Opinion Paper

# Wer klaut in der Cloud?

Chancen und Risiken des Cloud Computings

2010 / 07

Consulting
DETECON

We make ICT strategies work

# Inhaltsverzeichnis

1 Executive Summary ..... 4
2 Cloud Computing – Einführung ..... 5
2.1 Charakteristiken von Cloud Computing ..... 5
2.2 Servicemodelle des Cloud Computings ..... 6
2.3 Einsatzvarianten von Cloud Computing ..... 7
2.4 Treiber geschäftlicher Innovationen ..... 7
2.5 Marktpotenzial ..... 8
2.6 Kritischer Erfolgsfaktor: Sicherheit ..... 9
3 Cloud Computing – Chancen für die IT-Sicherheit ..... 11
3.1 Skaleneffekte ..... 11
3.2 Standardisierung ..... 11
3.3 Skalierbarkeit ..... 12
3.4 Patch Management ..... 12
4 Cloud Computing – Risiken für die IT-Sicherheit ..... 13
4.1 Risikoverteilung im Cloud Computing ..... 13
4.2 Technologie ..... 14
4.2.1 Hypervisor-Sicherheit ..... 14
4.2.2 Netzwerksegmentierung und Trennung von Datenverkehr ..... 15
4.2.3 Management Interface ..... 16
4.2.4 Distributed Denial of Service (DDoS) ..... 17
4.2.5 Fehlender Secure Software Development Life Cycle (SSDLC) Support ..... 18
4.2.6 Nutzerauthentisierung, Rollen- und Rechteverwaltung ..... 19
4.3 Compliance ..... 19
4.3.1 Datenlokation ..... 20
4.3.2 Nachforschungen ..... 21
4.4 Lock-In ..... 22
4.4.1 Daten- und Code-Portabilität ..... 22
4.4.2 Proprietäre Entwicklungstools und Application Programming Interfaces (APIs) ..... 23
4.5 Finanzen ..... 24
4.5.1 Economic Denial of Service (EDoS) ..... 24
4.5.2 Zukunftsfähigkeit des Providers ..... 25

4.6 IT-Governance ..... 26
4.6.1 Kontrollverlust ..... 26
4.6.2 Skalierbarkeit ..... 27
5 Sicheres Cloud Computing umsetzen ..... 28
6 Lektüreempfehlungen ..... 29
7 Die Autoren ..... 30
8 Das Unternehmen ..... 31

# 1 Executive Summary

Cloud Computing bietet die Möglichkeit, Anforderungen an die IT kostengünstiger zu erfüllen und ist deshalb für Unternehmensvorstände, v. a. CIOs, von besonderem Interesse. IT-Anforderungen werden von der IT-Infrastruktur entkoppelt, was zu einer erheblichen Flexibilisierung beiträgt und durch die Bereitstellung für mehrere Nutzer einen erheblichen Effizienzgewinn nach sich zieht. Die bei Cloud Computing üblichen nutzungsbasierten Abrechnungsmodelle versprechen aus Sicht des Nutzers zusätzliche Kosten-optimierungspotenziale. Die Zukunft von Cloud Computing scheint rosig. Wachstumsraten für die nächsten Jahre jenseits der 30 Prozent erscheinen als realistisch. So prognostizieren Analysten, dass im Jahr 2020 mehr als ein Drittel der digitalen Informationen direkt oder indirekt mit Cloud-Services oder -Infrastrukturen verarbeitet werden.[1]

Cloud Computing bietet erhebliche Chancen, auch für die IT-Sicherheit. So kann sich die IT-Sicherheit u. a. die Skaleneffekte, weitreichende Standardisierungsbestrebungen und hohe Skalierbarkeit im Cloud Computing zu Nutzen machen. Kleinere und mittelgroße Betriebe können durch die Konzentration auf das Kerngeschäft und die Auslagerung von IT-Aufgaben an einen erfahrenen Dienstleister in besonderem Maße profitieren.

Trotz aller Vorteile und positiver Signale existieren durchaus kritische Stimmen zu Cloud Computing. So kristallisiert sich heraus, dass für den Erfolg und die Akzeptanz von Cloud Computing das Thema Sicherheit und der Umgang mit den für Cloud Computing spezifischen Risiken entscheidend ist. Die Bewertung der bedeutendsten Risiken im Cloud Computing zeigt, dass alle Risiken mindestens eine mittlere Wahrscheinlichkeit oder Schadenshöhe aufweisen und somit ein signifikantes Gesamtrisiko darstellen. Gerade Risiken wie die z. T. nicht mögliche Festschreibung der Datenlokation oder die nicht ausreichende Trennung des Datenverkehrs verschiedener Nutzer wiegen dabei besonders schwer. Auch Themen wie mangelhafte Daten- und Codeportabilität oder der Kontrollverlust der Daten sind von besonderer Bedeutung.

Die Auseinandersetzung mit Risiken wie den oben genannten und die Planung entsprechend geeigneter Maßnahmen zur Reduzierung dieser Risiken ist wichtig und muss bereits in einer frühen Planungsphase berücksichtigt werden. In einem weiteren Schritt ist ein Kriterienkatalog zu erarbeiten, der auch Sicherheitsanforderungen und Schutzziele berücksichtigt und bei der Auswahl möglicher Cloud Provider hilft. Die Sicherheitsanforderungen fließen schließlich auch in die Vertragsverhandlungen mit potenziellen Cloud Providern ein und sind Basis für die Erstellung von Sicherheitskonzepten in der Migrationsphase. Nur so kann der sichere Betrieb eines Cloud Computing-Dienstes gewährleistet werden.

