtschaftsraums (EWR) auszugehen ist. Dies gilt gleichermaßen für Staaten wie Kanada und die Schweiz, denen die EU-Kommission ebenfalls ein angemessenes Schutzniveau attestiert.

3.3.2 Standardvertragsklauseln

Zur Übertragung von personenbezogenen Daten in Drittländer verlangt das BDSG auf Grundlage der EU-Datenschutzrichtlinie, dass ein dem deutschen Datenschutz vergleichbares und angemessenes Datenschutzniveau bei der empfangenden Stelle gewährleistet ist. Außerhalb der EU und des europäischen Wirtschaftsraums geht der Gesetzgeber grundsätzlich nicht davon aus, dass in den Drittländern auf Grund ihrer innerstaatlichen

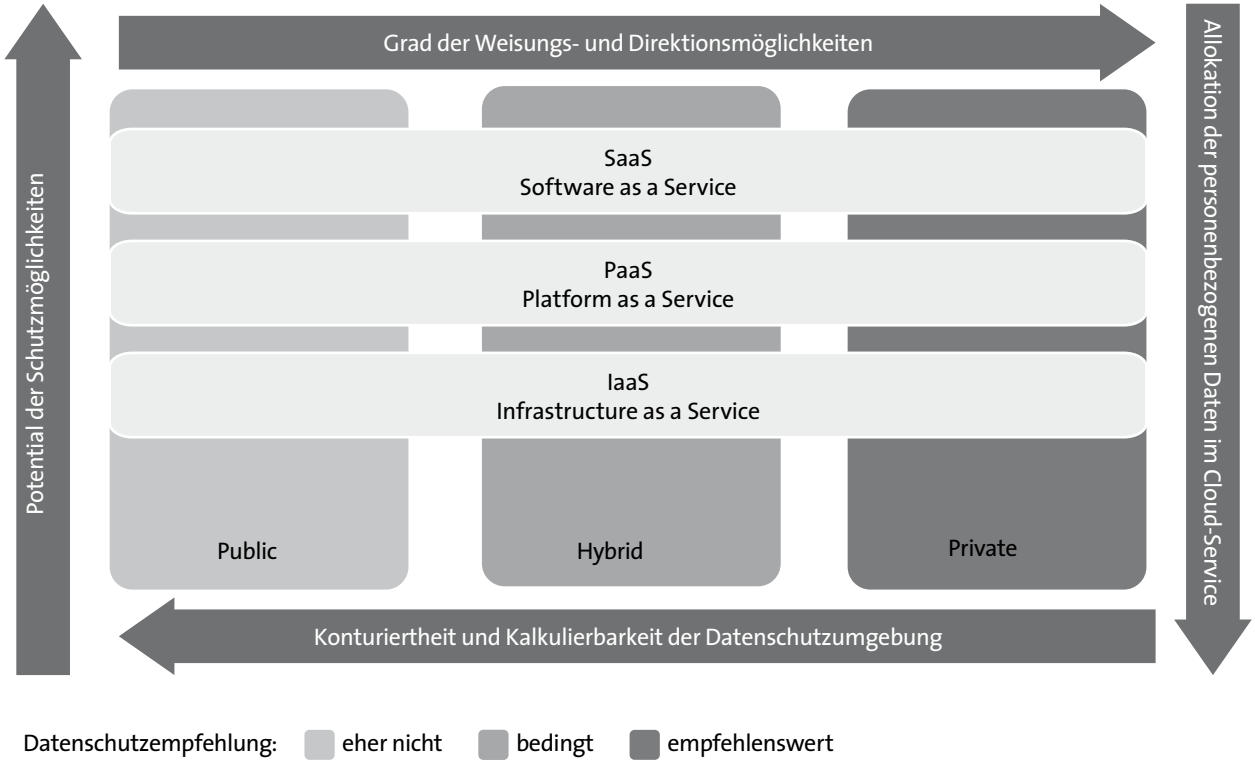


Abbildung 22: Datenschutz-Dynamik in der Cloud

Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Datenschutzniveau besteht. Zur Lösung dieses Problems erklärte die EU-Kommission die Nutzung von Standardvertragsklauseln als geeignetes Mittel, die sie 2001 verabschiedete und in den vergangenen Jahren modifizierte. Dabei folgte die Europäische Kommission in ihrem Beschluss der internationalen Entwicklung und Gepflogenheit überregional tätiger Konzerne, ihre Geschäftsbeziehungen grenzunabhängig zu betreiben. Und genau hier ist auch ein wesentliches Geschäftsmodell der Clouds anzusiedeln.

Sind daher die Unternehmenstöchter eines international operierenden Konzerns z.B. alle durch EU-Standardverträge verbunden, erübrigt sich auch bzgl. der meisten personenbezogenen Daten das Drittstaatenproblem, solange die Daten den Konzern im Drittstaat nicht verlassen.

Strittig ist jedoch, ob die Standardvertragsklauseln durch den Katalog von Schutzmaßnahmen des § 11 Abs. 2 BDSG zur Auftragsdatenverarbeitung ergänzt werden müssen, wenn die verantwortliche Stelle ihren Sitz in Deutschland hat.[25]

In diesem Zusammenhang ist darauf hinzuweisen, dass auf Grund der föderalen Struktur Deutschlands mit 16 Landes- und einer Bundesaufsichtsbehörde durchaus unterschiedliche Auffassungen in der Auslegung der europäischen und deutschen Datenschutzbestimmungen bestehen.

25. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Ein modernes Datenschutzrecht für das 21. Jahrhundert. Eckpunkte vom 18. März 2010 Nr. 2.3

3.3.3 Safe Harbor

Im Jahr 2000 hat die EU-Kommission das Safe-Harbor-Abkommen mit der US-Regierung geschlossen. Safe Harbor ist somit die nordamerikanische Datenschutz-Speziallösung, die auf einem Eintrag des amerikanischen Datenempfängers in die entsprechende Liste des US-Handelsministeriums beruht.[26] Damit einher geht die Anerkennung von bestimmten datenschutzrechtlichen Maßnahmen. Diese Selbstverpflichtung auf Einhaltung von europäischen Datenschutzstandards wird in regelmäßigen Abständen, die in der Liste auch genannt sind, erneuert (Zertifizierung).

Nach dem Beschluss des Düsseldorfer Kreises vom 28.04.2010[27] muss die Einhaltung des Datenschutzniveaus in den Mindestkriterien allerdings aktiv überprüft werden. Sollen also personenbezogene Daten in der Cloud eines in den USA gelegenen Unternehmens verarbeitet werden, so ist laut Düsseldorfer Kreis zu prüfen:

- der schriftliche Nachweis über den Beitritt zum Abkommen
- der Nachweis über die Einhaltung der Informationspflichten des Unternehmens nach Safe Harbor gegenüber den von der Datenverarbeitung Betroffenen.

Die besonderen Informationspflichten der Unternehmen nach Safe Harbor sind darüber zu informieren,

- zu welchem Zweck das Unternehmen die Daten erhebt und verwendet,
- welche Kontaktmöglichkeiten es bei Nachfragen oder Beschwerden gibt,
- an welche Kategorien von Dritten die Daten weitergegeben werden,
- welche Mittel und Wege zur Verfügung gestellt werden, die Weitergabe einzuschränken.

Diese Angaben sind unmissverständlich und deutlich bei der ersten Erhebung oder spätestens bei Zweckänderung zu machen.

Die Überprüfung kann durch Dritte bzw. beauftragte Unternehmen vor Ort vorgenommen werden. Die Schwierigkeiten und Unsicherheiten, die sich aus den Überprüfungen ergeben können, führen häufig dazu, dass US-Firmen Cloud-Lösungen anbieten, die ausschließlich mit Rechner- und Speichersystemen auf dem europäischen Kontinent betrieben werden.

Hier hat die verantwortliche Stelle es sprichwörtlich „in der Hand“, alle Datenschutzkomponenten einzurichten.

Das ist jedoch eher nicht die Regel und schon gar nicht der Trend. Outsourcing gerade im Bereich Storage und auch Personaldatenverarbeitung durch externe Anbieter werden immer stärker genutzt.

3.4 Auftragsdatenverarbeitung

Wird eine Cloud-Lösung nicht ausschließlich von einem Unternehmen (verantwortliche Stelle) für eigene Geschäftszwecke betrieben, ist zu prüfen, ob eine Auftragsdatenverarbeitung vorliegt. Ist das der Fall, so kommen grundsätzlich die gleichen Regelungen wie bisher beim klassischen IT-Outsourcing zur Anwendung. Insbesondere die Regeln des § 11 BDSG sind insbesondere seit der Änderung des BDSG am 01.09.2009 zu beachten. Wichtig sind dabei die vertragliche Fixierung des „10-Punkte-Katalogs“, die nunmehr festgeschriebene Vorabprüfung nach § 11 Abs. 2 Satz 4 und die Dokumentationspflicht nach § 11 Abs. 2 Satz 5 BDSG.

26. https://www.export.gov/safehrbr/list.aspx
27. so z.B. die Aufsichtsbehörde Unabhängiges Landeszentrum für Datenschutz und Informationsfreiheit Schleswig-Holstein, wobei deren Vorsitzender im übrigen davon ausgeht, dass die Verarbeitung von personenbezogenen Daten außerhalb der EU/EWR mangels fehlender Umsetzung von Datenschutzmöglichkeiten in den Drittstaaten grundsätzlich auch unzulässig sein kann - so auf dem IT-Rechtstag, Juni 2010 in Österreich , https://www.datenschutzzentrum.de/cloud-computing/

Wie die Verarbeitung von personenbezogenen Daten außerhalb Deutschlands durchaus Raum gewinnt, zeigt eine von PricewaterhouseCoopers durchgeführte Befragung von Cloud-Anbietern.[28] Immerhin 39 Prozent der befragten Unternehmen lassen in Rechenzentren in den USA, weitere 24 Prozent in Ländern außerhalb der EU (exkl. USA) personenbezogene Daten verarbeiten (vgl. Abbildung 23).

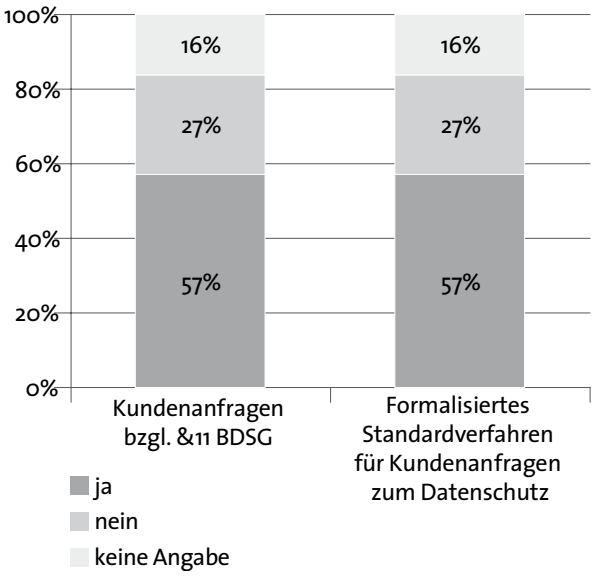


Abbildung 23: Lokation der Verarbeitung

Eine weitere Frage in der Studie zielte darauf, wie Rechenzentrumsbetreiber auf Kundennachfragen zu Maßnahmen nach § 11 BDSG (Auftragsdatenverarbeitung) reagieren bzw. aufgestellt sind. So waren 57 Prozent der befragten Unternehmen mit einem formalen Standardverfahren gerüstet, 27 Prozent jedoch auf eine solche Kundenanfrage nicht vorbereitet (vgl. Abbildung 24).[29]

In diesem Bereich sollten die Anbieter besser aufgestellt sein, denn wie die Vergangenheit gezeigt hat, können Datenlecks gerade in der Cloud massive Datenkompromittierung oder Datenverluste nach sich ziehen.

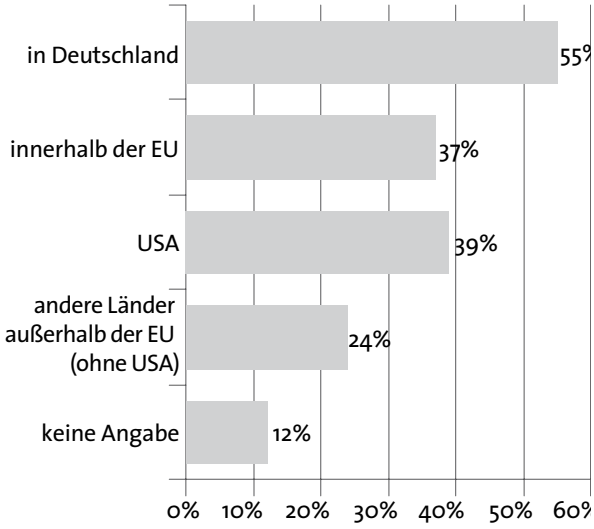


Abbildung 24: Kundennachfragen zum Datenschutz

3.4.1 Managed Private Cloud

Ende 2001 wurden spezielle EU-Modell-Standardvertragsklauseln für Auftragsdatenverarbeiter in Drittländern verabschiedet, die mittlerweile ein eingeführter Standard sind. Im Februar 2010 wurden sie in überarbeiteter Form veröffentlicht. Danach müssen sich die in den Cloud-Betrieb eingebundenen Partnerbetriebe (Subunternehmer) den Weisungen der verantwortlichen Stelle unterwerfen. Nur so ist die Sicherstellung der datenschutzrechtlichen Vorgaben durchgängig möglich, die der Anbieter seinen Kunden gegenüber zu erbringen hat.

Dementsprechend ist auch die Managed Private Cloud meist als Auftragsdatenverarbeitung nach § 11 BDSG einzustufen.

Sollten darüber hinaus mehr als eine verantwortliche Stelle im Drittland bei der Verarbeitung von Daten in der Cloud mitwirken, wird durch eine Einbindung der Unterauftragsverarbeiter / Cloud-Betreiber durch diese Modell-Standardvertragsklauseln der Schutz der betroffenen Kundendaten einklagbar gewährleistet.

28. Vgl.: Vehlow, Markus; Golkowsky, Cordula (2010): Cloud Computing, Navigation in der Wolke. PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft, S. 43.
29. ebenda

Zudem ist garantiert, dass die Zweckbindung durchgängig erhalten bleibt, da auch diese in den neuen Standardverträgen unabdingbar zum Vertragsinhalt zwischen Auftraggeber in der EU und den Drittstaatenverarbeitern wird.

3.4.2 Abgrenzung Auftragsdatenverarbeitung zu Datenweitergabe an Dritte

Bei der Datenverarbeitung in Drittstaaten stehen die Regeln der §§ 4b, c in Verbindung mit § 28 BDSG zur Verfügung (Fälle der Übermittlung bei der sogenannten Funktionsübertragung). Die Regelungen des § 28 BDSG enthalten erheblich restriktivere Bestimmungen und Vorgaben als die für die Eigen- oder Auftragsdatenverarbeitung. Meistens wird jedoch die kontrollierte, durch Weisungen gesteuerte Verarbeitung der erhobenen personenbezogenen Daten gewünscht sein, schon allein um eine Zweckentfremdung der Daten zu vermeiden. Dann sind jedoch auch die in der Stellungnahme des BITKOM zur Auftragsdatenverarbeitung niedergelegten Prinzipien und Varianten passend und hilfreich.[30]

In der Abbildung 22 finden sich ausgehend von den Cloud-Organisationsformen „Public", „Hybrid" und „Private" eine Ampel-Matrix aus den Parametern Weisungs- und Direktionsmöglichkeiten, Volumen des Cloud-Service, Obscurity und Unkalkulierbarkeit der Datenschutzumgebung sowie dem Potential der Schutzmöglichkeiten je nach Service-Ebene.

Die farbliche Unterscheidung der drei Cloud-Organisationsformen signalisiert auch die Empfehlung für eine Nutzung für personenbezogene Datenverarbeitung.

3.4.3 Mehrere verantwortliche Stellen

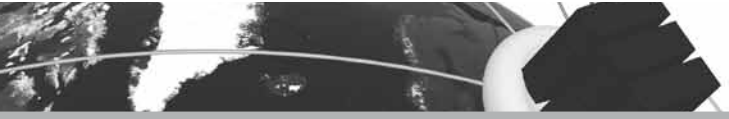
Völlig neue Aspekte ergeben sich, wenn an der Verarbeitung mehrere verantwortliche Stellen mitwirken. Diese mögliche Vertragssituation hat z.B. der Düsseldorfer Kreis in seinem Eckpunktepapier vom 18.03.2010 als Thema für zukünftige Regelungen im modernen Datenschutz aufgegriffen.[31] Die Arbeitsgruppe der Landesdatenschutzbeauftragten kommt zu dem Schluss, dass beim Mitwirken mehrerer Verantwortlicher in der Cloud die bisherigen Instrumente der rechtlichen und tatsächlichen Kontrolle und Steuerung, wie z.B. Auftragsdatenverarbeitung oder Funktionsübertragung, nicht mehr vollständig passen. Ein Vorschlag geht wieder zurück zur gemeinsamen EG-Richtlinie 95/46, wo unter Art. 2 lit. (d) von für die „Verarbeitung gemeinsam Verantwortlichen" die Rede ist, der sogenannte „Joint Controllership".

Diese neue Ansicht der Datenschutzzuständigkeit führt uns zu dem Begriff der sogenannten Accountability – der nachhaltigen Verantwortlichkeit: Jede Stelle ist verantwortlich, wenn und soweit sie in tatsächlicher Hinsicht über Mittel und Zwecke der Datenverarbeitung verantwortlich bestimmen kann. Als Folge davon sollen Betroffene ihre Datenschutzrechte bei jedem Verantwortlichen geltend machen können.

3.4.4 Innereuropäische Verarbeitungsketten

Eine zunehmend praktizierte Form der Datenverarbeitung ist die Einschaltung von Sub-Subunternehmern, also die Bildung von Ketten in der Weitergabe von (personenbezogenen) Daten.

30. http://www.bitkom.org/files/documents/BITKOM_Echo_Duesseldorfer_Kreis_Int__ADV.pd
31. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Ein modernes Datenschutzrecht für das 21. Jahrhundert. Eckpunkte vom 18. März 2010 Nr. 2.3



Wenn man das europäische Datenschutzniveau als Maßstab heranzieht, ist eine rein europäische Cloud-Lösung unproblematisch. Es gilt das Sitzlandprinzip (im BDSG § 1 Abs. 5), Grenzüberschreitungen schaden daher nicht. Die Auftragsdatenverarbeitung nach § 11 BDSG (aus „deutscher Sicht“) kann an alle in der Kette befindlichen Unternehmungen verlängert werden. Alle in der Vertragskette befindlichen Unternehmen sind dann Teil der verantwortlichen Stelle.

Auch die Funktionsübertragung, sozusagen die „Werksdienstleistung“ bei der Datenverarbeitung personenbezogener Daten (z.B. die vollständige Abwicklung der Lohn- und Gehaltsbuchhaltung oder die CRM-Analytik) ist innerhalb der EU/EWR und anerkannten Staaten unproblematisch. Aber auch hier sind wieder Ausnahmen zu beachten, vor allem wenn es sich um Gesundheitsdaten handelt.

Die hierfür notwendigen Verträge sind allerdings sowohl für die Auftragsdatenverarbeitung als auch für die Funktionsübertragung so zu formulieren, dass die „Endkontrolle“ der Lieferung/Leistung der auftraggebenden Stelle vorbehalten ist.

3.5 Datenschutzrechtliche Einordnungen der Public Cloud

Wie sich aus der Definition der Public Cloud und aus den vorstehenden Ausführungen zur Auftragsdatenverarbeitung ergibt, wird die Public Cloud in der Regel nur eingeschränkt oder mit erheblichem Aufwand in technischer und organisatorischer Hinsicht für die Verarbeitung personenbezogener und vor allem besonders geschützter Daten nutzbar sein.

3.5.1 Virtual Private Cloud

Gleichermaßen stellt es eine erhebliche Herausforderung für die verantwortliche Stelle dar, den Schutz personenbezogener Daten auf dem nach deutschem Datenschutzrecht geforderten Schutzniveau zu gewährleisten. Auf Grund der unterschiedlich auszugestaltenden Verschlüsselungstechnik, der eine zentrale Rolle zukommt, wird hier ganz besonders die Einzellfallprüfung im Vordergrund stehen.

3.5.2 Hybrid Cloud

Abhängig von der technischen und organisatorischen Ausgestaltung einer Hybrid Cloud wird der Zuordnungsaufwand erheblich sein, welche datenschutzrechtlichen Bestimmungen für welche Leistung oder Funktionalität einschlägig sind. Entscheidend sein kann dabei eine intelligente Trennung zwischen der Verarbeitung von z. B. sensiblen Daten in einem Private-Cloud-Umfeld und von nichtpersonenbezogenen Daten im Public-Cloud-Umfeld.

3.6 Technisch-organisatorische Maßnahmen

Zahlreiche Maßnahmen können die Nutzung des Cloud Computing in datenschutzrechtlich einwandfreier Form ermöglichen. Einige seien hier beispielhaft aufgeführt.

3.6.1 Prüfung und Bewertung eines Cloud-Anbieters

Grundsätzlich empfiehlt sich die Prüfung und Bewertung eines Cloud-Anbieters durch die Einführung eines sogenannten Privacy Impact Assessments in Verbindung mit einem Security-Audit zur Risikoabwägung und Dokumentation vor dem Start des Datentransfers und der Datenverarbeitung.

Der Katalog der Maßnahmen entsprechend der Anlage zu § 9 BDSG ist standardmäßig als Prüfgrundlage heranzuziehen. Die dort geregelten Kontrollmaßnahmen gehören in die Vorabprüfung einer jeden Cloud-Variante und der Nachweis der auszuführenden Kontrollen ist zu dokumentieren.