[1] IDC: Digital Universe, 2010

# 2 Cloud Computing – Einführung

Unter Cloud Computing wird eine bedarfsgerechte und flexible Bereitstellung von IT-Ressourcen verstanden, deren tatsächliche Nutzung abgerechnet wird.

Zunächst werden im Folgenden Grundlagen für ein Verständnis von Cloud Computing beschrieben. Das National Institute of Standards and Technology (NIST) kategorisiert Cloud Computing-Dienste anhand von Charakteristiken, Servicemodellen sowie Einsatzvarianten (vgl. Kapitel 2.1 bis 2.3). Möglichkeiten, mit Hilfe von Cloud Computing Business Innovation voranzutreiben, veranschaulicht Kapitel 2.4. Das Marktpotenzial von Cloud Computing sowie seine Bedeutung für Unternehmen ist Gegenstand von Kapitel 2.5.

Um einen langfristigen Erfolg von Cloud Computing sicherzustellen, ist die Betrachtung kritischer Erfolgsfaktoren, allen voran das Thema Sicherheit, besonders bedeutsam. Diese werden in Kapitel 2.6 thematisiert.

## 2.1 Charakteristiken von Cloud Computing

- **On-Demand Self-Service:** Ein Kunde kann selbstständig und vollautomatisch Rechenressourcen, wie Rechenleistung oder Netzwerkspeicher, Anwendungen, Upgrades etc. abrufen und buchen, ohne dass hierzu eine Interaktion mit dem Service Provider nötig ist.
- **Broad Network Access:** Sämtliche Ressourcen sind breitbandig über das Internet oder Intranet angebunden. Der Zugriff erfolgt über Standardmechanismen, die eine Nutzung von Cloud-basierten Diensten mittels herkömmlicher Server oder auch Endgeräte wie PCs, Laptops, PDAs oder Smartphones ermöglichen.
- **Resource Pooling:** Die Rechenressourcen des Providers werden an einer Stelle gebündelt und mehreren Nutzern zur Verfügung gestellt.
- **Rapid Elasticity:** Ressourcen können in Echtzeit schnell und teilweise automatisiert auf die veränderten Bedürfnisse des Nutzers angepasst werden. Aus der Sicht der Nutzer stehen unbeschränkt Ressourcen zur Verfügung, die jederzeit und in jedem Umfang gekauft bzw. genutzt werden können.
- **Measured Service:** Cloud Computing Systeme kontrollieren und optimieren die Zuteilung von Ressourcen vollautomatisiert. Der Ressourcenverbrauch wird kontinuierlich gemessen, kontrolliert und berichtet, um Transparenz für den Provider und den Kunden herzustellen. Nur die genutzten Dienste und Ressourcen werden abgerechnet.

## 2.2 Servicemodelle des Cloud Computings

Im Cloud Computing existiert eine Klassifizierung der Services in drei unterschiedliche Modelle:

- **Infrastructure as a Service (IaaS):** Bei IaaS werden grundlegende Infrastrukturleistungen zur Verfügung gestellt (z. B. Rechenleistung, Speicherplatz), auf deren Basis der Nutzer individuelle Software wie Betriebssysteme oder Anwendungsprogramme betreiben kann. Der Nutzer ist nicht für das Management oder die Wartung der Infrastruktur zuständig, hat aber dennoch die Kontrolle über Betriebssysteme, Speicherverwaltung und Anwendungen. Auf die Konfiguration bestimmter Infrastrukturkomponenten, wie bspw. Host-Firewalls, hat er evtl. eine beschränkte Einflussmöglichkeit.
- **Platform as a Service (PaaS):** Nutzer können auf Basis einer Cloud-Plattform Anwendungen entwickeln oder bereitstellen. Dazu werden entsprechende Frameworks und Entwicklungswerkzeuge zur Verfügung gestellt. Dabei hat der Nutzer die Kontrolle über die Anwendungen und individuelle Konfigurationsparameter der Bereitstellungsumgebung.
- **Software as a Service (SaaS):** Bei SaaS wird dem Nutzer eine Anwendung als Dienst zur Verfügung gestellt. Die Änderung nutzerspezifischer Konfigurationseinstellungen ist evtl. nur eingeschränkt durch den Nutzer möglich.

Je nach Cloud Computing-Servicemodell ist von unterschiedlichen Sicherheitsphilosophien auszugehen. Infrastruktur-Provider (IaaS) bieten Sicherheitsfeatures lediglich auf Hardware- bzw. Infrastrukturebene an, z.B. mittels geeigneter Maßnahmen gemäß BSI-Grundschutz, und garantieren somit eine Basissicherheit und -verfügbarkeit. Für das Management und die Umsetzung der darüber hinausgehenden Sicherheitsmaßnahmen ist der Kunde verantwortlich. Bei PaaS verantwortet der Anbieter i. d. R. Plattformdienste, wie z. B. Datenbanken und Middleware. SaaS Provider regeln Details der Applikationsnutzung vertraglich, beispielsweise geltende Service Level, Sicherheit und Compliance (Abbildung 1).

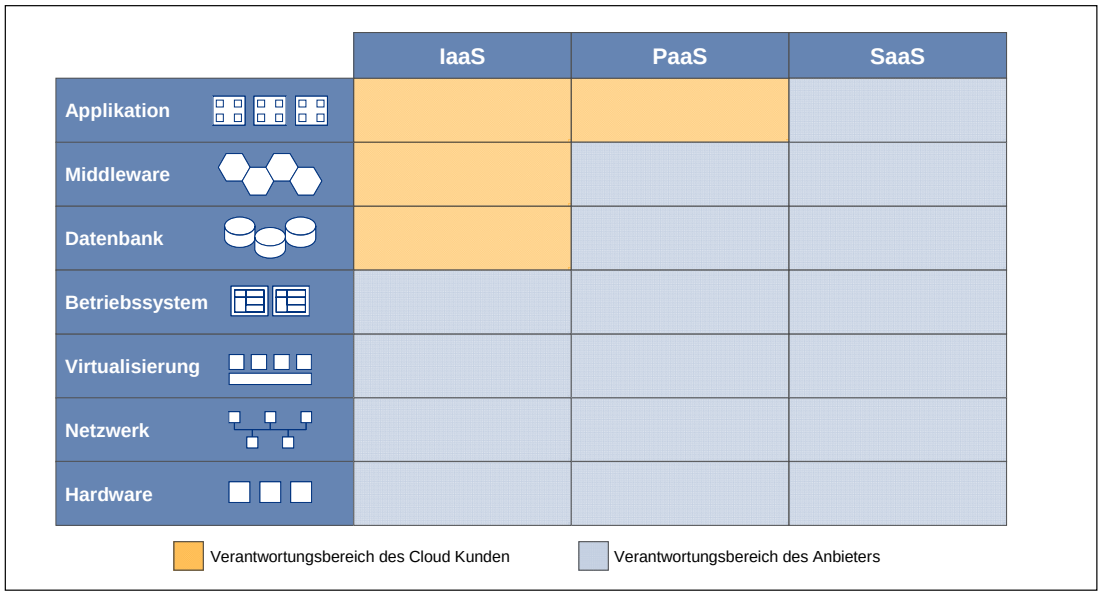


Abbildung 1: Cloud Computing Servicemodelle

## 2.3 Einsatzvarianten von Cloud Computing

In der Praxis sind vier grundsätzliche Einsatzvarianten für Cloud Computing zu unterscheiden. In einer Public Cloud-Umgebung sind Risiken tendenziell häufiger vorhanden, in einer Privaten Cloud-Umgebung gibt es weniger Risiken.

- **Public Cloud**: Die Cloud-Infrastruktur ist öffentlich zugänglich und wird von einem IT-Dienstleister betrieben. In der Regel wird dieser Service von einer sehr großen Nutzeranzahl in Anspruch genommen, wodurch sich entsprechende Skaleneffekte erzielen lassen. Durch die hohe Anzahl der Nutzer ist eine Individualisierung der Dienste und eine maßgeschneiderte Anpassung hier am wenigsten möglich.
- **Private Cloud**: Die Cloud-Infrastruktur wird für eine einzelne Organisation betrieben, die ausschließlichen Zugriff auf die Cloud hat. Sie kann die Infrastruktur selbst oder durch Dritte betreiben lassen. Skaleneffekte und Kosteneinsparungen werden reduziert, aus Sicht der Organisation nimmt die Kontrolle über die Cloud zu.
- **Community Cloud**: Im Rahmen einer Community Cloud wird die Cloud-Infrastruktur gemeinsam von mehreren Organisationen genutzt, die ähnliche Interessen bzw. Ziele verfolgen. Das Management der Infrastruktur erfolgt durch die Organisationen selbst oder extern durch einen Dritten.
- **Hybrid Cloud**: Die hybride Variante einer Cloud-Infrastruktur ist eine Mischung zweier oder mehrerer Varianten. Dabei bleiben die unterschiedlichen Clouds eigenständige Einheiten, die jedoch mit standardisierter oder proprietärer Technologie miteinander verbunden werden. So wird die Daten- bzw. Anwendungsportabilität sichergestellt. Mittels einer Hybrid Cloud können die Vorteile mehrerer Varianten kombiniert und Kostenvorteile von Public Clouds mit Sicherheitsvorteilen von Private Clouds kombiniert werden. Allerdings ist hierbei auch eine strikte und somit oftmals kostspielige Trennung der Daten notwendig.

## 2.4 Treiber geschäftlicher Innovationen

Cloud Computing vereint verschiedene grundlegende Verbesserungspotenziale und hat sowohl auf Seite des Anbieters, als auch auf Seite des Nutzers das Potenzial zu geschäftlichen Innovationen.

Es ist zum heutigen Zeitpunkt abzusehen, dass Cloud Computing die Erbringung von Dienstleistungen in der Informationswirtschaft nachhaltig verändern wird. Noch befindet sich Cloud Computing in der frühen Phase der Marktdurchdringung. Mittel- bis langfristig wird jedoch ein erheblicher Anteil traditioneller IT-Dienstleistungen durch Cloud-basierte Services ersetzt werden.

Cloud Computing bietet grundlegend die folgenden Verbesserungspotentiale:

- Kosten für IT-Infrastruktur und -Dienste können durch eine hohe Standardisierung der IT-Erbringung reduziert werden.
- Die Kostenstruktur verändert sich: Aus Investitionskosten werden Betriebskosten.
- Durch eine nutzungsabhängige Verrechnung können Budgets variabler genutzt werden.
- Neue Geschäftsprozesse lassen sich schneller und flexibler umsetzen. Die Reorganisation eines Unternehmens, z. B. im Rahmen von Mergers und Acquisitions, wird erleichtert.
- Die Fachbereiche im Unternehmen erhalten mehr Verantwortung für die Prozessunterstützung durch IT.