Grundsätzlich sollte dabei an folgende Risiken gedacht werden, wobei Datenschutz und -Sicherheit auf allen Verarbeitungs-Layern (Applikations-, Datenbank-, Netzwerk- und Datensatz-Ebene) berücksichtigt sein sollen:

- Missbrauch durch Zweckentfremdung von Daten durch Kriminelle
- Unsichere API: dadurch Eindringen krimineller Elemente möglich
- interner Missbrauch durch Subunternehmerketten und schlecht integrierte Mitarbeiter
- Übergriffe aus parallelen Accounts durch schlechte Mandantentrennung (Segregation)
- Datenverluste durch Sicherheitslöcher
- Account-Jacking u. ä.
- Fehlendes oder nur vorgegebenes Sicherheitskonzept
- Cloud-Provider-Migration – wer ist Herr der Daten?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierzu als Diskussions-Grundlage am 27.09.2010 einen Entwurf für Mindestsicherheitsanforderungen an Cloud-Anbieter veröffentlicht, der die komplexen Vorüberlegungen auch aus Datenschutzsicht aufgreift und mit den Sicherheitsanforderungen an den Auftragnehmer/Anbieter verknüpft (vgl. Abbildung 25).[32]

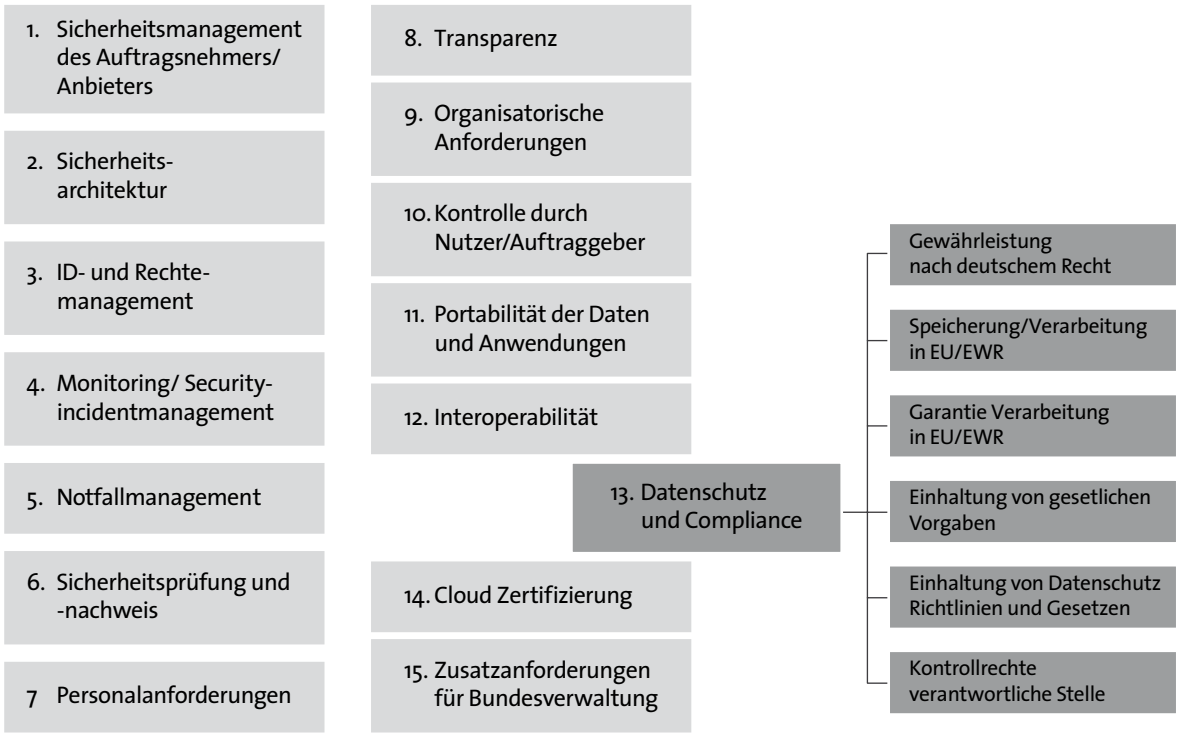
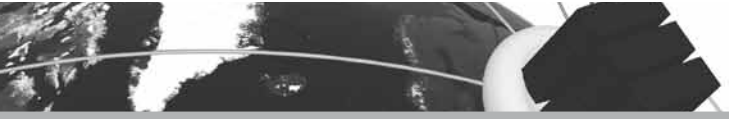


Abbildung 25: 15-Punkte-Check des BSI für Cloud-Anbieter

32. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sonstige/Cloud_Computing_Mindestsicherheitsanforderungen.pdf?__blob=publicationFile#download=1



3.6.2 Kontrollmöglichkeiten

Aus dem Blickwinkel der vorauszusetzenden Kontrollmöglichkeiten wird sich der Aufwand nicht auf einige wenige Maßnahmen beschränken können. Als eine der wirksamsten ist jedoch der Schutz durch ein Verschlüsselungsverfahren gemäß dem Stand der Technik zu wählen. Dies ist neuerdings auch durch die geänderte Anlage zu § 9 Satz 1 BDSG ausdrücklich als Maßnahme der Zugangs-, Zugriffs- und Weitergabekontrolle vorgesehen.

Unabhängig und parallel davon ist die Berechtigung, also die Zugangs- oder Zugriffsrechte-Regelung, zu aktivieren. Der Nachweis des betriebenen Aufwands durch Vorlage eines aktuellen Zertifikats oder Prüfberichts des Datenschutzbeauftragten der verarbeitenden Unternehmung, ein Datenschutzaudit gem. § 9a (wohl eher nur bei deutschen Anbietern) oder der Nachweis einer bestandenen ISO-Zertifizierung im Bereich Datenschutz sind Merkmale eines sicheren Vorgehens zum Schutz der personenbezogenen Daten von Kunden oder Mitarbeitern in der Cloud.

3.6.3 Einbindung eines Subunternehmers

Die Einbindung eines Subunternehmers (im Ausland) ist wahrscheinlich, wenn Data- Center im Ausland genutzt werden. Die praktische Frage aber bleibt – wer kontrolliert den Subunternehmer? Empfehlenswert, aber nicht unbedingt preisgünstig, ist eine direkte Auditierung der Systeme und deren Sicherheitsvorkehrungen und Logs des Anbieters und Auftragnehmers, was vor allem im Ausland auch durch Dritte bewerkstelligt werden kann.

Die European Network and Security Agency (ENISA) bringt in ihrer Risikobewertung ebenfalls den hohen Risikograd beim unbedachten Cloud Computing zum Ausdruck.[33] Reputationsverlust, Kundenvertrauen, sensible oder kritische Personaldaten und Serviceleistungen können als Firmen-Assets betroffen werden.

Die verantwortliche Stelle, die sich der Subunternehmer bzw. einer Kette von Subunternehmern bedient, bleibt immer für die Verarbeitung in der Haftung und kann sich nicht mit Nichtwissen exkulpieren oder die Haftung abbedingen.

Das gilt auch, wenn die verantwortliche Stelle / unmittelbarer Vertragspartner des Auftraggebers Datenlecks nicht an den Auftraggeber weitermeldet. Mit zunehmender Zahl der eingebundenen Cloud-Betreiber steigt demgemäß das Risiko, die Kontrolle über die Daten vollends zu verlieren.

3.6.4 Anonymisierung und Verschlüsselung

Ein weiterer Ansatz für die datenschutzkonforme Cloud-Nutzung ist die Überlegung, durch eine entsprechende datenschutzgerechte Cloud-Softwarelösung (Datenschutz per Design) den zu verarbeitenden Daten die Eigenschaft „personenbezogen“ zu nehmen.

Dies kann durch eine Anonymisierung der Daten geschehen. Dabei werden diejenigen Merkmale separat gespeichert, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (§ 30 Abs. 1 BDSG). Diese Lösung entfällt allerdings da, wo für die verantwortliche Stelle bei der Verarbeitung der Namensbezug wichtig bleibt.

Auch die Pseudonymisierung kann helfen, den Datenschutz im Drittland zu stärken. Aus dem gleichen Grund wie beim Anonymisieren ist diese Möglichkeit allerdings nur von begrenztem Wert in der praktischen Anwendung.

Es bleibt aber in vielen Fällen die Möglichkeit der Verschlüsselung auf der Softwareebene. Eine komplett verschlüsselte Personal-Datenbank ist im Sinne des BDSG ohne Personenbezug, solange der Zugang zu den Daten

33. http://www.enisa.europa.eu/

darin ohne Schlüssel nicht möglich ist, ja noch nicht einmal zu erkennen ist, dass hier Daten mit Personenbezug verarbeitet werden. Bleibt der Schlüssel zudem im Bereich der EU/EWR, so können auch nicht vorhersehbare Zugriffe[34] keinen Schaden anrichten.

Insbesondere bei diesen Maßnahmen wird erkennbar, dass die Vorbereitung eines Cloud-Projekts entscheidend ist für den späteren Einsatz der Cloud-Lösung unter datenschutz-konformen Bedingungen.

3.7 Informationspflichten und Rechte des Betroffenen

Abhängig von den jeweiligen Cloud-Computing-Leistungen bestehen Informationspflichten, die grundsätzlich als Vorraussetzung oder ständige Verpflichtung für die verantwortliche Stelle aufgesetzt sind. Sie sollen dem Schutz der Betroffenen dienen, deren Daten verarbeitet werden, ihre informationelle Selbstbestimmung sichern, dabei Transparenz über die Datenverarbeitung herstellen und somit vor ungewollter Verarbeitung der personenbezogenen Daten schützen. Hiervon abzugrenzen sind Informationspflichten, die erst bei einer fehlerhaften Informationsverarbeitung auftreten und damit einer Schadensminimierung dienen sollen.

3.7.1 Allgemeine Informationspflichten

Beispiel hierfür sind die Verpflichtung zur Angabe von Name und Sitz eines Unternehmens als Anbieter elektronischer Informations- und Kommunikationsdienste im Impressum gem. § 5 Abs. 1 TMG. Hat das Unternehmen seinen Sitz oder eine Niederlassung in Deutschland, so ist in der Regel deutsches (Datenschutz-)Recht anwendbar, auch wenn Leistungen weltweit über das Internet angeboten werden. Denn es gilt das sogenannte Herkunftsland-Prinzip im Datenschutzrecht: Der Sitz der verantwortlichen Stelle gibt auch das anzuwendende Recht vor.

Darüber hinaus hat jeder deutsche Cloud-Anbieter derartiger Dienste in seiner Datenschutzerklärung gem. § 13 Abs. 1 TMG die Nutzer über den Umgang mit deren personenbezogenen Daten zu informieren. Diese Angaben erleichtern es dem Nutzer, ggf. eine Einwilligungserklärung für die Verarbeitung der personenbezogenen Daten abzugeben.

3.7.2 Vorfallbehandlung

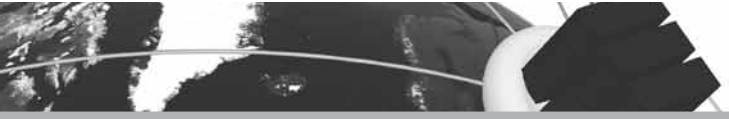
Für den Fall der Verarbeitung von besonders sensiblen personenbezogenen Daten, deren unrechtmäßige Übermittlung an Dritte nach § 42a BDSG an die Aufsichtsbehörde und die Betroffenen gemeldet werden muss, ist zu berücksichtigen, dass es bei einem Vorfall in Form einer unrechtmäßigen Übermittlung an Dritte schwierig werden könnte zu sagen, wo genau die Daten-Panne stattfand. Es wird möglicherweise auch schwierig sein, die Betroffenen schnell festzustellen, deren Daten kompromittiert wurden. Dies gilt umso mehr bei der Verarbeitung in Public Clouds mit ggf. mehreren Auftragsverarbeitern.

Deshalb ist bei der Vertragsgestaltung mit Subunternehmern darauf zu achten, dass für den Fall von Datenverlusten klare Prozesse und Zuständigkeiten vereinbart werden.

3.8 Sanktionen

Verstöße gegen datenschutzrechtliche Bestimmungen werden mit einer ganzen Bandbreite von Sanktionen belegt. Dies reicht von den vorbeschriebenen Informationen und Auskunftspflichten über Bußgeldvorschriften, wie sie § 43 BDSG in einem umfangreichen Katalog aufführt, bis hin zu empfindlichen Freiheitsstrafen. Letztere werden jedoch nur bei gezielt vorsätzlichen Handlungen verwirkt.

34. und im Ausland sogar legale Interceptions – z.B. nach dem Home Patriot Act



Der Bußgeldrahmen wurde inzwischen angehoben auf nunmehr bis zu 50.000,00 EUR bei einfacheren Ordnungswidrigkeiten wie unzureichender Vorabkontrolle im Rahmen der Auftragsdatenverarbeitung oder einem Verstoß gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten. Schwerwiegendere Ordnungswidrigkeiten wie die unbefugte Datenerhebung und Verarbeitung können mit bis zu 300.000,00 EUR geahndet werden. Übersteigt allerdings der wirtschaftliche Vorteil, den ein Täter aus der Ordnungswidrigkeit gezogen hat, diesen Grenzwert, so darf er entsprechend überschritten werden. Abschließend ist darauf hinzuweisen, dass der Gesetzgeber nicht grundsätzlich von einem Fortsetzungszusammenhang ausgeht, wenn z.B. gegen die Rechte mehrerer Betroffener verstoßen wurde und somit diese Beträge auch mehrfach in Ansatz gebracht werden können.

Das TMG sieht einen Bußgeldrahmen von 10.000,00 bis 50.000,00 EUR vor, das TKG in besonders schweren Fällen sogar bis 500.000,00 EUR. Schwerer wiegen dürfte jedoch bei erheblichen Datenschutzverstößen der Image- und Vertrauensverlust in der Öffentlichkeit bzw. bei Kunden sowie zunehmend das Risiko der persönlichen Haftung der Geschäftsführung bei Organisationsverschulden.

4 Cloud Computing und Informationssicherheit

- Für die Auslagerung von Applikationen und Teilen der betrieblichen IT-Infrastruktur in die Cloud, die sensible Funktionen und Daten umfasst, ist bis dato ein definiertes Vorgehen unverzichtbar, welches Sicherheit in jeder Phase gewährleistet. Ein solcher Prozess wird als Life Cycle Prozess Cloud Computing bezeichnet und umfasst die Phasen Planung, Umsetzung und Migration, Betrieb und Beendigung.

- Die Einhaltung der klassischen Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit ist im Rahmen von Cloud-Computing-Architekturen unabdingbar. Aus technischer Sicht muss dazu die Sicherheit der Rechenzentren, der Daten sowie Plattformen und der Verwaltung der Cloud-Services gewährleistet sein.

- Der Einsatz von Cloud-Services verändert merklich die Ausgestaltung traditioneller IT-Infrastrukturen. So ist u. a. die skalierbare, flexible und zentrale Bereitstellung von Sicherheitsfunktionen und -maßnahmen für Cloud-Services möglich und schafft auf diese Weise die Voraussetzung zur bedarfsgesteuerten Erfüllung variierender Sicherheitsanforderungen.

- Die Sicherheit von Applikationen, die von Cloud-Services bereitgestellt werden, kann analog zur Sicherheit von Web-Applikationen betrachtet werden. Daher verlangen die heutzutage überwiegend auf Applikationsebene stattfindenden Angriffe sowohl Vorgehen zur sicheren Entwicklung als auch Techniken für den sicheren Einsatz von Web-Applikationen bzw. Cloud-Services.

- Die Festlegung und Einhaltung organisatorischer Maßnahmen seitens der Anbieter und Nutzer von Cloud-Services trägt zur Gewährleistung der Informationssicherheit bei. Dabei nehmen die jeweilige Sicherheits- und Risikostrategie der Service-Nutzer, die Zertifizierungen des Service-Anbieters (z. B. nach ISO/IEC 27001), Best-Practice-Modelle zur Erbringung von IT-Services (z. B. ITIL) und Maßnahmen zur Qualitätssicherung zentrale Rollen ein.

- Neben der Informationssicherheit innerhalb von Cloud-Computing-Architekturen kann Sicherheit auch durch den Einsatz von Cloud-Services weiter erhöht werden (Security as a Service, SecS). Als Ausprägung von Software as a Service birgt SecS alle ökonomischen Vorteile wie z. B. die Verschiebung von CapEx zu OpEx. Zudem ist der Einsatz von SecS für Nutzer aus technischer Warte vorteilhaft, denn z. B. Aktualisierungen werden zentral vom SecS-Anbieter durchgeführt (z. B. Antispam-Signaturen, Websicherheit).

4.1 Informationssicherheit im Cloud Computing als Life Cycle-Prozess

Im Abschnitt 4.1 wird auf Cloud-Computing-Vorhaben fokussiert, die die Auslagerung von kritischen Funktionen (Applikationen, Plattformen) in eine Public Cloud beinhaltet. Natürlich können auch unkritische Funktionen ausgelagert werden. Die Inanspruchnahme von Cloud-Services wird aber in diesem Fall üblicherweise über Self Service Portale des Cloud-Anbieters erfolgen. Danach wählt das Unternehmen die im Portal angebotenen Services aus. Spezielle Anforderungen des Unternehmens können dann nicht berücksichtigt werden.

In seiner Idealform zielt das Cloud-Computing-Paradigma darauf ab, dass die Auslagerung und der Betrieb von Funktionen unter Verwendung einer Cloud mit einem hohen Automatisierungsgrad erfolgt und damit kein

kompliziertes Verfahren für die Vertragsschließung oder für die Migration notwendig macht. Werden jedoch sensible Daten betroffen, so wird man im Allgemeinen nicht auf ein Vorgehen verzichten können, wie es in Abbildung 26 gezeigt ist. Das Vorhaben für die Auslagerung von Applikationen und/oder IT-Infrastruktur muss dann durch einen klar definierten Prozess erfolgen, um in jeder Phase die Sicherheit gewährleisten zu können. Dieser Prozess wird im Folgenden als „Life Cycle Prozess Cloud Computing" bezeichnet. Es besteht aus den in Abbildung 26 gezeigten Phasen.

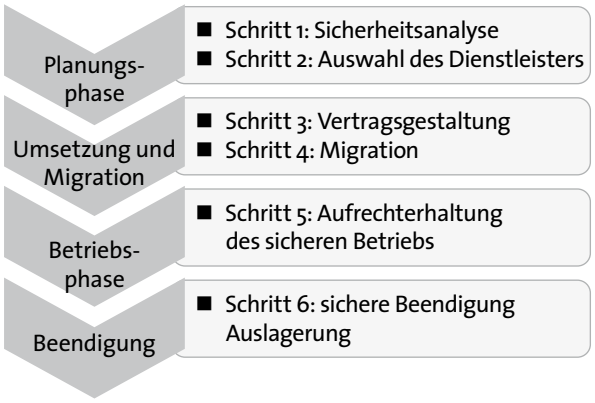


Abbildung 26: Life Cycle Prozess Cloud-Computing

4.1.1 Planungsphase

In dieser Phase werden verschiedene Alternativen für das Cloud Computing auf grober Ebene entwickelt. Varianten können sich aus den Service-Ebenen (vgl. Tabelle 1) und Organisationsmodellen (Tabelle 2) ergeben. Hierzu dient Schritt 1 „Sicherheitsanalyse". Die grob entwickelten Varianten für die Auslagerung in die Cloud werden skizziert und einer Struktur-, Schutzbedarfs- und Risikoanalyse unterzogen. Zudem wird ermittelt, welche gesetzlichen[35] und organisatorischen Anforderungen für die verschiedenen Varianten gelten. Aus all diesen Informationen werden die Sicherheitsanforderungen abgeleitet, die zu erfüllen sind.

Danach wird entschieden, welche Alternativen in die engere Auswahl fallen. Für diese wird in Schritt 2 „Auswahl des Outsourcing-Dienstleisters" ein Pflichtenheft erstellt, das detailliert die Auslagerung und alle geforderten Leistungen inklusive aller Sicherheitsanforderungen beschreibt. Dieses Pflichtenheft dient als Basis für eine Angebotsaufforderung. Auf der Grundlage der Antworten der Cloud-Anbieter wird die in Schritt 1 durchgeführte Risikoanalyse vertieft. Insbesondere werden Schwachstellen des Anbieters berücksichtigt. Kriterien für die Auswahl eines Anbieters sind u. a. Kosten, das verbleibende Restrisiko, ein gelebtes und dokumentiertes Sicherheitsmanagement, Referenzen, Vertrauenswürdigkeit, Kompetenz und Verfügbarkeit der Mitarbeiter, Zertifizierungen. Auch eine Due-Diligence-Prüfung des Anbieters kann durchgeführt werden. Danach erfolgt eine Entscheidung für eine Alternative und für einen Anbieter.

4.1.2 Migrationsphase

In Schritt 3 „Vertragsgestaltung" erfolgt die Ausarbeitung eines Vertrages (vgl. Kapitel 2). In Verträgen und/oder SLA ist eine vollständige, eindeutige und kontrollierbare Leistungsbeschreibung zur Gewährleistung der Qualität und Informationssicherheit der Auslagerung in die Cloud mit dem Anbieter zu vereinbaren. Ganz besonders wichtig sind hier folgende Aspekte (siehe hierzu Kapitel 2 und 3):

- Einräumung von Audit-Rechten für den Nutzer,
- Regelungen für die Beendigung der Auslagerung in die Cloud,
- Schnittstellendefinition für die Kontrolle und das Monitoring, insbesondere das Security Monitoring,
- Zugriffskontrolle,
- Verschlüsselung der Daten bei Speicherung und Transport,
- Standort der Daten,
- Disaster Recovery.

Nach Abschluss des Vertrages beginnt die Migration. Zunächst werden in Zusammenarbeit mit dem Dienstleister Sicherheitskonzepte erstellt. Diese betreffen sowohl

35. Besonders wichtig ist der Datenschutz (vgl. Kapitel 3).

die Migrations- als auch die Betriebsphase. Als Basis dienen hier die Ergebnisse der Sicherheitsanalyse aus der Planungsphase, die natürlich gemäß dem vertraglich vereinbarten Rahmen nochmals angepasst werden. Danach beginnen der eigentliche Umbau und die Umsetzung der Auslagerung in die Cloud des Anbieters. Dies betrifft auch die Prozesse und die Organisation sowohl des auslagernden Unternehmens als auch des Anbieters. Die Realisierung erfolgt schrittweise, wobei die Vorgaben aus den Sicherheitskonzepten jederzeit eingehalten werden müssen. Die Sicherheitskonzepte werden dabei laufend an die Projektentwicklung angepasst. Die Umsetzung wird durch Abnahmetests begleitet, bis die ausgelagerten Funktionen vollständig an den Dienstleister übergeben wurden.