## 2.5 Marktpotenzial

Für das Jahr 2008 berechneten Analysten ein Marktvolumen (international) von 46 Mrd. US-Dollar. Bis 2013 wird mit einem Anstieg des Marktvolumens für Cloud Computing auf bis zu 150 Mrd. US-Dollar gerechnet. Dies entspricht einer jährlichen Wachstumsrate von mehr als 26 Prozent.[2]

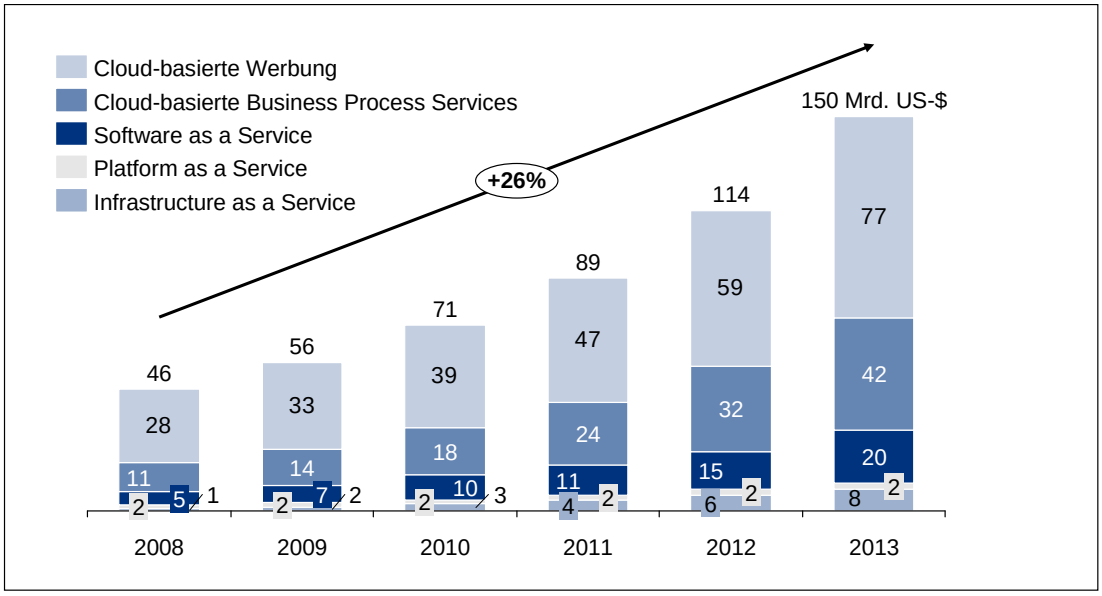


Abbildung 2: Marktentwicklung Cloud Computing 2008 - 2013 (international)

Laut Gartner[3] teilte sich das internationale Marktvolumen aus 2010 (71 Mrd. US-Dollar) wie folgt auf:

- 54,9 Prozent entfielen auf Cloud-basierte Werbung,
- 25,4 Prozent entfielen auf Cloud-basierte Business Process Services, z. B. E-Commerce, Human Resources und Personalabrechnung,
- 14,1 Prozent auf Software as a Service (SaaS),
- 2,8 Prozent entfielen auf Platform as a Service (PaaS) und
- 4,2 Prozent entfielen auf Infrastructure as a Service (IaaS).

Auch für den deutschen Markt wird eine positive Marktentwicklung prognostiziert. Sieben Prozent aller deutschen Unternehmen mit über 100 Mitarbeitern nutzen bereits Cloud Computing.[3] Für 2008 wurde der Umsatz mit SaaS in Deutschland mit 380 Mio. Euro beziffert.[4] Für den B2B-Bereich wurde ein Umatz für 2008 von 222 Mio. Euro, für 2009 von

[2] Gartner: Forecast: Sizing the Cloud; Understanding the Opportunities in Cloud Services, 2009; IDC: Cloud Computing Shaping the Next 20 Years of IT, 2008 bestätigt diesen Trend.

[3] IDC: Cloud Computing und Services – Status quo und Trends in Deutschland, 2009

[4] Experton Group: Software as a Service - Marktzahlen Deutschland 2009 – 2011, 2009

285 Mio. Euro, für 2010 von 388 Mio. Euro und für 2011 von 564 Mio. Euro geschätzt. Diese Entwicklung entspricht einer jährlichen Wachstumsrate von 36,5 Prozent.[5] Der deutsche Markt verzeichnet mit einem jährlichen Wachstum von 36,5% eine höhere jährliche Wachstumsrate als der Weltmarkt. Ein Grund dafür ist die anfängliche Zurückhaltung im Cloud Computing Umfeld und der dadurch entstandene Nachholbedarf in der deutschen Industrie.

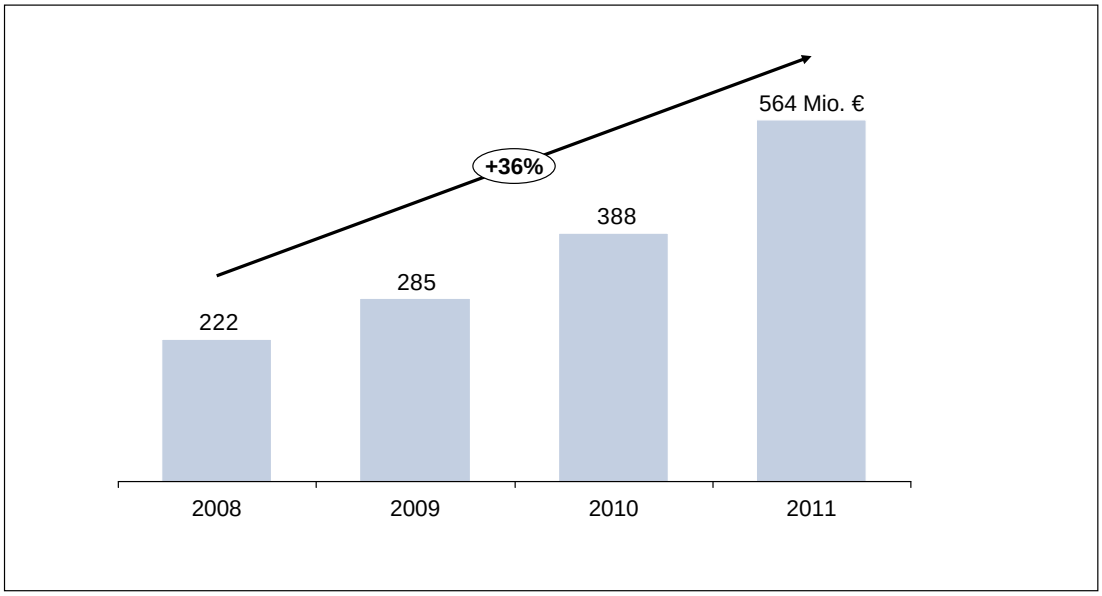


**Abbildung 3: Marktentwicklung Cloud Computing 2008 - 2011 (Deutschland)**

Obwohl die prognostizierten Umsätze für Cloud Computing sich unterscheiden, sprechen dennoch alle Quellen von zweistelligen jährlichen Wachstumsraten, teilweise jenseits der 30 Prozent. Cloud Computing verspricht damit das begehrteste Segment des ITK-Marktes der nächsten Jahre zu werden.

## 2.6 Kritischer Erfolgsfaktor: Sicherheit

Trotz aller Potenziale ist für den Erfolg und die Akzeptanz von Cloud Computing der Umgang mit kritischen Erfolgsfaktoren entscheidend. So stehen CIOs momentan Cloud Computing noch abwartend gegenüber. Umfragen verdeutlichen, dass „Sicherheit“ zurzeit die Achillesferse des Cloud Computings ist.

[5] BITKOM: Leitfaden - Cloud Computing - Evolution in der Technik, Revolution im Business, 2009

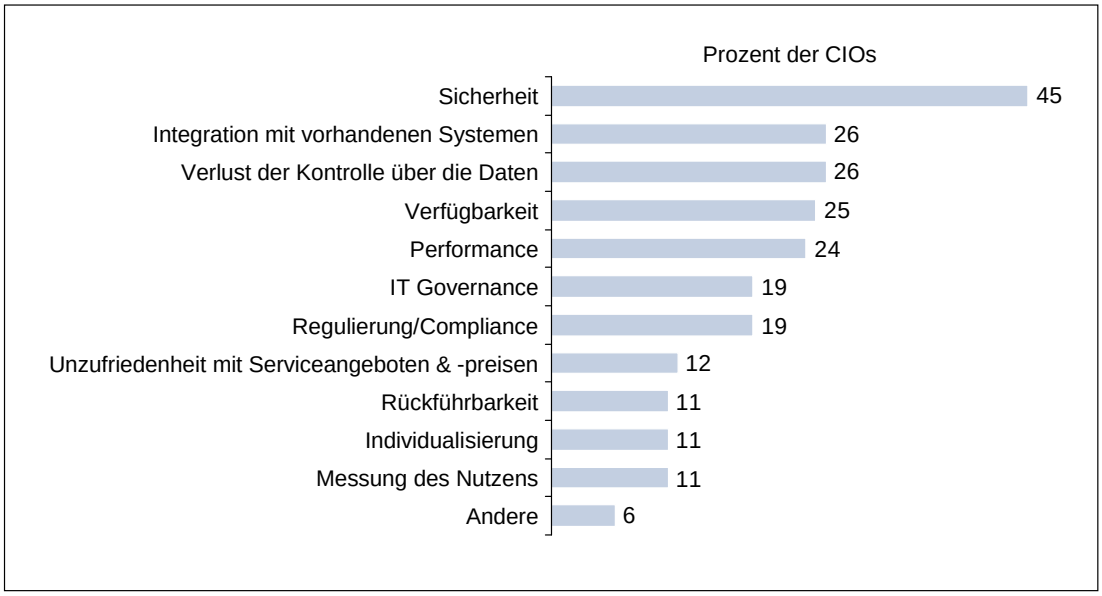


**Abbildung 4: Erfolgsfaktoren von Cloud Computing aus CIO-Sicht**[6]

45 Prozent der befragten CIOs nennen Sicherheit als kritischen Erfolgsfaktor für Cloud Computing (siehe Abbildung 4). 26 Prozent befürchten einen Verlust der Kontrolle über die Daten und monieren eine mangelnde Integrationsfähigkeit mit vorhandenen Systemen. Weitere Erfolgsfaktoren sind Verfügbarkeit, Performance, IT Governance und Compliance.

Kontrollverlust und/oder mangelnde/eingeschränkte Verfügbarkeit der Daten beeinträchtigen in der klassischen Sichtweise die IT-Sicherheit; daher sind auch diese Faktoren für den zukünftigen Erfolg von Cloud Computing-Diensten entscheidend.