4.1.3 Betriebsphase

In Schritt 5 „Aufrechterhaltung des sicheren Betriebs“ werden die ausgelagerten Funktionen gemäß Vertrag und Sicherheitskonzepten durch den Anbieter betrieben. Der Betrieb wird durch das auslagernde Unternehmen kontrolliert. Störungen und Abweichungen vom definierten Betrieb oder Sicherheitsniveau müssen erkannt und korrigiert werden. Das Security Monitoring dient hier dazu, die Erfüllung der vertraglich vereinbarten Leistungen nachweisen, kontinuierlich verbessern und überprüfen zu können.

4.1.4 Beendigung der Auslagerung

In Schritt 6 „Sichere Beendigung der Auslagerung“ wird eine geregelte Beendigung der Auslagerung durchgeführt. Diese Beendigung muss nach den vertraglich vereinbarten Vorkehrungen erfolgen. zu jedem Zeitpunkt muss dabei das definierte Sicherheitsniveau des auslagernden Unternehmens gewährleistet werden. Der Anbieter muss insbesondere nachweisbar Daten auf seinen Systemen so löschen, dass sie auch mit ausgefeilten Methoden und Technologien nicht wieder hergestellt werden können.

Der in Abbildung 26 gezeigte Prozess entspricht mit den Schritten 1 bis 5 auch dem PDCA Zyklus (Plan, Do, Check, Act), wie er im ISO/IEC 27001 gefordert wird.

4.2 Technische Aspekte der Informationssicherheit

Dieser Abschnitt zeigt die technischen Aspekte der Informationssicherheit bei der Nutzung von Cloud Computing auf. Dabei wird zunächst die Sicherstellung klassischer Schutzziele in Cloud-Computing-Architekturen beleuchtet. Folgende Themenbereiche sind dafür wichtig:

- Sicherheit der Rechenzentren,
- Sicherheit von Daten und Plattformen sowie
- Sicherheit der Verwaltung.

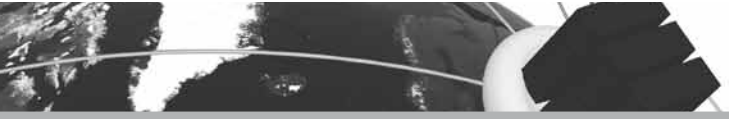
Daran anknüpfend werden die Auswirkungen des Cloud Computings auf traditionelle IT-Infrastrukturen untersucht. Dabei werden unter anderem folgende Aspekte aufgegriffen:

- Anpassungen, Erweiterungen und Aktualität von Sicherheitsfunktionen,
- Flexibilität der IT-Infrastruktur,
- Elastizität und kurzfristige Änderungen der Sicherheitsanforderungen,
- Applikations-Rollout und Time-to-Market,
- Verfügbarkeit und Performanz sowie
- automatisierte Bereitstellung mit Selbstbedienung.

Abschließend wird die Sicherheit von Applikationen dargestellt, welche durch Cloud-Services bereitgestellt werden. Dieses Unterkapitel beinhaltet folgende Punkte:

- Relevanz von Applikationen und Analogiebildung zu Web-Applikationen,
- Allgemeine Schwachstellen und Sicherheitsmaßnahmen von Applikationen,
- Web-Applikation Firewall und
- Secure Software Development Life Cycle.

In den Abschnitten 4.2.1 bis 4.2.3 werden die genannten Punkte näher untersucht und Besonderheiten des Einsatzes in Cloud-Computing-Systemen erläutert.



4.2.1 Sicherstellung klassischer Schutzziele in Cloud-Computing-Architekturen

Sicherheit der Cloud-Infrastruktur

Im Zentrum der Sicherheit einer Cloud-Infrastruktur stehen Rechenzentrumssicherheit, Hosts sowie Netzwerk und Netzwerkvirtualisierung.

Die Rechenzentrumssicherheit richtet sich insbesondere auf die Erfüllung der Schutzziele

- Verfügbarkeit,
- Integrität und
- Vertraulichkeit

und obliegt dem Cloud-Anbieter, insofern dieser ein eigenes Rechenzentrum betreibt. Ist dies nicht der Fall (Co-Location), muss der Cloud-Anbieter die Einhaltung der obigen Schutzziele durch den eigentlichen Rechenzentrumsbetreiber sicherstellen. Um die Verfügbarkeit der Rechner zu gewährleisten, werden u. a. Stromversorgung, Kühlungstechnik und Netzwerk innerhalb eines Rechenzentrums redundant ausgelegt sowie gespiegelte Rechenzentren in geographischer Nähe aufgebaut. Zudem berücksichtigt die Standortwahl des Rechenzentrums relevante Sicherheitsaspekte wie z. B. Klima, Katastrophenhäufigkeit etc.

Die Integrität und Vertraulichkeit der in Rechenzentren vorgehaltenen Daten sind eng miteinander verwoben und werden durch physische Maßnahmen wie Videoüberwachung vor und im Gebäude, Sicherheitspersonal und Zutrittskontrollen geschützt. Zudem werden die Gehäuse der Rechner durch Sensoren überwacht, die eine unberechtigte Öffnung identifizieren und automatisiert die Verwendung der betroffenen Maschine zeitweilig sperren.

Im Rahmen der physischen und virtuellen Knotenpunkte eines Netzwerkes, den sogenannten Hosts, gilt es insbesondere die Verfügbarkeit und Integrität der Daten zu sichern. Ein Host ist eine Umgebung, in der Prozesse und dazu notwendige Berechnungen zur Ausführung kommen. Diese Umgebung kann z. B. mehrere physische Server umfassen, deren Verfügbarkeit durch redundante Hardware im Bereich der Stromversorgung, physischen Speichermedien und Netzwerkschnittstellen gesichert ist. Ferner ermöglicht ein hoher Standardisierungsgrad der Server-Hardware einen transparenten Austausch defekter Komponenten, wodurch die Verfügbarkeit des Gesamtsystems weiter besichert wird.

Die Integrität der Daten und somit auch die Vertraulichkeit werden in der Regel durch feindliche Programme bedroht, die außerhalb einer Benutzerumgebung von Angreifern ausgeführt werden. Eine Benutzerumgebung bezeichnet in Cloud-Computing-Architekturen einen abgegrenzten Bereich, der durch einen Kunden verwendet wird. Unterschiedliche Benutzerumgebungen werden daher voneinander isoliert, sodass bösartigen Anwendungen das Verlassen einer zugewiesenen Umgebung nicht möglich ist. Eine solche Isolation lässt sich technisch durch das Konzept der Virtualisierung erzeugen. Ein direkter Zugriff auf die Ressourcen des Hosts ist damit nicht mehr zulässig; die Host-Ressourcen werden von einem so genannten „Virtual Machine Monitor“ bzw. „Hypervisor“ verwaltet.

Die Virtualisierung führt zu virtuellen Maschinen, die es ihrerseits gegen andere, böswillige virtuelle Maschinen sowie sonstige Bedrohungen des Netzwerkes zu schützen gilt. Wesentlich sind hierbei die folgenden Punkte:

- Secure-by-Default Konfigurationen:
  Nur das Minimum an Diensten wird für eine Anwendung bereitgestellt, um auf diese Weise die potentielle Angriffsfläche möglichst gering zu halten.
- Zugangsschlüssel:
  Schlüssel, die den Zugang zu einer virtuellen Maschine ermöglichen, werden geschützt gespeichert.
- Host-basierte Firewall:Einsatz einer Firewall, welche Ports nur so einsetzt und konfiguriert, die für die Erbringung tatsächlich erforderlich sind.
- Monitoring und Auditing:
  Die Speicherung von Log-Dateien wird getrennt von der virtuellen Maschine und verschlüsselt vorgenommen.

Zur Wahrung der Schutzziele Integrität, Vertraulichkeit, und Verfügbarkeit nehmen Kommunikationsprotokolle und Filtertechnologien als Komponenten eines Netzwerkes und dessen Virtualisierung eine zentrale Rolle ein. Kommunikationsprotokolle ermöglichen eine einheitliche Nutzung von Cloud-Services durch Benutzer und zwischen unterschiedlichen Cloud-Computing-Systemen. Technologien wie Firewalls, Intrusion-Detection-Systeme und Intrusion-Prevention-Systeme werden eingesetzt, um Netzwerkverbindungen zu überwachen, zu filtern oder nur bestimmte zuzulassen, wodurch bösartigem Zugriff auf Cloud-Computing-Architekturen vorgebeugt wird.

Die Netzwerksicherheit von Cloud-Computing-Architekturen beruht auf der Einhaltung der oben genannten Schutzziele und den typischen Anforderungen der Cloud-Services, die einen orts- und geräteunabhängigen Zugriff unter Einbezug heterogener Netzinfrastrukturen ermöglichen. Neben diesen Cloud-spezifischen Sicherheitsaspekten von Netzwerken wird zudem das sichere Weiterleiten von Nachrichten und sicheres Multicasting berücksichtigt. Ausgehend vom ISO/OSI-Schichtenmodell wird die Kontrolle des Netzzugangs und wichtiger Sicherheitsfunktionen auf verschiedenen Ebenen wie beispielsweise auf der Netzwerkebene durch IPSec oder durch TLS/SSL auf der Transportschicht realisiert. Dabei kommen Verfahren zur Isolierung des Netzverkehrs durch Virtualisierung, Zugangskontrolle durch Firewalls, Integration von VPN-Technologien in Cloud-Services sowie zum Erkennen und Entfernen verdächtiger Netzpakete durch IDS bzw. IPS zum Einsatz.

Um den gleichzeitigen, aber sicheren Betrieb mehrerer virtueller Betriebssysteme auf einem Host zu realisieren, werden Virtual Local Area Networks (VLANs) eingesetzt. Diese Software ermöglicht es, Server und virtuelle Maschinen in einem lokalen Netz in Gruppen einzuteilen, zwischen denen Verbindungen grundsätzlich unterbunden sind, aber gezielt ermöglicht werden können.

Ferner werden Services, die durch Cloud-Computing-Architekturen bereitgestellt werden, üblicherweise per Fernzugriff genutzt. Daher sind zusätzliche Sicherungsmaßnahmen wie die Benutzung eines virtuellen, privaten Netzes (VPN) erforderlich, um die Daten über einen verschlüsselten und isolierten Tunnel in das Rechenzentrum des Cloud-Computing-Anbieters zu übertragen.

Sicherheit von Daten und Plattformen in Cloud-Computing-Architekturen

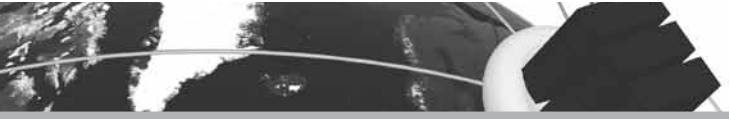
Im Zusammenhang mit Datensicherheit stehen die Schutzziele Integrität und Vertraulichkeit im Mittelpunkt. Dabei werden die Daten eines Cloud-Benutzers unter Verwendung der Speicherinfrastruktur eines Cloud-Anbieters gespeichert. Folglich muss der Cloud-Serviceanbieter Sicherheitsfunktionen implementieren und bereitstellen, die die Daten schützen, und gegebenenfalls dem Cloud-Benutzer Rechenschaft über die Wirkung eingesetzter Sicherheitsfunktionen ablegen.

Ein Cloud-Konsument klassifiziert seine Daten vor der Übertragung und legt damit fest, welche Daten bei einem Cloud-Anbieter auf welche Weise gespeichert werden dürfen. Dies wird durch unterschiedliche Speicher- und Sicherheitsoptionen für die vom Kunden klassifizierten Datenkategorien ergänzt, die der Cloud-Serviceanbieter bereithält. Dies können bestimmte kryptografische Verfahren oder aber auch Richtlinien sein, die der Anbieter unterstützt. Zur Sicherstellung der Schutzziele bietet sich zudem die Definition von Sicherheitsrichtlinien durch den Konsumenten an, die vom Anbieter eingehalten werden müssen.

Überdies kann ein Konsument das Prinzip der Datenminimierung anwenden. Dabei können z. B. Inhalte von Datensätzen, die durch einen Cloud-Service verarbeitet werden, so entfernt oder ersetzt werden, dass sie nur durch unternehmensintern vorgehaltene Daten, wieder ihre ursprüngliche Bedeutung erlangen.

Vor dem Hintergrund der klassischen Schutzziele sind speziell in Cloud-Computing-Architekturen folgende Problemstellungen und Maßnahmen relevant:

- Vermischung der Daten mit anderen Kunden:
  Vor allem bei vertraulichen Daten muss eine logische Trennung durch Virtualisierung und je nach Anforderung durch den Kunden auch eine physische Trennung



der Kundendaten durch dedizierte Server vorgenommen werden.
- Daten-Backup und Wiederherstellung:
  Es werden Sicherungsmechanismen eingesetzt, um die Daten verschlüsselt zu archivieren und wiederherzustellen. Es gilt auch hier, die logische oder physische Trennung der Kundendaten zu gewährleisten.
- Datensuche:
  Es werden Mechanismen eingesetzt, die die Suche und Extraktion von Daten zur Erfüllung regulatorischer Vorgaben jederzeit ermöglichen. Diese Aktionen können durch den Kunden angestoßen werden, und es werden Datenformate eingesetzt, die eine Weiterverarbeitung ermöglichen.

Die Plattformsicherheit betrifft neben der sicheren Bereitstellung von Cloud-Services auch die Entwickler von Cloud-Services, die eine Cloud-Plattform für die Entwicklung eigener Cloud-Applikationen einsetzen. Cloud-Nutzer sollen hierbei von den Sicherheitsfunktionen der Cloud-Anbieter profitieren können. Wichtige Sicherheitsmerkmale der Plattform beziehen sich auf die Entwicklungsprozesse der Cloud-Applikationen, die zum Einsatz kommenden Werkzeuge sowie die Isolierung der Anwendungen und Daten auf einer Cloud-Plattform. Vor allem die Isolierung von Anwendungen und Daten ist für die Einhaltung der Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit entscheidend.

Wegen ihrer Komplexität und Bedeutung wird die Sicherheit von Applikationen im Rahmen von Cloud Computing in einem separaten Abschnitt 4.2.3 behandelt.

Sichere Verwaltung von Cloud-Services

Cloud-Services sicher zu verwalten, stellt derzeit noch eine große Herausforderung dar. Im Folgenden werden kurz die ausstehenden, sicherheitsrelevanten Aspekte
- Prüfung,
- Identitäts- und Rechteverwaltung,
- Schlüsselverwaltung sowie
- Interoperabilität und Portabilität

samt der bedrohten Schutzziele aufgeführt.

Der Bereich der Prüfung beschäftigt sich mit der Frage, wie sicherheitsrelevante Ereignisse in Cloud-Computing-Systemen aufgezeichnet, überwacht und überprüft werden können. Dieses Gebiet ist daher eng mit dem Monitoring von Anwendungen und Daten verknüpft und nimmt in Cloud-Computing-Architekturen eine besondere Bedeutung ein, da für alle Schutzziele eine entsprechende Prüfungsmöglichkeit existieren sollte.

Ziel der Prüfung ist es, eine Beweissicherung auf Grundlage aufgezeichneter Daten zu ermöglichen. Hierfür muss die Beweissicherung in alle relevanten Komponenten eines Cloud-Computing-Systems eingebaut werden, um so eine möglichst lückenlose Überprüfung zu ermöglichen.

Die Möglichkeit der Anpassung bestehender, traditioneller IT-Systeme auf Cloud-Computing-Architekturen zur Erreichung der Schutzziele beschreibt einen Schwerpunkt der Identitäts- und Rechteverwaltungssysteme. Bestehende Systeme zur Zugangsverwaltung müssen berücksichtigen, dass durch den Bezug von Cloud-Services über ein öffentliches Netzwerk der Authentifizierungsvorgang Bedrohungen des Internets ausgesetzt ist. Das bedrohte Schutzziel Authentizität kann hier z. B. durch Mehrfaktor-Authentisierung, One-Time-Pads, Public-Key-Infrastructure (PKI) oder Smartcards gewährleistet werden.

Die Rechteverwaltung wird in Cloud-Computing-Architekturen häufig durch eine Zugriffskontrollliste realisiert. Die Vorteile dieses Konzepts liegen in der einfachen Verwaltung der Zugriffsrechte, insbesondere der einfachen und effizienten Realisierung einer Rechterücknahme. Im Mittelpunkt der Autorisierung steht dabei das Benutzerprofil, das eine Liste an Eigenschaften eines Cloud-Nutzers darstellt. Diese Eigenschaften werden verwendet um den Zugriff auf einen Cloud-Service entsprechend der jeweiligen Rechte zu regeln. Die Zugangskontrolle lässt den Zugriff zu bestimmten Ressourcen zu und setzt auditierbar diese Richtlinien um. Die Sicherheit der Zugangskontrolle selbst muss dabei ebenfalls gewährleistet sein, denn durch verletzte Integrität der Profilinformationen kann ein authentisierter Benutzer mehr Rechte im System

erlangen und z. B. unberechtigterweise auf bestimmte Daten zugreifen.

Eine weitere wichtige Komponente innerhalb einer Cloud-Architektur stellt die Schlüsselverwaltung dar. Um insbesondere die Schutzziele Integrität und Vertraulichkeit zu wahren, muss der vollständige Lebenszyklus von Schlüsseln mit den Phasen Schlüsselerzeugung, Schlüsselspeicherung, Schlüsselaustausch, Schlüsselverifikation und Schlüsselvernichtung in Cloud-Computing-Architekturen sicher abgebildet werden. Im Zuge der elastischen Eigenschaften von Cloud-Services können Nutzer dabei Schlüssel kurzfristig und dynamisch von unterschiedlichen Anbietern beziehen. Die resultierenden Herausforderungen liegen somit darin, eine große Anzahl von Schlüsseln für unterschiedliche, kryptografische Verfahren, verschiedene Schlüsselspeicher und Schlüsselarten zu verwalten. Dabei müssen zudem Schlüssel an Akteure verteilt werden, die zum Zeitpunkt der Planung und Konzeption der Schlüsselverwaltung unberücksichtigt geblieben sind. Die Rollen der Akteure, die verschlüsseln und jener, welche die Schlüssel speichern, sind dabei strikt voneinander zu trennen, um einen unberechtigten Zugriff auf Schlüssel zu verhindern.

So genannte „Lock-in Effekte“ beschreiben eine potentiell unvorteilhafte Abhängigkeit eines Cloud-Kunden von einem Cloud-Anbieter und bedrohen das Schutzziel Verfügbarkeit. Um diese Effekte zu vermeiden und die Kosten eines Wechsels des Cloud-Anbieters möglichst gering zu halten, müssen Unternehmen bei der Auswahl von Cloud-Services auf

- Interoperabilität und
- Portabilität

achten.

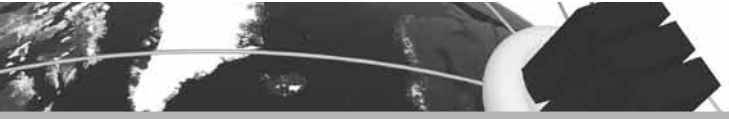
Die Interoperabilität beschreibt die Fähigkeit einer Cloud-Computing-Plattform mit anderen, unabhängigen Cloud-Computing-Plattformen zusammenarbeiten zu können, ohne dass spezielle Abstimmungen zwischen den kooperierenden Systemen notwendig werden. Portabilität bezeichnet ferner die Eigenschaft eines einzelnen Cloud-Services, auf unterschiedlichen Cloud-Computing-Plattformen ausgeführt werden zu können (Plattformunabhängigkeit). Eine technische Lösung, um Lock-in Effekten vorzubeugen, besteht im Einsatz von Standards wie Open Virtualization Format (OVF), vCloud API, Open Cloud-Computing-Interface (OCCI) oder per XML, die einen gewissen Grad an Interoperabilität und Portabilität ermöglichen. Überdies kann das Risiko eines Lock-In durch die Nutzung unterschiedlicher Cloud-Anbieter und redundanter Datenhaltung diversifiziert werden.

Nachdem im Abschnitt 4.2.1 die Sicherstellung klassischer Schutzziele in Cloud-Computing-Architekturen beleuchtet wurde, werden im folgenden Abschnitt 4.2.2 die Auswirkungen von Cloud Computing auf traditionelle IT-Infrastrukturen und daraus resultierende Sicherheitsimplikationen aufgezeigt.

4.2.2 Auswirkungen des Cloud-Computings auf traditionelle IT-Infrastrukturen und bestehende IT-Prozesse

Die Industrialisierung der IT treibt Arbeitsteilung und technische Spezialisierung voran, was branchenintern wie auch -übergreifend zu einem verstärkten Outsourcing IT-bezogener Teilbereiche führt. Diese Auslagerung von Teilen der Geschäftsprozesse kulminiert durch den Bezug von Services in Cloud-Computing-Systemen: Prinzipiell können Cloud-Services fein granular eingesetzt werden, um Aufgaben in Geschäftsprozessen zu unterstützen und zu realisieren. Aus diesem Grund verändert der Einsatz von Cloud-Services merklich die Ausgestaltung traditioneller IT-Infrastrukturen.

IT-Infrastrukturen erfordern laufende Anpassungen und Erweiterungen, um die Sicherheitsfunktionen stets auf dem neuesten Stand zu halten. Für diese Maßnahmen müssen in traditionellen IT-Lösungen unternehmensinterne Kapazitäten vorgehalten werden, wohingegen in Cloud-Computing-Architekturen externe Spezialisten diese Aufgaben lösen. Der Einsatz von Cloud-Services wirkt damit für Konsumenten unterstützend, da sich diese stärker auf ihre Kernbereiche konzentrieren können.



Bestimmte Sicherheitsmaßnahmen sind in Cloud-Computing-Architekturen aufgrund der elastischen und skalierbaren Eigenschaften flexibel an kurzfristig geänderte Sicherheitsanforderungen anpassbar. Dabei erfolgt das Kapazitäts-Management automatisiert durch den Cloud-Anbieter. Im Unterschied zu traditionellen internen IT-Infrastrukturen können so bei potentiellen Angriffen auf die Anwendung eines Nutzers Kapazitäten vorgehalten werden, die z. B. eine schnelle Ausweitung benötigter Ressourcen im Falle von DDoS-Attacken (Distributed Denial of Service) ermöglichen.