Trotz der zunehmenden Popularität wird die Sicherheit von Diensten und Daten von Cloud Computing Anwendern stiefmütterlich behandelt. Nach einer aktuellen Studie des Ponemon Institute[7] unterzieht nicht einmal jedes zehnte Unternehmen den in Anspruch genommenen Cloud-Service einer ernsthaften Prüfung oder schult Mitarbeiter im Hinblick auf erhöhte Gefährdungen. So fehlt es den meisten Unternehmen laut der Studie an Prozessen, Richtlinien und Werkzeugen, um die Sicherheit ihrer sensiblen Daten in einer Cloud-Umgebung zu gewährleisten. Die Ergebnisse zeigen, dass viele Unternehmen im Hinblick auf die Sicherheitsaspekte gleichsam „im Blindflug“ in Cloud-Umgebungen steuern und damit potenziell ihren Betrieb, die eigenen Daten und die Daten ihrer Kunden gefährden.

[6] CIO Research: Cloud Computing Survey: IT leaders see big promises, have big security questions, 2009

[7] Ponemon Institute: Security of Cloud Computing Users - A Study of Practitioners in the US & Europe, 2010

# 3 Cloud Computing – Chancen für die IT-Sicherheit

Die Nutzung von Ressourcen durch mehrere Parteien, wie im Cloud Computing üblich, führt zwangsläufig zu neuen potenziellen Sicherheitsschwachstellen. Allerdings besteht durch die Zentralisierung auch die Chance, die IT-Sicherheit der Services zu erhöhen, z. B. durch Standardisierung von IT-Prozessen und spezialisiertes Fachwissen.

Bei kleineren und mittleren Betrieben ist durch die Konzentration auf das Kerngeschäft und das Auslagern von IT-Aufgaben an große, erfahrene Dienstleister mit einem tendenziell höheren Sicherheitsniveau zu rechnen.

Die vielfältigen Chancen, die Cloud Computing-Dienste Anbietern und Nutzern bieten, sind in den folgenden Abschnitten zusammengefasst.

## 3.1 Skaleneffekte

| **Definition** |
|---|
| Die Kosten für Sicherheitsmaßnahmen steigen nicht proportional zur Implementierungsgröße. Grund hierfür sind Skaleneffekte. Bei Sicherheitsmaßnahmen spielen Skaleneffekte eine bedeutende Rolle, da einmalig implementierte Sicherheitsmaßnahmen für eine große Anzahl von Systemen bzw. Services genutzt werden können. |
| **Chancen durch Cloud Computing** |
| Ein Cloud Provider kann durch die Vielzahl seiner Kunden auf der gleichen Infrastruktur Sicherheit erheblich günstiger anbieten, als einzelne Kunden individuell mit entsprechenden eigenen Maßnahmen. Aus der Sicht des Kunden sinken die Kosten für IT-Sicherheit oder es wird bei gleichbleibenden Kosten ein höheres Sicherheitsniveau erreicht. |

## 3.2 Standardisierung

| **Definition** |
|---|
| Eine Vielzahl von IT-Services unterhalten Schnittstellen zur Kommunikation mit anderen Services. Sind diese Schnittstellen standardisiert, fällt ein Wechsel des Anbieters besonders leicht, da keine langwierigen und damit kostspieligen Anpassungsmaßnahmen vorgenommen werden müssen. |
| **Chancen durch Cloud Computing** |
| Cloud Provider können ihren Kunden standardisierte, offene Schnittstellen und somit die Managed Security Services anbieten. Die Kunden profitieren von einer größeren Flexibilität bei der Wahl des Providers für Sicherheitsdienstleistungen. Dies setzt jedoch definierte, standardisierte Schnittstellen voraus, die von der Industrie zu etablieren sind. |

## 3.3 Skalierbarkeit

| Definition |
| --- |
| Aus der Sicht des Kunden wird unter Skalierbarkeit die Anpassbarkeit von Betriebsmitteln an die (wechselnden) Leistungsanforderungen der Anwendung, explizit auch in Zeiten mit einer höheren Auslastung, verstanden. Diese erhöhten Anforderungen ergeben sich z. B. bei Handelsplattformen zur Weihnachtszeit oder bei Finanzanwendungen zum Ende des Fiskaljahres. Reaktions- und Ansprechverhalten der Services sollen auch in diesen Fällen wie gewohnt bestehen. Dies bedeutet, dass die Qualität des zu erbringenden Services unabhängig von der zu bewältigenden Last sein muss. |
| **Chancen durch Cloud Computing** |
| Cloud Computing ermöglicht die dynamische Ressourcenallokation. Ressourcen werden im Bedarfsfall schnell und flexibel neu verteilt, um die Verfügbarkeit zu gewährleisten. Somit werden bspw. bei Angriffen Ressourcen gezielt umverteilt und dadurch potenzielle negative Auswirkungen auf die Verfügbarkeit des Services minimiert. |

## 3.4 Patch Management

| Definition |
| --- |
| Patch Management ist die Planung und Installation von Patches, sowohl auf Betriebssystem-, als auch auf höheren Abstraktionsebenen. Wichtig sind insbesondere Patches, die Sicherheitsschwachstellen adressieren. Beim Patch Management ist es von zentraler Bedeutung, dass Patches über die gesamte Infrastruktur hinweg ganzheitlich und regelmäßig eingespielt werden, da sonst Lücken von Angreifern sehr schnell ausgenutzt werden können. |
| **Chancen durch Cloud Computing** |
| Virtuelle Maschinen werden von Infrastruktur-Anbietern (IaaS) bereitgestellt und können in einem standardisierten Prozess mit aktuellen Aktualisierungen und Patches versorgt werden. Im Gegensatz zu Client-basierten Systemen können standardisierte Cloud-Plattformen einen erheblich höheren Effizienzgrad erreichen und Bereitstellungszeiten minimieren. Dies gilt ebenfalls für höhere Abstraktionsebenen, wie beispielsweise für Middleware bei PaaS oder Softwareupdates bei SaaS. Es ist möglich, dass wenige hochqualifizierte Spezialisten notwendige sicherheitsrelevante Patches auf verschiedenen Systemebenen zentral planen und einspielen und damit effizient für sichere Softwarestände sorgen. Dies steht im Gegensatz zum sukzessiven Planen und Aufspielen bei einzelnen Systemen und den damit einhergehenden meist erheblichen Ausfallzeiten. |

# 4 Cloud Computing – Risiken für die IT-Sicherheit

Im Vergleich zu den Chancen sind die Risiken im Cloud Computing im Allgemeinen vielfältiger, allerdings auch oftmals genauer spezifizierbar. Risiken können in den folgenden übergeordneten Domänen auftreten: Technologie, Compliance, Lock-In, Finanzen und IT-Governance. Diesen Domänen werden die bedeutendsten Sicherheitsrisiken im Kontext von Cloud Computing zugeordnet.[8] Die Sicherheitsrisiken werden strukturiert analysiert und bewertet. Hierzu werden die Risiken definiert und abgegrenzt. Cloud-Spezifika stellen klar, warum dieses Risiko speziell für Cloud Computing relevant ist. Darüber hinaus werden Maßnahmen formuliert, die Risiken reduzieren. Des Weiteren erfolgt eine Zuordnung zu den in Kapitel 2.2 eingeführten Servicemodellen und die Bewertung der Relevanz in den Einsatzvarianten von Cloud Computing (vgl. Kapitel 2.3).

Das Risiko wird daraufhin den drei Komponenten der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) zugeordnet. Schließlich werden die Wahrscheinlichkeit des Eintritts des Risikos und die potenzielle Schadenshöhe bewertet (niedrig, mittel, hoch). Es erfolgt zudem ein Vergleich mit traditioneller IT (niedriger, gleich, höher). Aus der Wahrscheinlichkeit und der Schadenshöhe ergibt sich die Einstufung des Gesamtrisikos.

## 4.1 Risikoverteilung im Cloud Computing

Abbildung 5 zeigt die Risikoverteilung im Cloud Computing nach Eintrittswahrscheinlichkeit und möglicher Schadenshöhe. Die einzelnen Risiken werden in den Kapiteln 4.2 bis 4.6 im Detail analysiert und bewertet.

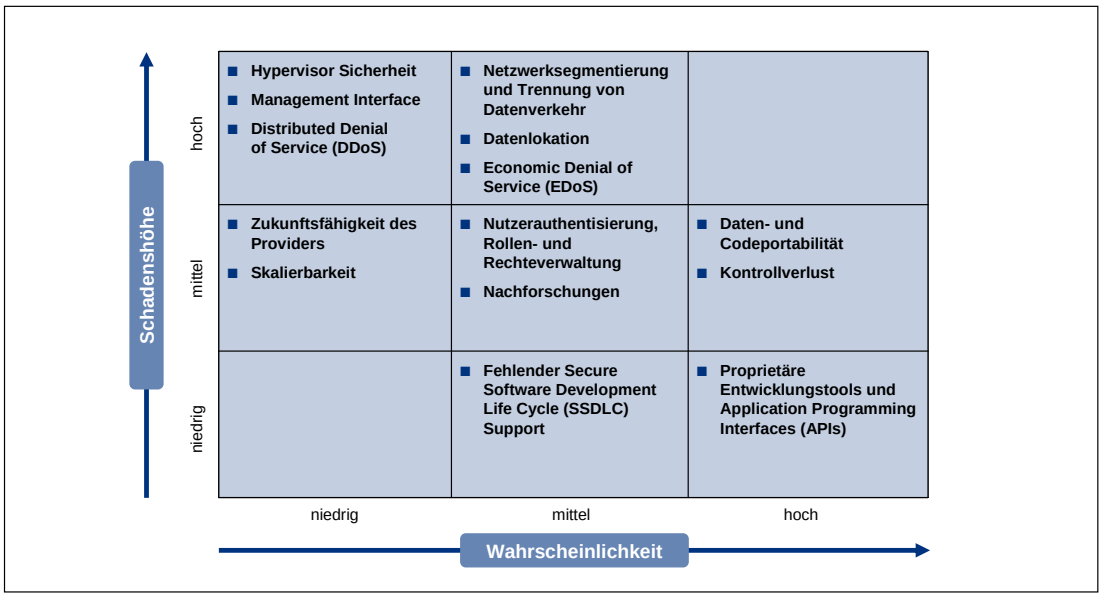


**Abbildung 5: Risikoverteilung im Cloud Computing nach Eintrittswahrscheinlichkeit und möglicher Schadenshöhe**

[8] Wenn mehrere Domänen in Frage kommen, wird das Risiko der Domäne mit der höchsten Relevanz zugeordnet.

Es zeigt sich, dass alle betrachteten Risiken mindestens eine mittlere Wahrscheinlichkeit oder Schadenshöhe aufweisen und somit ein signifikantes Gesamtrisiko darstellen. Aus diesem Grund sind die Risiken bereits im Vorfeld eines geplanten Cloud Computing-Vorhabens zu berücksichtigen.