Applikations-Rollouts in Cloud-Computing-Architekturen besitzen im Vergleich zu traditionellen IT-Systemen einen merklichen Zeitvorteil. Konsumenten von Cloud-Services werden neben der eigentlichen Applikation ebenfalls die benötigten Sicherheitsfunktionen unverzüglich zur Auswahl bereitgestellt. Dies ermöglicht Konsumenten, zusätzliche Ressourcen nicht nur sofort, sondern auch zeitlich beschränkt und projektbezogen zu beziehen, z. B. die Sicherheitsfunktionen flexibel zu- oder abzuschalten.

Die Zeitspanne zwischen einer unternehmerischen Entscheidung und der Realisierung eines Vorhabens (Time-to-Market) gewinnt hinsichtlich der IT-Sicherheit zusätzlich an Bedeutung, wenn neue Applikations-Releases mit innovativen Weiterentwicklungen von Sicherheitsfunktionen erscheinen oder wenn neue bzw. geänderte Bedrohungen (z. B. Malware, DoS-Angriffe, Spoofing, usw.) bekannt werden. Notwendige Patches werden zeitnah installiert und ein Konsument nutzt zwangsläufig die aktuelle und stabilste Fortentwicklung einer Applikation. Insofern wird damit immer der höchstmögliche Sicherheitsstandard eines Cloud-Anbieters gesichert. Folglich profitieren die Konsumenten von Cloud-Services von stets aktueller Software, ohne sich um die Aktualisierung via Updates und Upgrades kümmern zu müssen.

Prävention bei IT-Sicherheit – Bestandteil der Geschäftsstrategie bei Cloud-Anbietern

Für kleinere und mittlere Unternehmen bedeutet das Betreiben einer traditionellen IT-Infrastruktur mit hohen Anforderungen an Verfügbarkeit und Performanz einen unverhältnismäßig hohen Aufwand. Der Einsatz von Cloud Computing vermag hier Abhilfe zu schaffen. Um die Verfügbarkeit etwa im Katastrophenfall zu gewährleisten, verfügen die meisten Cloud-Anbieter über gespiegelte Rechenzentren, die geographisch voneinander entfernt platziert sind. Dabei können Konsumenten eine Vielzahl an Überwachungswerkzeugen nutzen, um die Verfügbarkeit von Cloud-Services selbst nachzuvollziehen und an einem vereinbarten Qualitätsniveau zu messen. Dazu zählen z. B. die interne Überwachung der einzelnen Systemkomponenten, performanz-relevante Überwachung oder End-User Monitoring.

Cloud Computing stellt mandantenfähige Services mit hoher Skalierbarkeit bereit. Diese Eigenschaften sind inhärenter Bestandteil der Konzeption von Cloud-Services. Aus diesem Grund ist die potentielle Gewährleistung definierter Zielgrößen für die Performanz, wie z. B. Antwortzeiten, höher zu werten als in traditionellen IT-Infrastrukturen. Eine Ausnahme stellen hier die Anforderungen von Echtzeitanwendungen in Public Cloud-Computing-Systemen dar, da, im Vergleich zu unternehmensinternen Netzwerken, größere Latenzzeiten des Datentransfers über öffentliche Netzwerke zu erwarten sind.

Cloud-Services sind ferner nicht auf bestimmte Endgeräte festgelegt, sondern können bei ausreichend hoher Standardisierung und Bandbreite geräteunabhängig von einem beliebigen Ort bezogen und genutzt werden. Selbst komplexe Sicherheitsfunktionen können auf diese Weise kurzfristig auf Endgeräten mit beschränkter Leistungsfähigkeit bereitgestellt werden, da die notwendigen Berechnungen durch die Cloud übernommen werden.

Traditionelle IT-Infrastrukturen im eigenen Haus entwickeln nicht präventiv technische Vorkehrungen, um externen Angriffen entgegenzuwirken, sondern fügen diese eher in Folge von Sicherheitsvorfällen reaktiv hinzu. Dies rührt daher, dass Prävention und damit IT-Sicherheit in traditionellen IT-Systemen nicht Teil des Geschäftszwecks sind. Demgegenüber zählen präventive Maßnahmen, sich gegen externe Bedrohungen abzusichern, für Cloud-Anbieter zum zentralen Bestandteil ihrer Geschäftsstrategie und avancieren damit zur deren technischer Kernkompetenz.

In der praktischen Umsetzung wird z. B. durch die Inszenierung wöchentlich stattfindender Tests mittels unabhängiger Dienstleister die Sicherheit implementierter Mechanismen überprüft. Die Ergebnisse bieten wiederum Anhaltspunkte zur Verbesserung der Mechanismen, wobei die Iteration dieses Vorgehens einen dynamischen Prozess hervorbringt, der stetig zur Erhöhung der Systemsicherheit beiträgt.

Bedeutung des Multi-Tenancy-Konzepts

Innerhalb von Unternehmen bestimmter Branchen ist es essentiell, dass Abteilungen eines Unternehmens nicht die identische Sicht bzw. keinen Zugriff auf Anwendungen und damit verknüpfte Daten anderer Abteilungen haben. Dadurch sollen Vertraulichkeit und Integrität der Daten sichergestellt werden. Ein prominentes Beispiel sind Banken, die ihre Aktivitäten im Investmentbereich von denen des Commercial Banking trennen müssen, um rechtlichen Vorgaben zu genügen und Interessenskonflikte zu vermeiden. In traditionellen IT-Systemen stellt ein solches Abbilden von organisationalen durch technische Strukturen eine Herausforderung dar. Diese Trennung verschiedener Nutzer innerhalb eines Services und anhängiger Daten findet sich hingegen im Cloud Computing im Multi-Tenancy-Konzept wieder. Dieser Ansatz repräsentiert die technische Spezialisierung, die aus der Arbeitsteilung rührt. Konkret nutzen hier mehrere Konsumenten einen identischen Service, z. B. eine Instanz einer bestimmten Software, und sind über streng voneinander isolierte Kundenumgebungen separiert. Im Unterschied zu traditionellen IT-Infrastrukturen entsteht diese Isolierung nicht als Konsequenz regulatorischer Vorgaben. Im Gegenteil: Die Fähigkeit von Cloud-Services, durch mehrere Konsumenten simultan genutzt zu werden, ist integrales Element der Entwicklung von Cloud-Computing-Komponenten.

Automatisierte Bereitstellung mit Self Service

Abschließend werden die Interaktionen zwischen Konsumenten und Anbietern von Cloud-Services betrachtet, die zur Abstimmung des Bezugsprozesses dienen. Diese sind auf ein Minimum reduziert, was sich in dem Kriterium Automatisierte Bereitstellung mit Selbstbedienung (vgl. die Definition in Abschnitt 1.2.1) widerspiegelt, das neben anderen vom NIST zur Definition von Cloud Computing herangezogen wird. Oft wird dabei ein veränderter Bedarf an standardisierten Services gänzlich automatisiert angepasst, ohne dass der menschliche Endnutzer einer Anwendung dies aktiv steuern muss. Diese Automatisierung wirkt sich aus technischer Sicht ferner auf die Weiterentwicklung und Umsetzung der Services aus. Dabei nimmt ein Konsument weder am Entwicklungsprozess teil, noch bemerkt er oft die Umsetzung von Neuerungen. Aus technischer Sicht muss der Nutzer daher kein Know-how einbringen. Dies umfasst im Rahmen von Cloud Computing insbesondere die Entwicklung und Umsetzung von Gegenmaßnahmen und Mechanismen zur Gewährleistung höchstmöglicher IT-Sicherheitsstandards. Somit findet die Operationalisierung der Sicherheitsimplikationen anbieterseitig statt, was im Zuge der Spezialisierung zu einem wichtigen Bestandteil der Kernkompetenz des Anbieters zählt.

4.2.3 Applikationssicherheit in Public Clouds

In diesem Abschnitt werden die technischen Aspekte der Sicherheit von Applikationen detailliert dargelegt, welche durch Services in Public Clouds bereitgestellt werden. Die Behandlung in einem separaten Abschnitt wird durch die besondere Bedeutung der Applikationen gerechtfertigt, die sich aus ihrer ansteigenden Verbreitung und Komplexität ergibt.

In Public Clouds werden Applikationen über das Internet bereitgestellt und genutzt. An diese Applikationen werden folglich identische Anforderungen wie an andere Web-Applikationen gestellt. Die Sicherheit von Applikationen, die durch Cloud-Services bereitgestellt werden, kann somit analog zu der von Web-Applikationen betrachtet werden. Web-Applikationen bezeichnen komplexe verteilte Systeme, die das World Wide Web zur Interaktion und das Internet als Infrastruktur zur Kommunikation nutzen.

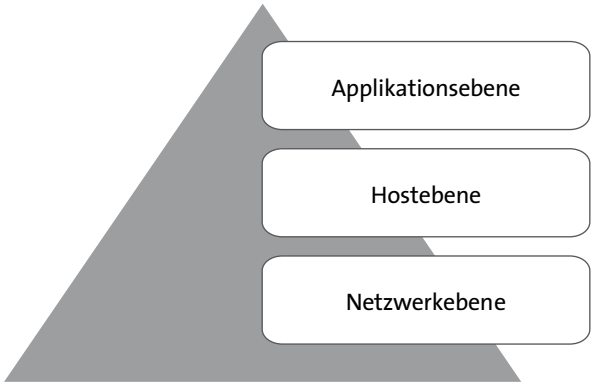


Abbildung 27: Ebenen der Sicherheit von Web-Applikationen

Sichere Web-Applikationen setzen die Sicherheit auf Applikations-, Host- und Netzwerkebenen voraus (vgl. Abbildung 27). Die Sicherheit der unterliegenden Ebenen wurde bereits stark verbessert.[36] Dies führt dazu, dass Angriffe heutzutage vermehrt auf Applikationsebene stattfinden.[37]

Neben den zunehmenden Angriffen auf Applikationsebene stellen Compliance-Bestimmungen (vgl. Kapitel 5) eine weitere, zentrale Triebfeder für die sichere Entwicklung und den sicheren Einsatz von Web-Applikationen dar. Diese Vorgaben umfassen sowohl gesetzliche als auch unternehmensinterne Regelungen für den Einsatz von Web-Applikationen. Drei bedeutende Beispiele gesetzlicher Bestimmungen sind:

- Sarbanes-Oxley-Act (SOX),
- Health Insurance Portability and Accountability Act (HIPAA) und
- Payment Card Industry Data Security Standard (PCI DSS).

Weitere Erläuterungen zu diesen Bestimmungen werden im Kapitel 5 gegeben.

Im Folgenden werden

- zunächst allgemeine Schwachstellen und Sicherheitsmaßnahmen von Web-Applikationen dargestellt.
- Daran knüpfen Web-Applikation Firewalls an, die in Folge ihrer hohen Relevanz für Web-Applikationssicherheit separat behandelt werden.
- Abschließend werden wesentliche Aspekte aufgezeigt, die im Rahmen der Entwicklung sicherer Web-Applikationen zu beachten sind.

Sicherheitsaspekte von Web-Applikationen

Aus technischer Perspektive nimmt der sichere Zugang zu einer Web-Applikation zentrale Bedeutung ein. Die Web-Applikationssicherheit umfasst daher unter anderem Verfahren und Methoden zur Sicherstellung des authentifizierten Zugangs. Da Web-Applikationen per Definition über das Internet zugänglich sind, ist neben Authentizität die Betrachtung der Schutzziele Integrität und Verfügbarkeit notwendig. Allgemein ergeben sich vor diesem Hintergrund folgende sicherheitsrelevanten Themen:

- Nachrichtenauthentifizierung und -verschlüsselung,
- Sitzungsverwaltung,
- Konfiguration,
- Eingabevalidierung,
- Auditing and Logging sowie
- Ausnahme-Management.

Web-Applikation Firewall

Eine Web-Applikation Firewall (WAF) ist eine Komponente, die auf Applikations-Ebene eine Auswahl an Regeln auf die Datenübertragung anwendet. Dadurch ist eine WAF in der Lage, eine Vielzahl an Angriffen auf Web-Applikationen abzuwehren und somit die Sicherheit der Applikation deutlich zu verbessern. Eine WAF kann in den nachfolgenden Betriebsarten eingesetzt werden:

- Reverse Proxy,
- Transparent Proxy,
- Layer 2 Bridge,
- Network Monitor und
- Host/Server-basiert.

36. Die dabei eingesetzten Verfahren wurden im Abschnitt 4.2.1 aufgezeigt.
37. Untersuchungen haben ergeben, dass 75 Prozent aller Angriffe auf Applikationsebene erfolgen.

Eine WAF kann zudem Konsumenten auch selbst als Cloud-Service bereit gestellt werden. Diese spezielle Ausprägung von SaaS wird als Security as a Service (SecS) bezeichnet und im Abschnitt 4.4 weiter detailliert.

Secure Software Development Life Cycle (Secure-by-Design)

Die klassischen Phasen eines Software Development Life Cycles umfassen

- Planung,
- Entwurf,
- Implementierung,
- Test,
- Einsatz und
- Wartung.

Die individuelle Ausgestaltung und Abfolge dieser Phasen hängt vom gewählten Vorgehensmodell (z. B. Wasserfallmodell) ab. Sicherheitsanforderungen an Web-Applikationen werden dabei bereits während des Entwicklungsprozesses berücksichtigt. Dieser Ansatz wird als Secure-by-Design bezeichnet. Die individuelle Ausgestaltung eines Secure Software Development Life Cycles kann je nach Umfeld sehr unterschiedlich ausfallen. Deshalb werden in diesem Leitfaden keine phasenspezifischen Sicherheitsmaßnahmen aufgezeigt, sondern zentrale Momente beleuchtet, die es übergreifend bei Secure Software Development zu beachten gilt.

Die eingesetzten Methoden zur Gewährleistung der sicheren Entwicklung und des sicheren Einsatzes von Web-Applikationen spielen eine zentrale Rolle. Dabei gibt es eine Vielzahl an Ansätzen, die sich zunächst in formale und semi-formale Methoden unterscheiden lassen. Formale Methoden zeichnen sich dadurch aus, dass ein System entsprechend getroffener Spezifikationen automatisiert validiert werden kann. Typischerweise werden diese Methoden auf spezifische Problemstellungen angewendet wie z. B. Protokolle zur Authentisierung und Authentifikation. Ferner kann mit semi-formalen Methoden wie etwa der Unified Modelling Language (UML) ein System strukturiert beschrieben werden. Die Ergebnisse dieser Methoden können nicht wie die der formalen automatisiert validiert werden. Dafür sind semi-formale Methoden, unter anderem aufgrund ihrer graphischen Darstellungen, von Personen ohne umfassenden mathematischen Hintergrund oder Modellierungsexpertise zu verstehen.

Sicherheits-Tools, wie z. B. Web-Applikation Scanner, eignen sich ferner dazu, Prozesse zur Prüfung der Sicherheit von Web-Applikationen zu beschleunigen. Diese Tools können überdies weiteres Wissen bereitstellen und nicht zuletzt monotone Aufgaben übernehmen. Daher wirkt der Einsatz von Sicherheits-Tools in der Regel erweiternd auf die Fähigkeit der Entwickler von Web-Applikationen. Der potentielle Mehrwert eines eingesetzten Tools hängt dabei von folgenden Kriterien ab:

- Überprüfbarer Einsatz des Tools in einem definierten und vollständig erfassten Prozess,
- Schulung der Nutzer des Tools,
- regelmäßige Revision zum Evaluierungs- und Selektionsprozess von Sicherheits-Tools (vorzugsweise durch externe Experten).

Die Einführung von Secure Software Development bedeutet für Entwickler von Web-Applikationen eine merkliche Veränderung. Um Überforderungen der Entwickler zu vermeiden, sollte ein Plan zur inkrementellen Einführung entwickelt werden, der die Sicherheitsanforderungen umfasst und zwischen Effektivität und reibungsloser Einführung von Secure Software Development vermittelt. Code Analyse und Sicherheitstests stellen effektive erste Schritte dieser Einführung dar. Ein besonders geeigneter Ansatzpunkt ist hier das Konzept Continuous Integration (CI), welches fortwährend neue Software im Entwicklungsprozess integriert. Dieses Konzept ist in der Softwareentwicklung weit verbreitet und beinhaltet bereits Code Analyse und Tests. Diese Analysen und Tests können mit vertretbarem Mehraufwand um Sicherheitsaspekte erweitert werden, um die Schwachstellen einer Web-Applikation während der Entwicklung sichtbar zu machen.

Entwickler von Web-Applikationen sind sich zwar der unzureichenden Sicherheit bewusst, verfügen aber oft nicht über das notwendige Wissen, um effektiv sichere

Web-Applikationen zu entwickeln. Aus diesem Grund sind Trainingsmaßnahmen für die Entwickler von Web-Applikationen unerlässlich. Diese in Anwendungen integrierten Sicherheitsmaßnahmen reduzieren die Wahrscheinlichkeit der Manipulation von Anwendungen und Daten durch Angreifer und vermeiden den Zugriff auf sowie die Änderung, Löschung und Mitnahme von sensiblen Daten. In Anlehnung daran stehen intern und extern durchgeführte Tests, denen Web-Applikationen im Rahmen des Code-Auditing unterzogen werden.

Sicherheitsanforderungen hingegen in einer bereits in der Entwicklung befindlichen Web-Applikation zu berücksichtigen, wirft vielschichtige Probleme auf. Neben entstehenden Engpässen der Budget- und Zeitplanung sind die beteiligten Entwickler oft nicht in der Lage, Sicherheit in laufende Projekte zu integrieren. Wenn die Erfüllung der Sicherheitsanforderungen unverzichtbar für die zu entwickelnde Web-Applikation ist, empfiehlt es sich, das bestehende Entwicklerteam um Sicherheitsexperten zu ergänzen.

Nachdem der Abschnitt 4.2 technische Aspekte der Informationssicherheit im Rahmen des Cloud-Computings behandelte, sollen nun im Abschnitt 4.3 organisatorische Aspekte der Informationssicherheit im Cloud Computing erörtert werden. Dau gehören unter anderem die Anforderungen der Nutzer und das Identitätsmanagement.

4.3 Organisatorische Aspekte

Neben den technischen Anforderungen sind eine ganze Reihe organisatorischer Maßnahmen und Schnittstellen mit dem Dienstleister zu definieren und einzuhalten. Die Darstellung konzentriert sich auf folgende wichtige Aspekte:

- Sicherheits- und Risikostrategie des Unternehmens (vgl. Abschnitt 4.3.1),
- Zertifizierungen des Dienstleisters (vgl. Abschnitt 4.3.2),
- grundsätzliche organisatorische Anforderungen (vgl. Abschnitt 4.3.3),
- Qualitätssicherung (vgl. Abschnitt 4.3.4).

4.3.1 Sicherheitsstrategie des Unternehmens

Die Auslagerung von Funktionen in die Cloud muss der definierten Sicherheits- und Risikostrategie des Unternehmens entsprechen. Diese Strategie wird durch die Geschäftsleitung festgelegt. Hierzu gehören folgende Aspekte:

- Festlegung von Kriterien, die eine Auslagerung von Geschäftsprozessen in die Cloud unter Berücksichtigung der Geschäftsziele gewährleisten. Hier ist insbesondere zu beschreiben, welche generellen Ziele durch die Auslagerung in die Cloud verfolgt werden. Weiter können Funktionen explizit benannt werden, die aus Sicht der Geschäftsleitung ausgelagert werden sollen oder die auf keinen Fall in einer Cloud betrieben werden dürfen.
- Angabe der relevanten Gesetze, Standards und Verordnungen, die aus Geschäftssicht für die Auslagerung in eine Cloud maßgeblich sind. Es muss insbesondere deutlich werden, welche Vorhaben aus gesetzlichen Anforderungen heraus oder aus Risikogründen nicht möglich sind.
- Klärung welche Daten in welchen Staaten überhaupt verarbeitet werden dürfen. Hier können aus Gründen des Datenschutzes (vgl. Kapitel 3) erhebliche Einschränkungen notwendig sein.
- Identifizierung genereller Risiken und Sicherheitsanforderungen, die mit dem Cloud Computing verbunden sind. Zudem muss die Höhe akzeptabler Risiken festgelegt werden.
- Es ist zu klären, wie mit Risiken des Cloud Computing umzugehen ist. Hier wird fixiert, welche Arten von Risiken vermindert oder umgelagert werden können bzw. durch eine Risikodeckung bewältigt werden sollen.
- Generelle Fallback-Strategien und Ausstiegsszenarien auf der Ebene des Business müssen vorgegeben werden.
- Die Strategie kann zudem festlegen, wann eine Due Diligence des Dienstleisters verpflichtend durchzuführen ist und wie diese in groben Zügen auszusehen hat.

4.3.2 Zertifizierungen des Dienstleisters

Zertifizierungen sind ein zweischneidiges Schwert:

- Einerseits bestätigen sie, dass der Dienstleister grundlegende Anforderungen bezüglich der Informationssicherheit erfüllt.
- Andererseits darf man sich auf eine Zertifizierung nicht allein verlassen und sollte ausreichende Kontrollen und Audits durchführen, um jederzeit das Sicherheitsniveau der Cloud zu kennen und nachweisen zu können.

Sinnvoll ist sicherlich die Zertifizierung nach ISO/IEC 27001, da hier nachgewiesen wird, dass ein Information Security Management System gelebt wird. Dieser Standard ist international gültig und somit auch für eine weltweit implementierte Cloud anwendbar. Der Standard deckt alle wesentlichen Elemente ab:

- Organisation,
- Vorgaben,
- Dokumentation,
- Prozesse.

In einem Satz von Controls werden zudem konkret Sicherheitsmaßnahmen vorgegeben. Die Grundlage des ISO/IEC 27001 ist der ISO/IEC 9001 Standard für Qualitätsmanagement. Damit wird also bei Anwendung des ISO/IEC 27001 auch die Grundlage für die Qualitätssicherung gelegt, die bezogen auf die Informationssicherheit nicht anderes darstellt als die Einhaltung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit.

4.3.3 Grundsätzliche organisatorische Anforderungen

Bedeutende organisatorische Anforderungen gelten bei jeder Auslagerung in eine Cloud. Diese können mit wesentlichen Prozessen identifiziert werden, wie sie aus dem ITIL-Standard bekannt sind. Dazu gehören u. a.

- Identity Management,
- Change Management,
- (Security) Incident Handling und Notfall-Management,
- Capacity Management,
- SLA-Management,
- Service Desk.

Bei Auslagerung von Funktionen in eine Cloud sind diese Prozesse anzupassen.

Das Fundament der Informationssicherheit stellen gesicherte Identitäten und korrekte Zugriffsrechte dar. Dies gilt umso mehr bei der Auslagerung von Funktionen in eine Cloud. Hier muss der Prozess zur Benutzer- und Rechteverwaltung mit all seinen Rollen auf Nutzer- und Dienstleisterseite klar definiert werden.

Unbedingt sollte darauf geachtet werden, dass die Genehmigung und die Einrichtung von Rechten durch verschiedene Mitarbeiter vorgenommen werden. Vielfach wird dabei ein Mitarbeiter des auslagernden Unternehmens die Genehmigung erteilen. Der Workflow für die Benutzer- und Rechteverwaltung muss also über die Unternehmensgrenzen hinweg zwischen dem auslagernden Unternehmen und dem Cloud-Anbieter implementiert werden. Der Dienstleister hat alle wesentlichen Administrations-Aktivitäten so zu protokollieren, dass die Rechte jedes Benutzers (jeder Applikation) zu jedem Zeitpunkt nachvollzogen werden können. Gerade Änderungen von Rechten und das Sperren von Berechtigungen und Accounts müssen schnell und gesichert erfolgen.

Weiter muss ein Change Management vertraglich fixiert werden. Auch hier muss der Change-Prozess eine klare Autorisierung eines Change garantieren (Trennung von Genehmigung und Umsetzung) und jede Änderung nachvollziehbar dokumentieren. Der Prozess sollte zudem absichern, dass Changes nur dann autorisiert werden können, wenn der Change einer Sicherheitsanalyse unterzogen wurde und ausreichend in Integrationsumgebungen getestet wurde.

Eine Herausforderung stellt das (Security) Incident Handling dar. Hier gilt es vertraglich zu vereinbaren, mit welchen Reaktionszeiten auf Incidents verschiedener Kritikalität reagiert werden muss. Insbesondere ist zu definieren, was ein Security Incident ist und welche

Kritikalitätsstufen gelten. Vor allem muss technisch ermöglicht werden, dass Security Incidents und ihre Kritikalität erkannt werden können. Deshalb ist ein hinreichend leistungsfähiges Security Incident and Event Monitoring (SIEM) mit einer geeigneten Schnittstelle zwischen auslagerndem Unternehmen und dem Cloud-Anbieter zu implementieren. Die Verantwortlichkeiten für dieses SIEM-System müssen ebenfalls vereinbart werden. Weiter sind klare Eskalationspfade zu definieren, die die Verantwortlichkeiten und Befugnisse im Falle von Störungen, Notfällen und Krisen festlegen. Notfallsituationen sind regelmäßig zu trainieren.

Ein Capacity Management muss garantieren, dass auch zukünftige Anforderungen an Verfügbarkeit, Performance, Bandbreite etc. erfüllt werden können. Die Analyse kann das auslagernde Unternehmen wie üblich durchführen. Die Realisierung erfolgt jetzt aber mit Hilfe des Cloud-Anbieters und sollte damit einfacher und schneller erfolgen können, da man Ressourcen nicht erst aufbauen, sondern nur anfordern muss. Zu beachten ist aber, dass SLA-Vereinbarungen aktualisiert werden müssen. Ein SLA-Management sollte deshalb vertraglich mit seinen Rahmenbedingungen fixiert sein (vgl. Abschnitt 2.4.4).

Bei all den hier genannten Prozessen ist sicherzustellen, dass geeignete und abgesicherte Schnittstellen implementiert werden, die dem auslagernden Unternehmen das Einstellen und Auslesen von Daten erlauben und ausreichende Verfügbarkeit gewährleisten. Insbesondere müssen hier vom Cloud-Anbieter technische Schnittstellen bereitgestellt und Mappings von Daten und Formattransformationen vorgenommen werden. Dabei dürfen die Anforderungen an Vertraulichkeit und Integrität nicht verletzt werden. Deshalb sind auch die technischen Anforderungen an die Schnittstellen vertraglich zu regeln.

4.3.4 Qualitätssicherung

Die Qualität der Leistungserbringung ist regelmäßig zu kontrollieren. Hier werden die bereits oben genannten Elemente des ISMS genutzt:

- definierte Organisation,
- Vorgaben,
- Dokumentation,
- Prozesse und
- Security Monitoring.

Zu empfehlen sind regelmäßige Meetings mit dem Cloud-Anbieter, um die Qualität der Leistungserbringung zu überprüfen. Grundlage dieser Meetings sollten Statusberichte des Cloud-Anbieters sein, die alle vertraglich vereinbarten Leistungen verständlich und überprüfbar dokumentieren. Wichtige Security Incidents sollten einer Analyse unterzogen werden, um Sicherheitslücken aufzudecken. Ein Plan für Verbesserungsmaßnahmen ist abzustimmen.

Weiter sind regelmäßige Audits auch vor Ort beim Cloud-Anbieter durchzuführen, zu protokollieren und mit dem Cloud-Anbieter abzustimmen. Der Umfang der Audits und die Prüftiefe müssen vorab festgelegt werden. Das Audit-Vorgehen kann sich am ISO/IEC 19011 Standard für die Durchführung von Audits orientieren. Auch hier muss ein Plan für Verbesserungsmaßnahmen erstellt werden.

Im Abschnitt 4.3 wurden organisatorische Maßnahmen aufgezeigt, die beim Einsatz von Cloud-Computing-Architekturen von Anbietern und Nutzern zu erfüllen sind, um die Informationssicherheit zu gewährleisten. Im nachfolgenden Abschnitt wird Security as a Service (SecS) als eine konkrete Ausprägung von Software as a Service vorgestellt.

4.4 Sicherheit aus der Cloud: Security as a Service – ein Exkurs

Security as a Service (SecS) ist Teil des Cloud Computing Paradigmas. Es kommt allerdings in der aktuellen Diskussion um die Informationssicherheit von Cloud-Services häufig zu kurz, insbesondere auch in der Darstellung ihrer offensichtlichen Vorteile für Unternehmen und Privatnutzer. Mit Security as a Service wird die Möglichkeit bezeichnet, bestimmte sicherheitsrelevante Techniken

(beispielsweise Proxy, Antispam, Antivirus) aus der eigenen Netzwerkumgebung in eine Cloud zu verlagern. In diesem Exkurs sollen beispielhaft IT-Sicherheits-Dienstleistungen beleuchtet werden, die schon heute in der Cloud verfügbar sind.

Die wesentlichen Vorteile liegen bei SecS-Lösungen darin, dass für die zur Verfügung gestellten Sicherheitsfunktionen kein eigenes Personal und keine eigenen Hardwareressourcen mehr benötigt werden. Hierdurch spart der Anwender nicht nur die initialen Anschaffungskosten, sondern auch ggf. anfallende Lizenzkosten für Betriebssysteme sowie Wartungs- und Erneuerungskosten für die Infrastruktur. Ebenfalls entfallen hier indirekte Kosten für den Betrieb der entsprechenden Server.[38] Security as a Service ist somit für diejenigen Unternehmen und Organisationen von Interesse, die die Investitionen in eigene Sicherheitsinfrastrukturen und die Rekrutierung von entsprechenden Spezialisten aus Kostengründen scheuen.

Weiterhin ist die Verfügbarkeit von enormer Relevanz. Viele Anbieter von Sicherheitslösungen in der „Cloud" garantieren eine Quote von nahezu 100 Prozent (99,x Prozent). Dies wird durch komplex vernetzte Rechenzentren realisiert. Der Zugriff auf administrative Funktionen der jeweiligen Sicherheitslösungen ist von nahezu jedem Ort gegeben. Damit ist die Verwaltung der Lösung nicht mehr an das eigene Unternehmensnetzwerk gebunden.

Beispiel E-Mail-Sicherheit

Eine wichtige SecS-Lösung kommt schon heute im Bereich der E-Mail-Sicherheit zum Einsatz. 90 Prozent des heutigen Emailverkehrs sind unerwünschte Werbe-Mails (Spam). Eine lokale Filterung findet heute noch in vielen Unternehmen statt. Zukünftig werden aber Anti-Spam-Lösungen eher zentral aufgesetzt, wie es heute schon bei den großen Anbietern kostenloser E-Mail-Accounts üblich ist. Der Ansatz vieler Anbieter, Antispam beziehungsweise Antivirus in der Cloud abzudecken, zeigt auch bereits Wirkung. Der Vorteil liegt hier klar auf der Hand: Es wird nur noch der E-Mail-Verkehr an lokale Mailserver weitergeleitet, der für das Unternehmen relevant ist. Dies spart Ressourcen und administrativen Aufwand.

Außerdem sind Aufgaben wie die Aktualisierung der Lösung, beispielsweise Pattern oder Antispam-Signaturen, nicht mehr abhängig von dem Sicherheitskonzept des einzelnen Unternehmens. Die Expertise im Bereich der Sicherheit ist auch nicht an den jeweiligen Administrator gekoppelt. Auch dies erhöht das Potenzial der Sicherheitslösung.

Bei einer Verlagerung der Sicherheitsfunktionen für E-Mails stellen sich die gleichen Fragen, die sich bei allen Cloud-Services ergeben: Wer hat Zugriff auf meinen E-Mail-Verkehr? Kann man noch unternehmenskritische Daten per E-Mail versenden? Viele Anbieter werden diesen Anfragen zum Beispiel durch Verschlüsselungslösungen für die E-Mail-Sicherheit gerecht.

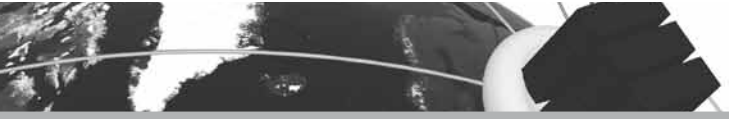
Beispiel E-Mail-Verschlüsselung

Bei Cloud-orientierten Lösungen für die E-Mail-Verschlüsselung hat der Kunde den Vorteil, dass das Schlüssel-Management aggregiert wird und somit keine aufwendigen Austauschverfahren beim Kontakt zu Geschäftspartnern nötig sind. Ebenfalls wird die teils rechenintensive Arbeit des Ver- und Entschlüsselns in den jeweiligen Datenzentren der SecS-Anbieter realisiert, was zu einer deutlichen Erhöhung der Performanz führt. Einige Dienstleister bieten die Möglichkeit, den Schlüssel-Server lokal zu hosten und diesen somit selbst zu verwalten.

Beispiel „Web-Sicherheit" – Web Security Appliances

Web Security Appliances sind häufig eine Kombination aus Hardware und Software, über die der Datenverkehr von Unternehmen zentral gefiltert werden kann. Die Appliances schützen vor Viren und Spyware und können URLs blockieren. Der Vorteil einer Cloud-basierten Lösung liegt vor allem in der hohen Aktualität der

38. Platz im Rack des Serverraums, Kosten für Klimatisierung, Strom etc



Sicherheitslösung und einer optimalen Konfiguration, die sich häufig durch eigenes Personal in der erforderlichen-Qualität nicht erreichen lässt.

Beispiel Endpunktsicherheit

Beim Schutz von Client-Systemen bietet Security as a Service die Möglichkeit, den Sicherheits-Server bzw. die Management- und Konfigurationskomponente in die Cloud zu verlagern. Dies ist insbesondere für kleinere Unternehmen sinnvoll, da hier keine lokalen zusätzlichen Ressourcen wie Hardware, Software oder Personal benötigt werden. Ein wesentlicher Vorteil ist die Aktualität von Schadsoftware-Signaturen. Ein weiterer Faktor ist die Mandantenfähigkeit. Fachhändler oder Service-Provider können so auf sehr einfachem Wege Sicherheitslösungen anbieten und mehrere Kundennetze zentral und hochverfügbar betreuen. Komplexe Reports und Analysen der Logdateien zählen hier ebenfalls zu den Stärken der Endpunktsicherheit.

Beispiel Ereignis- und Log-Management

Ein Ereignis- und Log-Management gestattet es, eine fortlaufende interne Ereignisdokumentation von Netzwerkkomponenten, Betriebssystemen und auch Sicherheitsprodukten des Unternehmens in einer zentralen Plattform zusammenzuführen. Als Ziel sollen Ereignisanomalien und damit Angriffe entdeckt werden, bevor diese eine Auswirkung auf die IT-Systeme des Unternehmens haben. Eine zentrale Verwaltung dieser Daten erhöht die Geschwindigkeit von Sicherheitsnachforschungen. Zusätzlich können die Daten forensisch sicher über mehrere Jahre aufbewahrt werden. Auch bei diesem Beispiel hat die zentrale Betreuung in der Cloud wesentliche Vorteile bezüglich Kosten und Qualität der Administration.

Beispiel Penetrationtest

Penetrationtests werden bereits heute regelmäßig von Unternehmen zur Prüfung der eigenen IT-Systeme oder einzelner Komponenten, wie zum Beispiel Webanwendungen und Datenbanken, eingesetzt. Cloud-basiertes internes und externes Scannen der Infrastruktur kann über ein zentrales Portal zur Verfügung gestellt werden. Der Dienst scannt kontinuierlich auf Schwachstellen, klassifiziert diese und empfiehlt passende Gegenmaßnahmen.

5 Cloud Compliance

- Cloud Compliance bezeichnet die nachweisbare Einhaltung von Regeln zur Nutzung oder Bereitstellung von Cloud Computing.

- Cloud Compliance hat zum Ziel, Transparenz und Sicherheit für alle Anspruchsgruppen (Stakeholder) zu schaffen. Cloud Compliance unterstützt insoweit dabei, die bestehende Zurückhaltung und die Vorbehalte gegenüber den Angeboten zum Cloud Computing aufzulösen. Damit schafft Cloud Compliance eine wichtige Basis, um alle Vorteile des Cloud Computings für Anbieter und Provider vollumfänglich nutzbar zu machen.

- Bei der Beschäftigung mit Cloud Compliance sind insbesondere die folgenden Herausforderungen zu bewältigen: Die Neuartigkeit und die damit verbundene Komplexität des Themas, die Vielzahl von Service-Angeboten und Geschäftsmodellen der Anbieter mit derzeit oft noch unklaren bzw. sich widersprechenden Cloud Definitionen sowie die fehlenden Standards im Markt.

- Die Folgen bei Nichterfüllung von Compliance-Anforderungen sind hinsichtlich Art und Ausmaß unterschiedlich. Sie reichen von Strafen und Bußgeldern über die Erfüllung von Schadenersatzansprüchen bis hin zur Einschränkung des Zugangs zum Kapitalmarkt. Auch der Verlust von Marktanteilen aufgrund von Imageschäden oder dem Ausschluss von Ausschreibungsverfahren sind möglich.

- Der Umgang mit den oben genannten Zielen und Herausforderungen wird durch den Einsatz eines geeigneten Compliance Management Systems (CMS) unterstützt. Es kann gleichermaßen von Anbietern sowie von Nutzern des Cloud Computings eingesetzt werden. Die Ausführungen in diesem Kapitel basieren auf einem CMS mit sieben Grundelementen. Diese lassen sich vereinfacht zu den Kernthemen „Anforderungen“, „Risiken“ und „Risikomaßnahmen“ zusammenfassen. Auf diese drei Kernthemen wird in diesem Kapitel explizit eingegangen.

- Zur Erreichung einer adäquaten Cloud Compliance gehört es, die Anforderungen insgesamt zu kennen und hinsichtlich ihrer Bedeutung zu bewerten. Die Kategorisierung der Anforderungen kann schematisch nach primär externen Vorgaben (Gesetzen und externen Regelwerken) sowie primär internen Vorgaben (interne Verpflichtungen und Verträge) erfolgen. Die Identifikation als auch die Kategorisierung sollten sowohl Nutzer als auch Anbieter von Cloud Computing individuell für ihre Geschäftszwecke vornehmen.

- Allgemein kann hierfür festgehalten werden, dass für Cloud Computing keine eigenen Regeln gelten und insoweit die allgemeinen IT-Compliance-Anforderungen Anwendung finden. Hinter den IT-Compliance-Anforderungen stehen insoweit in aller Regel Ziele zur adäquaten Behandlung klassischer IT-Risiken (Sicherheit, Verfügbarkeit, Vollständigkeit, Nachvollziehbarkeit, etc.). Diese verlangen jedoch in jedem Fall eine gesonderte Auseinandersetzung mit den für Cloud Computing spezifischen Risiken.

- Hinsichtlich der Risiken ist zu beachten, dass ein Service aus der Cloud neue Merkmale aufweist, die so in der klassischen IT kaum existierten. Dazu zählen z. B. der Applikationsbezug über das Internet, der hohe Grad an Virtualisierung, die Service-Orchestrierung, die Datenlokation sowie die Multi-Mandanten-Fähigkeit

der Anwendungen. Damit gehen neue Risikosituationen einher, die wie folgt gekennzeichnet werden können:

- neue Risiken (denen mit neuen Maßnahmen begegnet werden muss),
- gleichbleibende Risiken (bekannte Risiken für ein neues Cloud-Merkmal, denen mit analogen Maßnahmen zu begegnen ist),
- reduzierte Risiken (denen aufgrund der besonderen Merkmale des Cloud Computings nunmehr geringere Bedeutung beizumessen ist).

- Somit führt Cloud Computing zu einem Mix an Anpassungsmaßnahmen im Risikoregister der Anwender und auch der Anbieter.

- In diese Betrachtungen ist sowohl die für die Cloud-Umgebung spezifische Ebene (IaaS, PaaS, SaaS) als auch die gewählte bzw. zu wählende Organisationsform (Private, Hybrid, Public) einzubeziehen. Zur Verdeutlichung ist in Kapitel 5.6 ausgehend von einem fiktiven Beispiel eine Auswahl an Risiken mit entsprechenden Risikomaßnahmen hinterlegt.

- Bei allem Optimismus, die derzeit erkennbaren Risiken des Cloud Computings durch geeignete Maßnahmen zur Compliance zu steuern und damit die Chancen des Cloud Computings auf breiter Ebene nutzbar zu machen, müssen aber auch die bestehenden Grenzen beachtet werden, bei denen Cloud Compliance nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. An der Lösung dieser Compliance-Herausforderungen muss heute schon gearbeitet werden. In erster Linie sind hier die Anbieter, die auf derartige Lösungen setzen, gefordert.

5.1 Cloud Compliance – Motive, Herausforderungen und Hürden

Obwohl „Compliance“ in der Praxis oft als abstrakt, komplex und intransparent angesehen wird, ist es in der heutigen Geschäftswelt ein unausweichliches Thema. Im Zusammenhang mit Cloud Computing kommt der Compliance besondere Bedeutung zu:

- um die Verpflichtungen der Beteiligten klar zu formulieren und die Umsetzung zu unterstützen und
- um die erforderliche Transparenz für alle Anspruchsgruppen wie Anteilseigner, Kreditgeber, Interne Revision, Wirtschaftsprüfer, Management etc. zu gewährleisten.

Damit hilft der Compliance-Gedanke zugleich, die derzeitige Zurückhaltung und die bestehenden Vorbehalte im Markt aufzulösen und die Marktakzeptanz insgesamt zu steigern. Compliance leistet insoweit einen wichtigen Beitrag, um den neuen Cloud-Technologien mit allen positiven Eigenschaften und Vorteilen zum Durchbruch zu verhelfen.

Die Auseinandersetzung mit Compliance lenkt die Aufmerksamkeit insbesondere auf die folgenden Fragestellungen (vgl. Abbildung 28):

1. Welche Compliance-Anforderungen gelten für die Cloud? Haben sich diese Anforderungen im Vergleich zur bisherigen Situation geändert?
2. Welche (unter Umständen bisher nicht beachtete?) Risiken sind mit den neuen Technologien und Vorgehensweisen verbunden, und mit welchen Maßnahmen kann diesen begegnet werden?
3. Sind Grenzen absehbar (bereits heute bzw. für die Zukunft), die einem Einsatz von Cloud Computing nach Chance-Risiko-Erwägungen entgegen stehen?

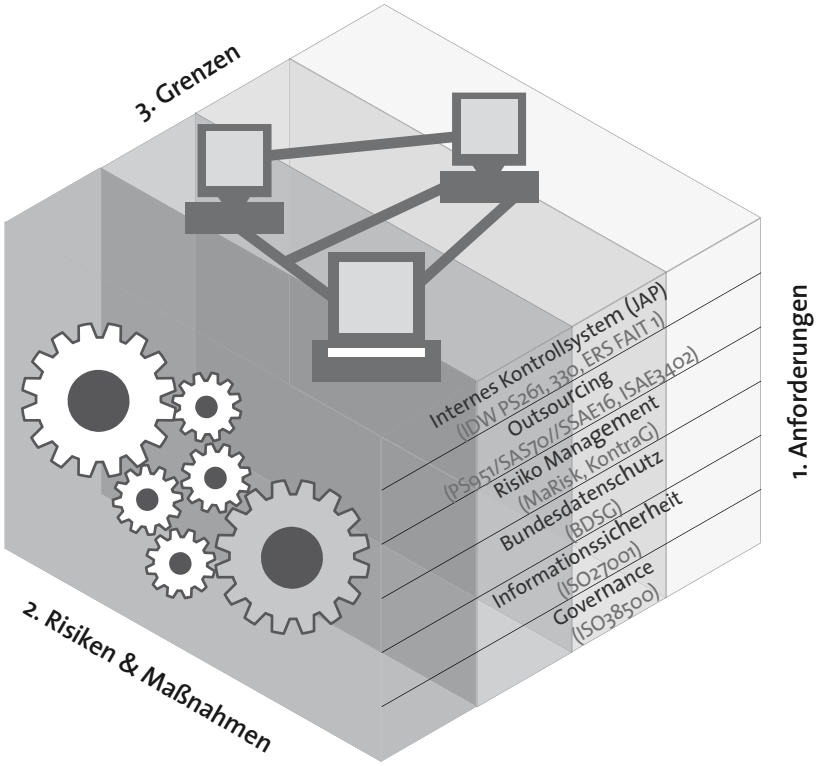


Abbildung 28: Cloud Compliance Herausforderungen

Der Umgang mit diesen Fragen wird durch die mangelnde Transparenz des Cloud-Marktes insgesamt erschwert. Diese ergibt sich aus

- der Neuartigkeit und Komplexität von Cloud Computing,
- der Vielzahl von Service-Angeboten und Geschäftsmodellen der Anbieter,
- unterschiedlichen Cloud Definitionen und
- derzeit noch fehlenden Standards. [39]

5.2 Von der Compliance zur IT-Compliance

Aus dem Englischen übersetzt lässt der Begriff „Compliance“ unterschiedliche Bedeutungen zu:

- Übereinstimmung oder Konformität mit „etwas“ (neutrale Bedeutung),
- Beachtung, Befolgung, Erfüllung (Bedeutung einer impliziten Aufforderung),
- Einhaltung (Bedeutung einer strikten Aufforderung).

In allen Fällen steht Compliance im Zusammenhang mit Vorgaben, Vorschriften oder Anweisungen, die ein Individuum oder ein Unternehmen befolgen soll, um sich „compliant“ zu verhalten. Solche Vorgaben können sowohl extern (beispielsweise durch den Gesetzgeber) als auch intern vorgegeben sein (also freiwilliger Natur, beispielsweise in Form von Qualitätsanforderungen). In jedem Fall sollte – aufgrund der Vielfalt der möglichen Anforderungen und der unterschiedlichen Interessengruppen – auch ein Nachweis über die Entsprechung mit den Anforderungen möglich sein.

39. Mit dem vorliegenden Leitfaden soll auch ein Beitrag zur Markttransparenz geleistet werden.

Compliance ist also ein Zustand, in dem zuvor definierte Vorgaben nachweisbar erfüllt sind. Folglich ist IT-Compliance die nachweisbare Konformität der IT mit den spezifisch für die IT geltenden Vorgaben.

Sofern diese Vorgaben nicht oder nicht vollständig eingehalten werden, ist mit unterschiedlichsten Konsequenzen zu rechnen. Sie hängen davon ab, welche Vorgaben im Einzelnen nicht erfüllt wurden und welcher Schaden in diesem Zusammenhang entstehen kann oder entstanden ist. Hierbei kann schon das Bekanntwerden einer Nichteinhaltung ein Risiko für die Reputation des Unternehmens bedeuten (auch wenn ein messbarer Schaden noch gar nicht erkennbar ist). Die möglichen Konsequenzen einer Nichteinhaltung von IT-Compliance-Anforderungen umfassen beispielsweise

- gesetzliche Strafen und Bußgelder,
- vertragliche Strafen und / oder Schadenersatzansprüche von Kunden oder Dritten,
- den Verlust einer Zulassung,
- die allgemeine Schädigung der Beziehung zu aktuellen und künftigen Geschäftspartnern (Vertrauensverlust; Verlust von Kunden und/oder Ausschluss von Auftragsvergabeverfahren) oder
- verschlechterte externe Bewertungen und Ratings und damit verbunden eine Einschränkung der Finanzierungsmöglichkeiten am Kapitalmarkt.

Um negative Konsequenzen dieser Art zu vermeiden, sollten sich Unternehmen mit den Fragen zur Compliance allgemein und zur IT-Compliance auseinandersetzen.

Aufgrund der hohen Durchdringung der Unternehmensfunktionen mit der IT ist es hierfür erforderlich, alle bestehenden Vorgaben, Vorschriften oder Anweisungen hinsichtlich der Relevanz für die IT zu untersuchen und laufend zu überwachen. Das gilt insbesondere dann, wenn ein Paradigmenwechsel wie Cloud Computing bevorsteht. Hier unterstützt ein entsprechendes Compliance Management System (CMS).

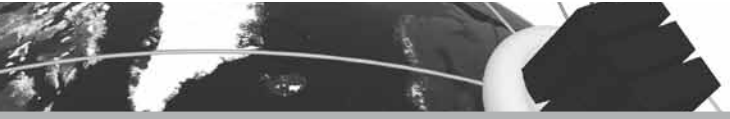
5.3 Compliance Management System

Ziel eines CMS ist es, das regelkonforme Verhalten aller Beteiligten (also die Einhaltung der Regeln und die Verhinderung von Regelverstößen) durch entsprechende Maßnahmen sicherzustellen. Eine praxisnahe Kurzdarstellung für ein CMS wird beispielsweise im Entwurf des Prüfungsstandard 980 des Instituts der Wirtschaftsprüfer (IDW) beschrieben. Für die Praxisumsetzung können aber auch andere Quellen herangezogen werden. Im Kern umfasst ein CMS demnach die nachfolgend (vgl. Tabelle 4 und Abbildung 29) beschriebenen Grundelemente, die in die Unternehmensabläufe eingebunden sind:

Abbildung 29: Grundelemente von Compliance Management Systemen

Tabelle 4: Beschreibung der Grundelemente eines Compliance Management Systems gemäß IDW

Grundelemente	Beschreibung
Compliance-Kultur	Die Compliance-Kultur ist der wesentliche Faktor für die Angemessenheit und Wirksamkeit des CMS. Wie hoch die Bereitschaft der Mitarbeiter zu einem regelkonformen Verhalten ist, hängt stark von der vorherrschenden Kultur ab. Damit sich jedoch eine günstige Compliance-Kultur entwickeln kann, muss eine Unterstützung von Seiten des Managements erfolgen, Anreizsysteme müssen geschaffen und dem Aufsichtsorgan eine gewisse Stellung im Unternehmen zugeordnet werden.
Compliance- Organisation	Die Compliance-Organisation im Unternehmen wird durch das Management festgelegt. Darunter versteht man die Vergabe der Rollen und Verantwortlichkeiten, die Konzeption der Aufbau- und Ablauforganisation und die Integration des CMS in andere bestehende Systeme. Die Compliance-Organisation bildet eine Grundlage für weitere Grundelemente des CMS, da mit dieser die Ressourcen für die Erreichung der Compliance-Ziele, für die Festlegung der Compliance-Risiken und für die Bereitstellung der Compliance-Überwachung und Verbesserung bestimmt werden.
Compliance-Ziele	Die Compliance-Ziele werden von den gesetzlichen Vertretern – z. B. Vorständen bei einer AG – unter Berücksichtigung der allgemeinen Unternehmensziele festgelegt. Auch die Analyse und Gewichtung der unternehmenskritischen Regeln und Vorschriften bilden eine Grundlage für die Entwicklung der Ziele. Diese legen die relevanten Teilbereiche und deren einzuhaltende Regeln für das Unternehmen fest.
Compliance-Risiken	Unter Beachtung der Compliance-Ziele werden die Compliance-Risiken abgestimmt. Diese Risiken stellen Regelverstöße und damit die Missachtung der Compliance-Ziele dar. Zur Festlegung kommt ein Verfahren zur systematischen Risikoerkennung und -berichterstattung zum Einsatz, das die Risiken hinsichtlich der Eintrittswahrscheinlichkeiten und möglichen Folgen analysiert.
Compliance- Programm	Das Compliance-Programm besteht aus Grundsätzen und Maßnahmen, die auf Basis der Risikoanalyse definiert und getroffen werden. Die Vorkehrungen dienen der Prävention von Compliance-Verstößen und sehen Handlungsrichtlinien vor, falls eine Verfehlung eintritt. Auch Kontrollmechanismen wie Funktionstrennungen, Berechtigungskonzepte, Genehmigungsverfahren und Unterschriftsregelungen müssen in das CMS integriert werden.
Compliance- Kommunikation	Damit alle betroffenen Mitarbeiter über die vorhandenen Compliance-Vorschriften informiert werden können, muss eine Compliance-Kommunikation im Unternehmen etabliert werden. Die Informationsweitergabe und das Sicherstellen, dass das Compliance-Programm und damit die Aufgaben im CMS verstanden wurden, stehen hierbei im Vordergrund. Zusätzlich regelt die Compliance-Kommunikation, inwiefern und an welche Stellen Compliance-Verstöße berichtet werden.
Compliance- Überwachung und -Verbesserung	Das letzte Grundelement, die Compliance-Überwachung und -Verbesserung, soll die Angemessenheit und Wirksamkeit des CMS sicherstellen. Eine angemessene Dokumentation gewährleistet die Nachvollziehbarkeit bei Verstößen und ermöglicht somit eine ständige Überwachung des CMS. Im Falle einer Verfehlung oder bei dem Aufdecken einer Schwachstelle kommt es zur Benachrichtigung des Managements bzw. eines Aufsichtsorgans. Die Herausforderung besteht nun darin, die Mängel zu beseitigen und somit das CMS zu verbessern. Eine zusätzliche, kontinuierliche Verbesserung durch das ständige Fahnden nach Sicherheitslücken steigert die Effizienz und erhöht die Effektivität des CMS.



Vereinfachend lassen sich diese Grundelemente des CMS auf die folgenden drei Kernthemen zurückführen:

- Anforderungen (vgl. Abschnitt 5.4),
- Risiken (vgl. Abschnitt 5.5) und
- Risikomaßnahmen (vgl. Abschnitt 5.6)

5.4 IT-Compliance-Anforderungen an Cloud Computing

Die individuellen Rahmenbedingungen eines Unternehmens, die sowohl den Nutzer von Cloud Computing als auch dessen Anbieter betreffen, führen zu unterschiedlichen Anforderungen an die IT-Compliance. Von Bedeutung sind hierbei unter anderem die Branche, die Rechtsform, der Ort der Unternehmung bzw. der Leistungserbringung oder die angebotenen Produkte und Dienstleistungen.

Diese Anforderungen betreffen in aller Regel nicht nur die IT des Anwenders selbst, sondern auch die von externen Anbietern beschafften (IT-)Dienstleistungen. Hierbei muss beachtet werden, dass zwar einzelne Aufgaben jederzeit an beliebige Dienstleister delegiert werden können, dass jedoch die Verantwortung zur Erfüllung dieser Anforderungen (und das Tragen der Konsequenzen bei Nichterfüllung) in aller Regel beim Auftraggeber und Nutzer der Dienste verbleibt.

Dieses Grundprinzip gilt sinngemäß auch für die Auslagerung von Aufgaben oder Prozesse in eine Cloud-Lösung. Für den Auftraggeber ist es daher wichtig herauszufinden, wo und wie seine IT insgesamt („innerhalb und außerhalb der Cloud") von den Anforderungen betroffen ist oder nicht.

Die Tabelle 5 zeigt beispielhaft eine vereinfachte Kategorisierung von Anforderungen mit Bedeutung für IT-Compliance im Überblick.

Tabelle 5: Beispielhafte Kategorisierung von IT-Compliance-Anforderungen

Primär externe Vorgaben		Primär interne Vorgaben	
Gesetzliche Regelungen	Externe Regelwerke	Interne Verpflichtungen	Verträge
SOX	GoBS	Ethik-Richtlinie (Code of Ethics)	Software-Lizenzverträge
HGB	GDPdU	IT-Einkaufsrichtlinie	Outsourcing-Verträge (SLA)
KonTraG	ISO 20000	E-Mail-Richtlinie	Wartungsverträge
EG Dual Use	ISO 38500	Richtlinie zur Internetnutzung	Verträge zur Geheimhaltung
...	...	...	...

Auf Basis vergleichbarer Überlegungen kann ein Unternehmen die jeweilige Relevanz der einzelnen Anforderungen überprüfen und erforderlichenfalls weitere Schritte zur Umsetzung seiner IT-Compliance-Maßnahmen planen.

Im Hinblick auf Cloud Computing insgesamt ist dabei festzuhalten, dass für Cloud Computing dem Grunde nach die bisher bekannten Anforderungen gelten. Cloud-Computing-Anforderungen unterscheiden sich also nicht von den allgemeinen IT-Compliance-Anforderungen.

Weiterhin ist darauf hinzuweisen, dass sich die IT-Compliance-Anforderungen im Prinzip in jedem Fall auf die allgemeinen Ziele zur adäquaten Behandlung von IT-Risiken reduzieren lassen. Dies können im Einzelnen insbesondere Sicherheit, Verfügbarkeit, Vollständigkeit und Nachvollziehbarkeit etc. sein.

Gesetzliche Regelungen

Auch Gesetze, deren Namen und Inhalt nicht sofort mit IT in Zusammenhang gebracht wird, enthalten nicht selten Einzelanforderungen im Sinne von IT-Compliance. Eine besondere (zweifelhafte) „Berühmtheit" hat hierzu in den letzten Jahren der viel zitierte Sarbanes Oxley-Act[40] erlangt.

Nun hat dieser Leitfaden nicht die Aufgabe, alle denkbaren Compliance-Anforderungen ausführlich darzustellen. Vor diesem Hintergrund werden nachfolgend exemplarisch grundlegende handelsrechtliche bzw. steuerrechtliche Aspekte allgemein dargestellt. Darüber hinaus wird als gesondertes Einzelbeispiel die Dual-Use-Verordnung im Zusammenhang mit exportwirtschaftlichen Fragestellungen zur Veranschaulichung weiter ausgeführt.

Für externe Interessenten allgemein, aber insbesondere auch für die Finanzverwaltung, bilden die Abschlüsse und Finanzinformationen eines Unternehmens eine wesentliche Informationsquelle. Die Finanzberichterstattung folgt daher strengen Regeln und unterliegt zum Teil der externen Überprüfung und Überwachung.

Betroffen sind von diesen Regeln im Prinzip alle Aktivitäten, die einen Einfluss darauf haben, wie Unternehmenstransaktionen initiiert, aufgezeichnet, verarbeitet und berichtet werden. Hierzu genügt es, dass diese Aktivitäten direkt oder indirekt die Vermögens-, Finanz- oder Ertragslage eines Unternehmens beeinflussen. Beispiele für solche Aktivitäten sind Produktion, Lagerhaltung, Logistik oder die Lohn- und Gehaltsabrechnung. In unmittelbarer Folge sind auch die unterstützenden IT-Aktivitäten von damit verbundenen Anforderungen betroffen. Der damit beispielsweise seitens der Finanzverwaltung verbundene Grundgedanke lässt sich in wenigen Schritten darstellen: Korrekte und verlässliche Finanzdaten können nur dann sichergestellt werden, wenn

- im Zuge ihrer Erstellung, Verarbeitung und Darstellung auch in der IT keine Möglichkeiten zur Verfälschung gegeben sind,
- dennoch (im Zusammenhang mit der IT) auftretende Fehler erkannt und behoben werden,
- allgemein die Sicherheit und Verfügbarkeit der IT-Systeme gewährleistet ist und
- die Nutzung der IT bestimmten allgemeinen Grundregeln unterliegt.

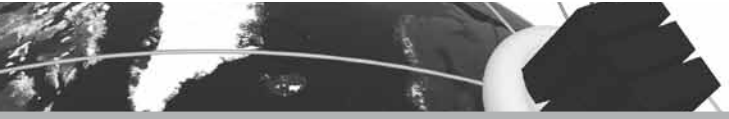
Um dieses Ziel zu unterstützen, wurden eine Reihe von Präzisierungen für IT Compliance-Anforderungen definiert (vgl. auch nächster Abschnitt). Diese betreffen umfangreiche Einzelregelungen zum Einsatz der IT im Unternehmen wie beispielsweise in den Bereichen IT-Umfeld, Informationssicherheit, Programmentwicklung, Programmpflege und IT-Betrieb.

Das Besondere an diesen Anforderungen im Zusammenhang mit Cloud Computing liegt darin, dass vor allem die Finanzverwaltung ein hohes Interesse daran hat, dass die Daten sicher und geschützt vor nicht autorisierten Änderungen verarbeitet werden. Wesentlich in diesem Zusammenhang ist auch die Frage der Verfügbarkeit für die Finanzverwaltung. Daher unterliegt eine Datenverarbeitung im Ausland für steuerliche Zwecke gesonderten Auflagen und Anforderungen.

Das zweite konkrete Einzelbeispiel bilden allgemeine exportkontrollrechtliche Bestimmungen (EG-Dual-Use-Verordnung). Auch diese sind im Hinblick auf IT Compliance-Anforderungen zu berücksichtigen.

Dabei ist zu beachten, dass der nicht-physische Transfer von Daten, Technologie und Software im Prinzip den gleichen exportkontrollrechtlichen Beschränkungen wie der physische Transfer von Gütern unterliegt. Entsprechend müssen die zu transferierenden Daten vor dem Zugriff durch sanktionierte („gelistete") Personen, Unternehmen

40. Die im Zusammenhang mit dem Sarbanes Oxley-Act in den USA getroffenen Regelungen sollen die Integrität, Vollständigkeit und Korrektheit der Daten für die Finanzberichterstattung unterstützen.



und Organisationen geschützt werden. Gleichzeitig müssen etwaige Beschränkungen für den Transfer von Daten beachtet werden, die an verschiedene Faktoren[41] anknüpfen. Die Beschränkungen gelten in erster Linie, aber nicht ausschließlich, für den grenzüberschreitenden Datentransfer. Bereits die bloße Zugriffsmöglichkeit durch einen ausländischen Administrator oder eine anderweitig beteiligte ausländische Person per se kann als Export im Sinne dieser Vorschriften gewertet werden.

Die Umsetzung der exportkontrollgesetzlichen Vorgaben wird (schon unabhängig von den besonderen Aspekten des Cloud Computing) dadurch erschwert, dass die exportkontrollrechtlich kritischen Daten häufig in verschiedenen Systemen und Anwendungen integriert sind, so dass eine Identifikation und Isolation dieser Daten einen sehr hohen Aufwand bedeuten. Hierzu bedarf es der Definition klarer Prozesse zur Selektion entsprechend der exportkontrollrechtlichen Relevanz.

Externe Regelwerke

Externe Regelwerke können in Form von Richtlinien und allgemeinen Standards auftreten. Exemplarisch zu nennen sind in Fortsetzung des Beispiels aus dem vorstehenden Abschnitt die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS) oder die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU). Beide Regelungen unterstützen letztlich die Durchsetzung des Steueranspruchs durch die Finanzverwaltung, indem konkrete Vorgaben bezüglich Art und Inhalt der Datenverarbeitung im Umfeld von Buchführungssystemen gegeben werden.

Auch privatrechtliche Institutionen können externe Regelwerke (meistens als allgemeine Qualitätsstandards und/oder „Good Practice“) erarbeiten. Hierzu zählen beispielsweise das Deutsche Institut für Normung (DIN) oder die International Organization for Standardization (ISO). Von der ISO entwickelte Standards umfassen unter anderem die ISO/IEC 20000 (IT Service Management) oder die ISO/IEC 38500 (Corporate Governance of Information Technology). Solche Standards sind rechtlich zunächst nicht verpflichtend. Dies gilt zumindest solange, wie sie nicht konkret in einzelne Rechtsnormen aufgenommen wurden. Unabhängig davon können sie aber jederzeit zivilrechtlich zwischen einzelnen Vertragsparteien gesondert vereinbart werden.

Etablierte Standards können bei wachsender Verbreitung und Akzeptanz als „Stand der Technik“ oder „übliche Berufsauffassung“ angesehen werden. Dies hat zur Folge, dass über allgemeine Grundsätze einer ordnungsgemäßen Geschäftsführung zumindest eine indirekte Verpflichtung zur Einhaltung entstehen kann. Einer derartigen Verpflichtung kann dann wiederum in gerichtlichen Auseinandersetzungen besondere Bedeutung zukommen, wenn im Zusammenhang mit der Nichteinhaltung / Zuwiderhandlung Nachteile oder Schäden entstehen.

Interne Verpflichtungen und Verträge

Interne Verpflichtungen umfassen beispielsweise eigens definierte Unternehmensrichtlinien (z.B. für ethische Werte, den IT Einkauf oder die Internet- bzw. E-Mail Nutzung) zur Umsetzung der jeweils gewünschten Vorgaben.

Bei den Verträgen handelt es sich um alle Vereinbarungen, die mit Geschäftspartnern geschlossen wurden. Mögliche Geschäftspartner sind neben den eigenen Kunden natürlich auch Hersteller und Lieferanten von Hard- und Software, Anbieter von Dienstleistungen sowie sonstige Zulieferer in der Wertschöpfungskette des Unternehmens.

Da es sich bei den internen Verpflichtungen und Verträgen jeweils um sehr unterschiedliche und individuelle Inhalte handelt, wird hier auf eine detaillierte Darstellung verzichtet.

Ein für den Umgang mit Cloud Computing besonderer Punkt zeichnet sich aus den oben angeführten Beispielen ab: Die Anforderungen können aufgrund der Ausgestaltung des Cloud Computings eine besondere und bisher im Zweifel nicht oder nicht so umfassend beachtete

41. Art der Daten, Verwendungszweck der Daten, Standort der Server, Nationalität der beteiligten Personen mit Zugriffsmöglichkeit

Bedeutung erlangen. Dies wird deutlich, wenn es direkt oder indirekt um die Frage geht, in welchen Ländern die Daten gehalten bzw. verarbeitet werden, oder wenn die Frage betroffen ist, wie die Anbieter von Cloud Computing mit spezifischen Anforderungen zur Sicherheit und zum Datenschutz länderübergreifend umgehen.

5.5 Compliance-Risiken in der Cloud

Der Begriff „Risiko" kann generell als das Produkt aus Eintrittswahrscheinlichkeit und Schadenshöhe bei Abweichung von einem angestrebten Zielzustand verstanden werden.

Der angestrebte Zielzustand ist die Erfüllung der Anforderungen aus externen und internen Regularien und Vorschriften. Wie im Abschnitt 5.4 dargelegt, verändern sich die grundlegenden Anforderungen auch bei Einsatz des Cloud Computings nicht.

Mithin stellt sich die Kernfrage, ob und inwieweit mit der Nutzung von Services aus der Cloud neue, bisher wenig oder nicht beachtete Risiken verbunden sind oder ob altbekannte Risiken angesichts der Cloud einer neuen Bewertung unterzogen werden müssen?

Ein Service aus der Cloud weist in der Regel „neue" Merkmale auf, die in der bisherigen „klassischen" IT nicht existieren. Dazu zählen u. a.

- der Applikationsbezug über das Internet,
- die hohe Virtualisierung sowie
- die Multi-Mandanten-Fähigkeit der Infrastruktur.

Einhergehend mit dieser Entwicklung müssen die Risiken neu bewertet werden.

Eine Virtualisierung der Betriebssysteme führt beispielsweise dazu, dass die Administratoren der Host-Systeme Zugriff auf die Gastsysteme haben können. Damit müssen die Maßnahmen, die bisher auf Betriebssystemebene für das Priviliged Account Management vorgesehen waren, auch auf die Betriebssystem-Virtualisierungsebene angewendet werden.

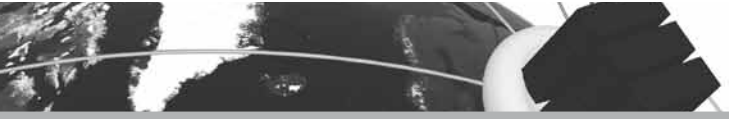
Ein anderes Beispiel: Wird der Cloud Service aus dem Internet bezogen, so birgt der Ausfall der Internetverbindung ggf. ein besonderes Risiko für die Geschäftsprozesse des Unternehmens (bei für das Geschäft des Anwenders kritischen Komponenten). Damit sind die Maßnahmen, die bisher die geforderte Verfügbarkeit des lokalen Netzes sicherstellen sollten, analog auch auf die Internetanbindung anzuwenden. Ergänzend kommen neue Risiken hinzu, die nur indirekt mit dem Ausfall von beteiligten Komponenten in Verbindung stehen. So können besondere Internetdienste, auch wenn es sich „nur" um das Live-Streaming während einer Fußball-Weltmeisterschaft handelt, die Internetverbindung so stark auslasten, dass ein Cloud-Service beeinträchtigt wird. Hier sind ggf. risikominimierende Maßnahmen zu treffen, die neu sind im Vergleich zu den Maßnahmen in der klassischen IT.

Anderseits dürfte das Verfügbarkeitsrisiko aufgrund von beispielsweise Festplattendefekten einzelner Server bei Bezug eines Services aus der Cloud tendenziell sinken (zumindest ist zu erwarten, dass die Service-Provider hierfür entsprechend Vorsorge getroffen haben).

Diese vereinfachten Beispiele zu den Risiken des Bezugs von Services aus der Cloud zeigen, dass verschiedene Arten von Risiken betrachtet werden müssen, um über geeignete Maßnahmen eine anforderungsgerechte Cloud-Dienstleistung (und damit die Cloud Compliance) sicherzustellen.

Im Einzelnen lassen sich diese Risiken, jeweils im Vergleich zu bisherigen „klassischen" IT-Lösungen, wie folgt kategorisieren:

- gleichbleibende oder erhöhte Risiken, die ein neues Cloud-Merkmal betreffen, denen mit analogen Maßnahmen begegnet werden kann (z. B. Privileged Accounts auf einer Virtual Storage Management Station).
- neue Risiken, denen mit neuen Maßnahmen begegnet werden muss (z. B. Internet Auslastung).
- tendenziell eher reduzierte Risiken, da die Infrastrukturelemente beispielsweise als Service und nicht als Hardwarekomponente eingekauft werden (z. B. Ausfall einer Festplatte)



Um einschätzen zu können, welche Risiken Cloud-Umgebungen in der spezifischen Ebene (IaaS, PaaS, SaaS) und Organisationsform (Private, Hybrid, Public) mit sich bringen, sind sowohl eine detaillierte Analyse des zu beziehenden Service und aller genutzten Komponenten, als auch die Kenntnis über die neuen Cloud-Merkmale notwendig.

Diese umfassende Risikobetrachtung ist erforderlich, um anschließend Maßnahmen zu ergreifen und somit den Anforderungen zu genügen. Die Komplexität der Risikoanalyse sollte hierbei nicht unterschätzt werden.

5.6 Exemplarische Risikobetrachtung

In diesem Abschnitt des Kapitels Cloud Compliance sind exemplarische Risiken anhand eines Beispiels aufgeführt, die bei der Nutzung von Cloud-Services auftreten können. Es soll dabei ein Überblick gegeben werden, welche Themen, Infrastrukturen, Prozesse und Organisationen betrachtet werden können (ohne Anspruch auf Vollständigkeit).

Zur Reduktion der Komplexität durch die Vielfalt an Kombinationsmöglichkeiten von Service-Ebene, Organisationsform und Cloud-Merkmal wird folgendes Einsatzszenario betrachtet:

Eine ERP-Lösung mit einem Modul zur Finanzbuchhaltung wird als Software as a Service genutzt.

- Der Zugriff auf die Lösung erfolgt ausschließlich über das Internet.
- Der Anbieter bietet ausschließlich Public-Cloud-Services an.
- Die Daten liegen derzeit in zwei Rechenzentren in Deutschland.
- Die Software ist mandantenfähig, d. h. auf einer Instanz arbeiten verschiedene Kunden.

Bei einer ERP-Software spielen unter anderem die Anforderungen an die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS), der Prüfungsstandard 330 des Instituts der Wirtschaftsprüfer (IDW) sowie die IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1) eine wichtige Rolle. Ebenso ist von einer gewissen Kritikalität für den Geschäftsprozess auszugehen.

In der Tabelle 6 werden beispielhaft für das gewählte Szenario geänderte und neue Risiken aufgezählt, die sowohl den Provider, als auch den Kunden betreffen.

Tabelle 6: Beispielhafte Risikosituationen

#	Risikosituationen
R1	Die Verfügbarkeit der Internetanbindung, sowohl der eigenen, als auch der des Provider, sind ein Risiko für die Verfügbarkeit der Anwendung und somit der Geschäftsprozesse. Der Internetzugang ist daher mehr als nur ein Instrument zu Informationsgewinnung der Mitarbeiter.
R2	Stellt der Anbieter seinen Service ein, z. B. durch Insolvenz oder im Rahmen einer Fusion, besteht das Risiko, dass der Service dem Nutzer nicht mehr zur Verfügung steht. Dann muss ein kurzfristiger Ersatz gefunden und die Daten müssen schnell auf die neue Plattform migriert werden.
R3	Der Update eines Service auf einen nächsten Release-Stand kann in einer Multi-Mandanten-Umgebung zu unerwünschten Seiteneffekten in der eigenen Anwendung führen. Der Nutzer sollte hierbei eigentlich in die Test- und Freigabeprozesse aktiv eingebunden sein. Der Anbieter muss allerdings, um kosteneffizient zu arbeiten, möglichst einheitliche Services anbieten, so dass es normalerweise kein Mitspracherecht der Kunden hinsichtlich des Upgrade-Zeitpunkts gibt.

#	Risikosituationen
R4	Angriffe auf und über den Web Browser des Mitarbeiters, der den Service nutzt (z. B. Cross-Site-Scripting), stellen ein zusätzliches Risiko für die Integrität und Vertraulichkeit der Daten dar.
R5	Werden seitens des Anbieters, z.B. für eine Fehlersuche, Protokolldaten herausgegeben, besteht das Risiko, dass in dem Protokoll auch Informationen von anderen Kunden (z. B. personenbezogene Daten) enthalten sind. Je nach Protokollierungseinstellung (Debug-Log) können hier kritische Daten irrtümlicherweise herausgegeben werden.
R6	Während des laufenden Vertrages kauft sich der Service-Provider IT-Kapazitäten (z. B. einen Datenbank-Service) von anderen Cloud-Anbietern ein, mit dem Ziel, die eigenen Kapazitäten zu erweitern. Hier besteht das Risiko, dass Daten zum Teil oder vollständig, zeitweise oder auf Dauer ins Ausland verlagert werden. Im konkreten Beispiel handelt es sich um einen beim zuständigen Finanzamt genehmigungspflichtigen Vorgang. Etwaige Verstöße können finanziell geahndet werden. Das Risiko für den Nutzer bleibt selbst dann bestehen, wenn er von seinem Dienstleister über den Vorgang informiert wird, selbst aber keine Eingriffsmöglichkeit hat, um den Transfer nachweislich zu unterbinden.
R7	Wird der Anbieter des Service von einer anderen (z. B. ausländischen) Unternehmung aufgekauft, kann es je nach Geschäftsgebaren dazu führen, dass die Daten in ein ausländisches Rechenzentrum verlagert werden. Dies ist auch der Fall, sofern der Cloud-Anbieter keine Garantie geben kann, dass sich die Daten exklusiv im Zugriff der deutschen Steuerbehörden (Staatsgebiet der Bundesrepublik) befinden.
R8	Dem Cloud Computing immanent ist der unbekannte bzw. nicht hinreichend zu identifizierende Standort der am Datentransfer beteiligten Server. Daher bestehen Unwägbarkeiten hinsichtlich der einzelnen involvierten Länder. Zur Vermeidung unberechtigter Zugriffe, die einen Verstoß gegen exportkontrollrechtliche Vorschriften bedeuten können, ist eine Identifizierung und Aussonderung von Daten (bzw. der diese speichernden Server), deren Transfer wegen exportkontrollrechtlicher Relevanz nicht zulässig ist, erforderlich.
R9	Dadurch, dass der Service über das Internet erreichbar ist, besteht das Risiko, dass Mitarbeiter von nicht vertrauenswürdigen Endgeräten (z. B. Internet Cafe, Mobile Device) auf den Service zugreifen. Alle Informationen, die über solche Endgeräte laufen, können potentiell von Dritten mitgelesen werden. Im Fall von mobilen Endgeräten können diese Daten verloren gehen oder gestohlen werden.
R10	Bei der Migration der Buchhaltung auf ein neues System sind eine Schlussbilanz und eine Eröffnungsbilanz zu erstellen, die auch der Prüfung durch den Abschlussprüfer und ggf. der Finanzverwaltung unterliegt. Kann die Vollständigkeit und Korrektheit der übertragenen Daten nicht oder nur manuell verifiziert werden, entsteht ein Risiko hinsichtlich Vollständigkeit und Richtigkeit sowohl für den Jahresabschluss des Nutzers, als auch hinsichtlich der Besteuerungsgrundlagen.

In der Abbildung 30 sind diese Risiken kontextbezogen dargestellt.

Bei anderen Szenarien können sich andere Risiken ergeben. So besteht bei einer „Platform as a Service“-Dienstleistung z.B. das Risiko, dass die von der Software lokal abgelegten Daten (z. B. Zugriffs-Protokolle) beim De-Provisionieren der Plattform verloren gehen. Damit erhöht sich z. B. das Risiko, dass Angriffe unentdeckt bleiben, die auf diesen Server erfolgt sind.

Allgemein kann man sagen, dass die Risiken bei der Nutzung von Cloud-Services tendenziell höhere Schichten der IT treffen. Die Risiken sind also weniger im Ausfall der System-Hardware begründet, als vielmehr in den Störungen der Kommunikation mit einem Service. Die höhere Anzahl an Schichten, deren verstärkte Abhängigkeiten sowie die relative Neuheit der Risiken führen zu der Schlussfolgerung, dass die Analyse der Risiken ein sorgsames Vorgehen erfordert.

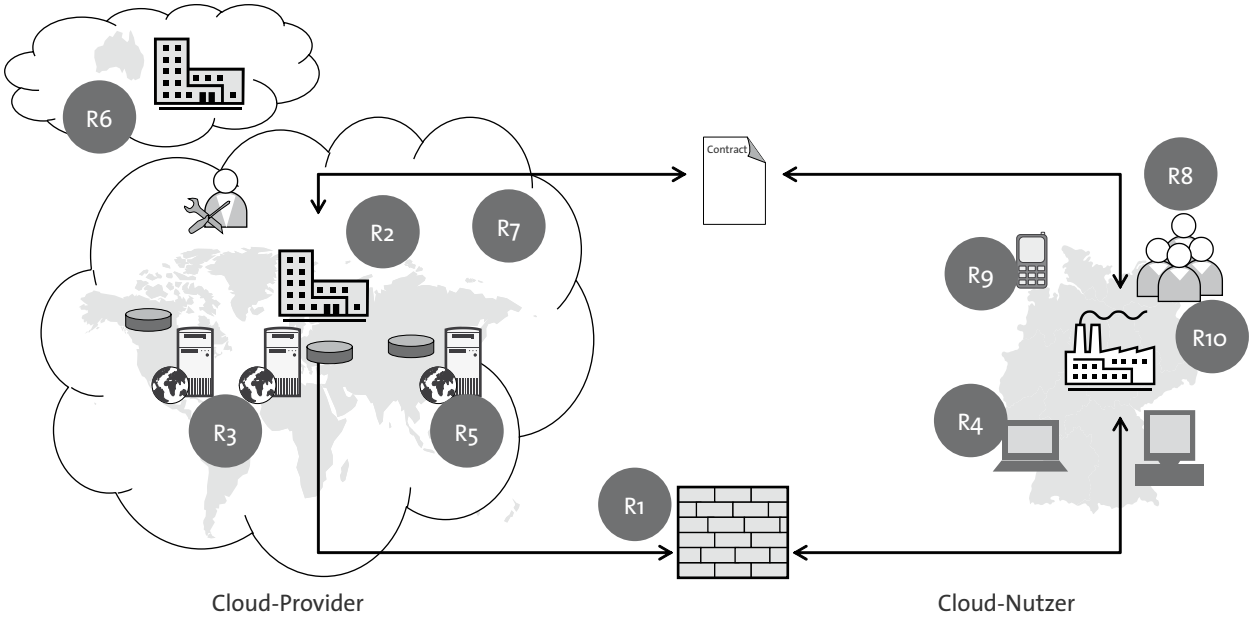


Abbildung 30: Kontextbezogene Risikosituationen

5.7 Grenzen zur Erreichung von Cloud Compliance

Auch bei Beachtung aller Hinweise in den bisherigen Ausführungen können Situationen nicht ausgeschlossen werden, in denen Cloud Compliance nur mit unverhältnismäßigem Aufwand oder gar nicht erreicht werden kann:

- Im Zuge von Cloud-Diensten können Prozessverantwortliche ihre Prozesse zukünftig dank Service-orientierter Architekturen ohne Beteiligung der IT-Abteilung konfigurieren und anpassen.
- Die mit der Serviceorientierung verbundene Orchestrierung kann dazu führen, dass sich Cloud-Services unterschiedlicher Anbieter flexibel und beliebig lange in eine bestimmte Prozessaktivität integrieren lassen. Ein Anbieterwechsel könnte somit mehrmals im Monat geschehen.
- Zudem könnten sich das Prozessdesign und die damit verbundenen Prozessaktivitäten ständig ändern, was aus Sicht der Kunden zu ständig wechselnden Risikosituationen führen kann. Neuere Systeme zur Warenwirtschaft und Unternehmensplanung sind hierzu bereits in der Lage.
- Die Entscheidung darüber, welcher Provider zu welchem Prozessschritt genutzt wird, könnte agentenbasiert auf einem Cloud-Marktplatz gefällt werden. Im Bereich Logistik gibt es das heute schon.
- Auch ein Dienste-Handel im Sinne einer Börse für Cloud-Services ist denkbar. Spezielle Service-Integratoren könnten sich hier bedienen und kombinierte Servicepakete als Dienstleistungen platzieren.
- Cloud Computing, wie in diesem Kapitel dargestellt, würde die gesamte Informationswirtschaft, ihre Technologien und das Business der Fachabteilungen nachhaltig verändern. An die IT-Compliance solcher Szenarien ist bisher noch gar nicht gedacht. Daher muss mit der Arbeit zur Lösung dieser Compliance-Herausforderungen rasch begonnen werden. Cloud-Anbieter, die derartige Möglichkeiten im Rahmen ihrer Service-Erbringung anbieten, sollten sich im Rahmen ihres Service-Designs bereits jetzt Gedanken darüber machen.

Autoren

Kapitel „Cloud Computing als neues Paradigma zur Erbringung von IT-Services“

- Dr. Achim Luhn, Siemens AG, Arbeitskreis „Cloud Computing und Outsourcing“
- Gerald Münzl, IBM Deutschland Management & Business Support GmbH, Arbeitskreis „Cloud Computing und Outsourcing“
- Bernhard Przywara, Oracle Deutschland B.V. & Co. KG, Arbeitskreis „Cloud Computing und Outsourcing“
- Dr. Martin Reti, T-Systems International GmbH, Arbeitskreis „Cloud Computing und Outsourcing“
- Karin Sondermann, Microsoft Deutschland GmbH, Arbeitskreis „Cloud Computing und Outsourcing“
- Christian Tüffers, Accenture GmbH, Arbeitskreis „Cloud Computing und Outsourcing“
- Dr. Mathias Weber, BITKOM e. V.

Kapitel „Vertragliche Regelungen“

- Dr. Lutz Beilschmidt, Becosys AG, Arbeitskreis „ITK-Vertrags- und Rechtsgestaltung“
- Dr. Oliver Bühr, SKW Schwarz Rechtsanwälte, Arbeitskreis „Cloud Computing und Outsourcing“
- Dieter Götz, Atos Origin GmbH, Arbeitskreis „ITK-Vertrags- und Rechtsgestaltung“
- Dr. Philipp Haas, Kabel Deutschland GmbH, Arbeitskreis „ITK-Vertrags- und Rechtsgestaltung“
- Christof Höfner, Nokia Siemens Networks GmbH & Co. KG, Arbeitskreis „ITK-Vertrags- und Rechtsgestaltung“
- Stefan Koll, DATEV eG, Arbeitskreis „ITK-Vertrags- und Rechtsgestaltung“
- Thomas Konowalczyk, CA Deutschland GmbH, Arbeitskreis „ITK-Vertrags- und Rechtsgestaltung“
- Jens Konradi, T-Systems International GmbH, Mitglied im Lenkungsausschuss „Steuern und Recht“, Stellvertretender Vorsitzender des Arbeitskreises „ITK-Vertrags- und Rechtsgestaltung“
- Dr. Ingo-Wolf Marfording, IDS Scheer EMEA GmbH, Stellvertretender Vorsitzender im Lenkungsausschuss „Steuern und Recht“, Stellvertretender Vorsitzender des Arbeitskreises „ITK-Vertrags- und Rechtsgestaltung“
- Dr. Jan Geert Meents, DLA Piper UK LLP, Arbeitskreis „Cloud Computing und Outsourcing“
- Martin Schweinoch, SKW Schwarz Rechtsanwälte, Mitglied im Lenkungsausschuss „Steuern und Recht“, Vorsitzender des Arbeitskreises „ITK-Vertrags- und Rechtsgestaltung“
- Michaela Tews, Thales Deutschland GmbH, Arbeitskreis „ITK-Vertrags- und Rechtsgestaltung“

Kapitel „Cloud Computing und Datenschutz“

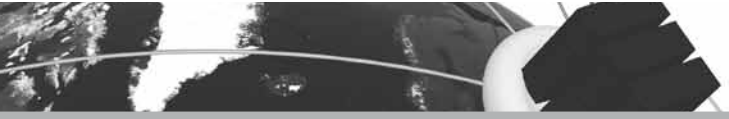
- Bernd H. Harder, Harder Rechtsanwälte, Mitglied im Hauptvorstand und im Lenkungsausschuss „Steuern und Recht“, Stellvertretender Vorsitzender des Arbeitskreises „Intellectual Property“
- Ralf Maruhn, Nokia GmbH, Stellvertretender Vorsitzender des Arbeitskreises „Datenschutz“

Kapitel „Cloud Computing und Informationssicherheit“

- Frank Hebestreit, IBM Deutschland GmbH, Arbeitskreis „Sicherheitstechnologien“
- Lutz Neugebauer, BITKOM e. V.
- Angelika Ruppel, Fraunhofer SIT Institut für Sichere Informationstechnologie, Arbeitskreis „Sicherheitstechnologien“
- Tobias Schubert, TREND MICRO Deutschland GmbH, Arbeitskreis „Sicherheitstechnologien“
- Philipp Stephanow, Fraunhofer SIT Institut für Sichere Informationstechnologie
- Dr. Thomas Störtkuhl, Secaron AG, Arbeitskreis „Sicherheitstechnologien“
- Iryna Tsvihun, Fraunhofer SIT Institut für Sichere Informationstechnologie, Arbeitskreis „Sicherheitstechnologien“
- Arno Van Züren, TREND MICRO Deutschland GmbH, Arbeitskreis „Sicherheitstechnologien“

Kapitel „Cloud Compliance“

- Dr. Markus Böhm, PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft, Arbeitskreis „Cloud Computing und Outsourcing“



- Eiko Ermold, PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft, Arbeitskreis „Cloud Computing und Outsourcing“
- Dr. Axel Keßler, Siemens AG, Arbeitskreis „Cloud Computing und Outsourcing“
- Markus Vehlow, PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft, Arbeitskreis „Cloud Computing und Outsourcing“
- Heino Wehran, PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft, Arbeitskreis „Cloud Computing und Outsourcing“

Unterstützende Unternehmen und Organisationen

Dieser Leitfaden ist ein Projekt des BITKOM aus dem Aktionsprogramm Cloud Computing des Bundesministeriums für Wirtschaft und Technologie. Die BITKOM-Projekte werden mit freundlicher Unterstützung folgender Unternehmen durchgeführt:

Accenture ist ein weltweit agierender Managementberatungs-, Technologie- und Outsourcing-Dienstleister mit rund 204.000 Mitarbeitern, die für Kunden in über 120 Ländern tätig sind. Das Unternehmen bringt umfassende Projekterfahrung, fundierte Fähigkeiten über alle Branchen und Unternehmensbereiche hinweg und Wissen aus qualifizierten Analysen der weltweit erfolgreichsten Unternehmen in eine partnerschaftliche Zusammenarbeit mit seinen Kunden ein. Accenture erwirtschaftete im vergangenen Fiskaljahr (zum 31. August 2010) einen Nettoumsatz von 21,6 Mrd. US-Dollar.
www.accenture.de [bzw .at/.ch]

Das Technologieunternehmen Alcatel-Lucent entwickelt innovative Lösungen und Dienste, die den Menschen neue Kommunikationsformen ermöglichen. Als einer der weltweit führenden Ausrüster bei Festnetz, Mobilfunk und konvergenten Breitbandnetzen weiß Alcatel-Lucent, wie sich die Kommunikationsnetze weiterentwickeln werden und welche Bedürfnisse der Kunden dahinter stehen. Mit seiner High-Leverage-Network Architektur bietet Alcatel-Lucent eine Antwort auf die zentrale Herausforderung der Netzbetreiber, eine leistungsfähige und kostengünstige Datenübertragung zu ermöglichen und gleichzeitig innovative Dienste anzubieten sowie neue Erlösquellen zu erschließen.
www.alcatel-lucent.de

CA Technologies (NASDAQ: CA) ist ein Anbieter von IT-Management-Software und -Lösungen mit Expertise über alle IT-Umgebungen hinweg - vom Mainframe über physische und virtuelle Umgebungen bis hin zur Cloud. CA Technologies verwaltet und sichert IT-Umgebungen und ermöglicht es so Unternehmen, flexiblere IT-Dienste zu liefern. Die innovativen Produkte und Services von CA Technologies ermöglichen den Einblick und die Kontrolle, die IT-Organisationen benötigen, um ihren Geschäftsprozessen die nötige Agilität zu verleihen. Die Mehrheit der Global Fortune 500-Unternehmen vertraut auf CA Technologies, um ihre sich kontinuierlich entwickelnden IT-Systeme zu steuern.
www.ca.com/de

Als der weltweit führende Anbieter von Netzwerk-Lösungen für das Internet verändert Cisco die Art und Weise, wie Menschen miteinander verbunden sind, kommunizieren und arbeiten. Cisco gestaltete die Durchsetzung des Internet-Protokolls (IP) als Standard wesentlich mit. Unternehmen steigern mit den Lösungen von Cisco ihre Produktivität, verbessern die Kundenzufriedenheit und verschaffen sich Wettbewerbsvorteile; Privatanwender vernetzen sich vielfältig über das World Wide Web. 2009 wurde Cisco zum dritten Mal in Folge beim Wettbewerb „Deutschlands Beste Arbeitgeber 2009“ vom Great Place to Work® Institute Deutschland mit einer Top 3 Platzierung ausgezeichnet.
www.cisco.com

Computacenter ist Europas führender herstellerübergreifender Dienstleister für Informationstechnologie. Computacenter ist der Integrator von Hybrid Modellen zwischen Public Clouds, Private Clouds und individuellen Lösungen. Im Rahmen seiner Outsourcing-2.0-Services verfügt der IT-Dienstleister über langjährige Erfahrung und Referenzen in der Überführung von Kunden auf seine Cloud-Plattform und in IaaS-End-to-End-Services. Durch die Abbildung in Private und Virtual Private Clouds bei Computacenter sind Datenhaltung und die Möglichkeit des Datenzugriffs für Kunden transparent und technisch wie auch prozessual abgesichert. Im Jahr 2009 erwirtschaftete die Computacenter-Gruppe mit 10.200 Mitarbeitern einen Umsatz von rund 2,5 Milliarden Pfund.

www.computacenter.de

Die DATEV eG, Nürnberg, ist das Softwarehaus und der IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren Mandanten. Über sein Rechenzentrum bietet das Unternehmen auch Cloud-Dienste in Bereichen wie klassische Datenverarbeitung, Bereitstellung von Software sowie von Infrastruktur, Datenverteilung, Managed Security Services und Speicherplatz für die Sicherung und Archivierung von Daten an. Aus Sicherheitsgründen setzt DATEV vornehmlich auf geschlossene Cloud-Systeme. Das DATEV-Rechenzentrum dient zudem als Datendrehscheibe zwischen mittelständischen Unternehmen und deren Steuerberatern sowie rund 200 Institutionen in Deutschland.

www.datev.de

Equinix Inc. verbindet Unternehmen mit Partnern und Kunden auf der ganzen Welt über seine globale Plattform an Hochleistungs-Rechenzentren, die über eine dynamische Infrastruktur und eine breite Palette an Netzwerkzugängen verfügen. Mehr als 3700 Unternehmen, Cloud-Service-Provider, Anbieter digitaler Inhalte und Finanzdienstleister nutzen die Leistungen von über 600 Netzwerkbetreibern in den Rechenzentren von Equinix und setzen diese Plattform als Basis für ihre Geschäftsentwicklung, für eine Optimierung der Applikationsleistungen sowie für die Bereitstellung und den Schutz ihrer digitalen Ressourcen ein. Insgesamt betreibt das Unternehmen Rechenzentren für 35 strategische Märkte weltweit.

www.equinix.de

Die forcont business technology gmbh stellt dokumentenzentrierte Anwendungen auf Basis der ECM-Business-Software forcont factory FX online als SaaS zur Verfügung (www.forcont-services.de). Bei diesem Konzept werden vollständige Geschäftsprozesse zur Nutzung auf Mietbasis über das Internet angeboten. Der Service für das Vertragsmanagement unterstützt z. B. die zentrale Verwaltung beliebiger Verträge inkl. aller Informationen, um Inhalte, Termine und Fristen im Überblick zu behalten. Und mit der Personalakte können sämtliche Daten und Dokumente zu einem Mitarbeiter in einer Akte elektronisch gespeichert und verwaltet werden.

www.forcont.de

Fraunhofer SIT

Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) in München entwickelt maßgeschneiderte Lösungen, um die Manipulationssicherheit sowie Zuverlässigkeit von Systemen zu erhöhen, und um die vertrauliche Verarbeitung der Daten zu gewährleisten. Arbeitsschwerpunkte sind die Sicherheit Eingebetteter Systeme, Netz-Sicherheit sowie Cloud-Computing. Im Kompetenzbereich Cloud-Computing erarbeitet das SIT Lösungen für die Entwicklung, Härtung und den Betrieb sicherer und verlässlicher Cloud-Ökosysteme. Im SIT-Cloud-Testlabor werden kommerzielle und Open Source Produkte hinsichtlich ihrer Funktions-, Zuverlässigkeits- und Interoperabilitäts-Eigenschaften evaluiert.
www.sit.fraunhofer.de

FUJITSU

Fujitsu ist einer der führenden internationalen Anbieter von ITK-basierten Geschäftslösungen. Zu den Portfolio-Elementen zählt z.B. Infrastructure-as-a-Service. Für seine Infrastruktur- und Applikations-Angeboten aus der Cloud kann Fujitsu in Deutschland auf seine eigenen Rechenzentren im Land zurückgreifen – ein entscheidender Vorteil mit Blick auf die rechtlichen Vorgaben zur Datenhaltung. Für eine globale Verfügbarkeit sorgen Fujitsu-Rechenzentren rund um den Globus. Je nach Kundenanforderung bietet Fujitsu dabei komplette Cloud-Lösungen, den Aufbau einer Private Cloud oder Hybrid-Modelle. Fujitsu hat 170.000 Mitarbeiter und einen Jahresumsatz von 50 Mrd. US-Dollar (FY 2009).
http://de.fujitsu.com/

Google | Enterprise

Google Enterprise wurde 2002 gegründet, um Software, die in der Verbraucherwelt erfolgreich ist, der Nutzung im Geschäftsumfeld anzupassen. Für Unternehmen wurde Google Apps for Business entwickelt. Mit diesem Kommunikations-Tool bietet Google einen komplett anderen Weg, IT-Anwendungen wie E-Mail, Kalender, Video sowie Kollaborations-Tools wie Textverarbeitung, Tabellenkalkulations- oder Präsentationssoftware zu nutzen. Der Kunde zahlt nur für das, was er wirklich benötigt.
Mehr als drei Millionen Unternehmen und 30 Millionen Internetnutzer in über 100 Ländern und in mehr als 40 Sprachen setzen bereits Google Apps an ihrem Arbeitsplatz ein.
www.google/apps

Hewlett-Packard, das weltgrößte IT-Unternehmen, bietet ein umfassendes Cloud-Lösungs-Portfolio für Unternehmen und öffentliche Einrichtungen. Dieses umfasst Dienstleistungen, Infrastruktur und Software für den Aufbau einer Private Cloud beim Kunden, als auch standardisierte und modulare Public und Private Cloud Services, geliefert aus HPs Rechenzentren. Ein weiterer Schwerpunkt ist die Unterstützung kollaborativer Geschäftsprozesse in verteilten Lieferketten mithilfe von Cloud-Plattformen.
Die HP Utility Services sind modulare und standardisierte Public- und Private-Cloud-Lösungen (IaaS, PaaS und SaaS), die auf die individuellen Bedürfnisse des Kunden angepasst werden können.
www.hp.com/de/us

IBM gehört mit einem Umsatz von 95,8 Mrd. $ in 2009 zu den weltweit größten Anbietern von Informationstechnologie, B2B-Lösungen und Cloud Computing. Eine Vielzahl von Basistechnologien und Services, die als Grundlage für Cloud Computing dienen, wurden von IBM entwickelt und am Markt eingeführt (Grid Computing, Utility Computing, on demand Services). Aufbauend auf Erfahrungen in zukunftsorientierten IT-Projekten mit Kunden und Partnern wurde das IBM Smart Business Cloud-Portfolio entwickelt, das aus integrierten Hardware-, Software- und Service-Bausteinen besteht. Darüberhinaus können Kunden aber auch individuelle IBM Services zur Planung, zum Aufbau und zum Betrieb ihrer Private Clouds nutzen.
http://ibm.com/de/cloud/

ITENOS

Die ITENOS GmbH bietet eine flexiblere IT bei geringen Kosten und die Nutzung von Cloud Computing und Virtualisierung bei exzellenter Sicherheit - die IT-Lösung mit Zukunft: Mit den ITENOS Cloud Services passt sich die Kunden-IT jederzeit den individuellen Bedürfnissen an. Die Kunden nutzen neueste Technologien, Applikationen und Plattformen, ohne sich um den Betrieb kümmern zu müssen. Durch die Virtualisierung erhalten sie optimale Flexibilität und Skalierbarkeit zu exakt kalkulierbaren Kosten bei hoher Verfügbarkeit und Performance. Sollten spezielle Anforderungen an die Hardware bestehen, so bietet ITENOS auch dedizierte, physikalische Markenserver zur Miete an. Und zwar einschließlich Konfiguration, die exakt auf die Kundenanforderungen zugeschnitten ist.
www.itenos.de

KPMG ist ein weltweites Netzwerk rechtlich selbstständiger, nationaler Firmen mit 140.000 Mitarbeitern in 146 Ländern. Auch in Deutschland gehört KPMG zu den führenden Wirtschaftsprüfungs- und Beratungsunternehmen und ist mit über 8.500 Mitarbeitern an mehr als 20 Standorten präsent. Unsere Leistungen sind in die Geschäftsbereiche Audit, Tax und Advisory gegliedert. Für wesentliche Sektoren unserer Wirtschaft haben wir eine geschäftsbereichsübergreifende Branchenspezialisierung vorgenommen. Hier laufen die Erfahrungen unserer Spezialisten weltweit zusammen und tragen zusätzlich zur Beratungsqualität bei.
www.kpmg.de

MATERNA
Information & Communications

MATERNA bietet ihren Kunden Beratung und Technologien rund um das Thema Cloud. Dies beginnt beim Aufbau einer Service-orientierten IT-Organisation, beinhaltet alle Services zur optimalen Nutzung von Virtualisierung und Automatisierung und reicht bis zum Aufbau der kompletten Cloud-Infrastruktur. Partnerschaften mit den führenden Technologieanbietern sowie eigene Produkte schaffen individuelle Lösungen für Unternehmen und Behörden jeder Art. Der Einsatz ausgereifter Technologien stellt zudem sicher, dass alle Investitionen langfristig geschützt sind. So gibt MATERNA ihren Kunden die Möglichkeit, Cloud-Computing als nachhaltige, strategische Art der Bereitstellung von IT-Services zu nutzen.
www.materna.de

Microsoft

Das Portfolio von Microsoft erstreckt sich von Betriebssystemen für PCs, mobile Endgeräte und Netzwerke über Serversoftware, Produktivitätssoftware für Unternehmen und private Nutzer, Multimedia-Anwendungen bis hin zu Entwickler-Tools. Neben Software für eine lokale Installation wie z.B. Windows 7, Internet Explorer, Microsoft Office, Exchange Server, Microsoft Dynamics CRM, bietet Microsoft umfangreiche Cloud Services, auf die Unternehmen und private Anwender über das Internet zugreifen. Das Angebot umfasst dabei alle Aspekte des Cloud Computing, von der Infrastruktur für die Entwicklung eigener Lösungen durch Microsoft-Kunden und Partner, über Komplettpakete zur Kommunikation und Zusammenarbeit bis hin zu leistungsfähigen Consumer-Diensten.
www.microsoft.de/cloud

NetApp
Go further, faster

Das Engagement für Einfachheit, Innovation und den Erfolg seiner Kunden ließ NetApp zu einem der am schnellsten wachsenden Storage- und Datenmanagement-Hersteller werden. Das breite Lösungsportfolio für Business-Applikationen, Storage für virtuelle Server, Disk-to-Disk Backup und mehr veranlassen Kunden weltweit sich für NetApp zu entscheiden. Sie erreichen mit NetApp die konstante Verfügbarkeit geschäftskritischer Daten und können Business-Prozesse vereinfachen. Im Vertrauen auf NetApp Lösungen sind Unternehmen in der Lage, neue Möglichkeiten umzusetzen, schneller denn je Einnahmen zu erzielen und die Kosten für den Schutz ihrer Daten, ihres Business und ihrer Reputation zu senken.
www.netapp.de

Novell

Novell, Inc. ermöglicht es Unternehmen, IT-Services sicher über klassische Client-Server, virtuelle und Cloud-basierte Umgebungen hinweg zu liefern und zu verwalten. Die Lösungen für Intelligent Workload Management umfassen Identity und Security, System Management, Collaboration sowie Linux-basierte Plattformen. Novells Lösungen und ein umfassendes Partnernetzwerk verbinden heterogene IT-Umgebungen zu einer Einheit.
Novell Cloud Security Service bietet als einzige Lösung Provisionierung, Authentifizierung, Autorisierung und Unterstützung für Compliance-Vorgaben.
Novell Cloud Manager ermöglicht Kunden das Erstellen und sichere Verwalten von Cloud Umgebungen über alle führenden Plattformen hinweg.
www.novell.com/de-de/products/

ORACLE

Oracle ist der weltweit größte Anbieter kompletter, offener und integrierter Anwendungssoftware und Hardware-Systeme. 370.000 Kunden setzen in über 145 Ländern Produkte und Lösungen von Oracle ein. Oracle ist Technologieanbieter für alle Arten von Cloud Computing. Die weltweit erste integrierte Middleware Maschine - Oracle Exalogic Elastic Cloud - ist ein integriertes Hardware- und Software-System, das für den hochskalierbaren und unternehmenskritischen Einsatz entwickelt wurde. Durch die Unterstützung tausender Anwendungen mit den unterschiedlichsten Anforderungen an Sicherheit, Zuverlässigkeit und Leistung ist sie die ideale Plattform für alle Arten von Rechenzentren-Konsolidierungen.
www.oracle.de

PricewaterhouseCoopers ist in Deutschland mit 8.700 Mitarbeitern und einer Gesamtleistung von rund 1,33 Milliarden Euro eine der führenden Wirtschaftsprüfungs- und Beratungsgesellschaften. An 28 Standorten arbeiten Experten für nationale und internationale Mandanten jeder Größe. PwC bietet Dienstleistungen an in den Bereichen Wirtschaftsprüfung und prüfungsnahe Dienstleistungen (Assurance), Steuerberatung (Tax) sowie Beratung in den Bereichen Deals und Consulting (Advisory). Cloud Computing betrachten wir für Nutzer und Anbieter ganzheitlich mittels Einbeziehung strategischer, finanzieller, betrieblicher, steuerlicher, juristischer und Compliance-bezogener Aspekte.

www.pwc.de

SAP entwickelt als führender Anbieter von Unternehmenssoftware und drittgrößter unabhängiger Softwarelieferant der Welt maßgeschneiderte Unternehmenslösungen für mehr als 102.500 Kunden rund um den Globus. Seit mehr als 37 Jahren bürgt der Name SAP für Innovation, Erfolg und Kreativität. Unseren Erfolg verdanken wir der hohen Qualität unserer Produkte sowie der langjährigen Erfahrung und dem Know-how unserer mehr als 47.598 Mitarbeiter weltweit. Zum Cloud Computing Portfolio zählt bspw. SAP Business ByDesign. Die vollständig integrierte On-Demand-Lösung wurde speziell für wachstumsstarke mittelständische Unternehmen entwickelt.

www.sap.de

Siemens Enterprise Communications (SEN) ist ein führender Anbieter von End-to-End-Lösungen für die Unternehmenskommunikation. Offene, standardbasierte Architekturen führen Kommunikations- und Unternehmensanwendungen zusammen und ermöglichen so die nahtlose Zusammenarbeit im gesamten Unternehmen. Die hochskalierbare, virtualisierbare und mandantenfähige OpenScape UC Suite eignet sich sowohl für den Einsatz in Private Cloud Umgebungen, als auch für die Bereitstellung von Communication as a Service (CaaS) Diensten durch Service Provider über eine Public Cloud. Die OpenScape UC Suite ist hochflexibel und lässt sich aufgrund ihrer OpenSOA Architektur leicht in gehostete Cloud-Anwendungen wie SalesForce.com, SAP oder Google Apps integrieren.

www.siemens-enterprise.com/de/

Siemens IT Solutions and Services GmbH verfügt über langjährige Erfahrungen in Betrieb und Management von IT-Infrastrukturen und Lösungen und bietet ein umfassendes Cloud Computing Portfolio an. Dazu gehören neben Infrastructure, Platform und Software as a Service (IaaS, PaaS, SaaS) auch deren Integration in Hybrid Cloud-Lösungen und geschäftsspezifische Community Clouds für die Zusammenarbeit zwischen Geschäftspartnern. Ein weiterer Schwerpunkt des Angebots von Siemens IT Solutions and Services liegt im Cloud Computing Consulting, um Potenziale bei der Transformation hin zu Cloud Services zu identifizieren und Risiken und Schwachstellen zu minimieren.

www.siemens.com/cloud-computing

Die Software AG ist weltweit führend im Bereich Business Process Excellence. Seit mehr als 40 Jahren liefert sie Innovationen, angefangen bei Adabas, der ersten transaktionalen Hochleistungsdatenban, über die SOA-basierte Integrationsplattform webMethods bis hin zu ARIS , der Plattform zur Analyse von Geschäftsprozessen und der ARIS Community, einer der größten sozialen BPM-Plattformen weltweit. Diese kombiniert Werkzeuge für soziales Networking (ARISalign) mit intuitiven Werkzeugen für Design und Modellierung von Prozessen (ARIS Express). Die branchenführenden Marken ARIS, webMethods, Adabas, Natural und IDS Scheer Consulting fügen sich zu einem einzigartigen Portfolio zusammen.
www.softwareag.com

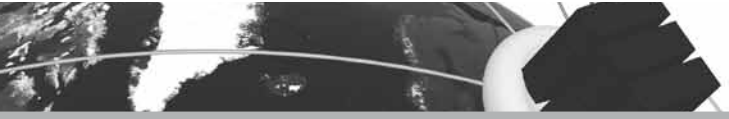
T-Systems ist die Großkundensparte der Deutschen Telekom. Mit einer weltumspannenden Infrastruktur aus Rechenzentren und Netzen betreibt das Unternehmen ICT-Technik für multinationale Konzerne und öffentliche Institutionen. Als viertgrößter Rechenzentrumsbetreiber der Welt ist T-Systems heute weltweit die Nummer 1, wenn es darum geht, SAP für Konzerne wie MAN und Linde nach Bedarf (Cloud Computing) bereitzustellen und abzurechnen. 2009 erzielte die Großkundensparte mit rund 45.300 Mitarbeitern einen Umsatz von rund 8,8 Mrd. Euro.
www.t-systems.de

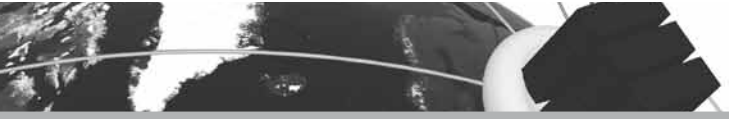
visionapp gehört zu den weltweit führenden Anbietern von Private und Public Cloud Computing-Lösungen sowie intelligenten „Software as a Service“-Plattformen und Automatisierungssoftware. as aus der Allianz-Gruppe im Jahr 2006 heraus gelöste Unternehmen vermarktet seine Plattform-Technologie über ein Netzwerk von hoch qualifizierten Partnern und unterstützt die Konzeption und Implementierung von Cloud Computing-Architekturen mit eigenen Services. Die Lösungen werden unterstützt durch strategische Partnerschaften mit Microsoft, Citrix, VMware und weiteren Herstellern. Über 15.000 Kunden - vom kleinen Handwerksbetrieb bis zum multinationalen Finanzdienstleister - nutzen bereits Produkte und Services der visionapp AG.
www.visionapp.de

VMware, der weltweit führende Anbieter für Cloud-Infrastrukturen, liefert bewährte Virtualisierungslösungen, die die Komplexität der IT-Landschaft deutlich verringern. VMware beschleunigt den Übergang von Unternehmen zum Cloud Computing bei vollem Schutz für getätigte IT-Investitionen. Dabei ermöglicht VMware effizientere, flexiblere Servicebereitstellung ohne Kompromisse bei der Kontrolle eingehen zu müssen. Firmen verlassen sich auf VMware, seine Partnerunternehmen und seine branchenführende Plattform für die virtuelle Infrastruktur. Im Jahr 2009 erzielte VMware Umsätzen von 2 Mrd. US-Dollar und verfügte weltweit über 170.000 Kunden und 25.000 Partnerunternehmen.
www.vmware.com/de/solutions/cloud-computing/

Vodafone Deutschland ist mit 13.000 Mitarbeitern und rund neun Mrd. Euro Umsatz einer der größten und modernsten Telekommunikationsanbieter in Europa. Als innovativer und integrierter Technologie- und Dienstleistungskonzern steht Vodafone Deutschland für Kommunikation aus einer Hand: Mobilfunk und Festnetz sowie Internet und Breitband-Datendienste für Geschäfts- und Privatkunden. Kontinuierliche Entwicklungen, zahlreiche Patente sowie Investitionen in neue Produkte, Services und das moderne Netz haben Vodafone zum Innovationsführer im deutschen Telekommunikationsmarkt werden lassen. 2010 wurde Vodafone von der Fachzeitschrift „connect“ erneut für das beste Sprach- und Datennetz in Deutschland ausgezeichnet.

www.vodafone-deutschland.de





Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.350 Unternehmen, davon über 1.000 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik 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