## 4.2 Technologie

IT-Sicherheit umfasst allgemein die Sicherheit von technischen und logischen Systemen der Informations- und Kommunikationstechnologie. Hier werden speziell Risiken untersucht, die sich aus den dem Cloud Computing zugrunde liegenden Technologien ergeben. Um definierte Schutzziele bei der IT-gestützten Verarbeitung von Informationen einzuhalten, müssen geeignete betriebliche und technische Maßnahmen getroffen werden.

### 4.2.1 Hypervisor-Sicherheit

| **Definition** | | | | | |
|---|---|---|---|---|---|
| In einer virtualisierten Umgebung ist der Hypervisor der Bereitstellungsmechanismus, d.h. der Software-Teil, der die virtualisierte Hardware für die darauf betriebenen virtuellen Maschinen (VMs) bereitstellt. Es ist denkbar, dass eine VM auf Speicherbereiche des Hypervisors oder auf den Speicherbereich anderer VMs zugreift und die Vertraulichkeit der Daten gefährdet. Ein Angriff kann aufgrund von Besonderheiten in der Systemarchitektur, fehlender Isolation der VMs voneinander sowie durch Fehler im Design und in der Implementierung der VM-Software ermöglicht werden. | | | | | |
| **Cloud-Spezifika** | | | | | |
| In Cloud-Umgebungen sind Schwachstellen in der Hypervisor-Software sehr kritisch zu bewerten. Wenn mehrere VMs verschiedener Kunden auf dem Hypervisor laufen, kann ein Angreifer eine bösartige VM starten, die die Sicherheitslücken der VM-Software ausnutzt. Der Zugriff auf den Speicherbereich anderer VMs, die Störung des Dienstes oder sogar die Übernahme des Hypervisors sind denkbar. | | | | | |
| **Maßnahmen** | | | | | |
| Es sind ausreichende Kenntnisse über die Virtualisierungsinfrastruktur und deren verfügbare Sicherheitsmechanismen, sowie der Einsatz von sicheren Hypervisoren und die Durchführung geeigneter Härtungsmaßnahmen notwendig. | | | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | | | |
| IaaS | ☑ | PaaS | ☐ | SaaS | ☐ |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | | | |
| Private Cloud | ◔ | Community Cloud | ◑ | Hybrid Cloud | ● |
| Public Cloud | ● | | | | |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | | | |
| Vertraulichkeit | ☑ | Integrität | ☑ | Verfügbarkeit | ☐ |
| **Wahrscheinlichkeit** | | | | **Vergleich zu traditioneller IT** | |
| niedrig | | | | höher | |
| **Schadenshöhe** | | | | **Vergleich zu traditioneller IT** | |
| hoch | | | | höher | |
| **Einstufung Gesamtrisiko** | | | | | |
| mittel | | | | | |

### 4.2.2 Netzwerksegmentierung und Trennung von Datenverkehr

| **Definition** | | | |
|---|---|---|---|
| Die Segmentierung eines Netzes ist eine Strategie, um IT-Dienste, Server und/oder Applikationen entsprechend ihren Sicherheitsanforderungen in einer Netzwerkzone zu platzieren. Traditionell erfolgt diese Segmentierung durch physikalische Netzwerk-komponenten wie Switches, Router und Firewalls. | | | |
| **Cloud-Spezifika** | | | |
| In einer Cloud Computing-Umgebung wird die Segmentierung logisch in der Virtualisierungsumgebung konfiguriert. Durch Softwareschwachstellen oder operative Fehler (fehlerhafte Konfiguration) kann es möglich sein, diese Mechanismen zu umgehen und somit die Segmentierung, die Systeme mit unterschiedlichen Sicherheitsanforderungen voneinander trennt, zu umgehen. | | | |
| **Maßnahmen** | | | |
| Der Einsatz von physischen Geräten, z.B. Switches und Firewalls, ist sinnvoll, besonders wenn die Geräte als Begrenzung einer Netzwerkzone eingesetzt werden. Zur Trennung des Netzwerkverkehrs verschiedener Kunden oder zur Segmentierung von Systemen mit verschiedenen Sicherheits-anforderungen wird der Einsatz der VLAN (Virtual Local Area Network) Technologie empfohlen. | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | |
| IaaS ☑ | PaaS ☐ | SaaS ☐ | |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | |
| Private Cloud ◑ | Community Cloud ◑ | Hybrid Cloud ● | Public Cloud ● |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | |
| Vertraulichkeit ☑ | Integrität ☐ | Verfügbarkeit ☐ | |
| **Wahrscheinlichkeit** | | **Vergleich zu traditioneller IT** | |
| mittel | | höher | |
| **Schadenshöhe** | | **Vergleich zu traditioneller IT** | |
| hoch | | höher | |
| **Einstufung Gesamtrisiko** | | | |
| mittel bis hoch | | | |

### 4.2.3 Management Interface

| **Definition** | | | | | | | |
|---|---|---|---|---|---|---|---|
| Eine wichtige Komponente eines Cloud Computing Providers sind die Schnittstellen zur Verwaltung der Betriebsmittel, das Management Interface. Mit dessen Hilfe werden Maschinen-Instanzen u. a. verwaltet, gestartet, gestoppt und erzeugt, sowie die Fernwartung der Virtualisierungsumgebung ermöglicht | | | | | | | |
| **Cloud-Spezifika** | | | | | | | |
| Die notwendigen Skaleneffekte eines Cloud Providers können nur durch einen sehr effizienten IT Management-Prozess erreicht werden. Aus diesem Grund muss die Administration der virtuellen Server per Fernzugriff auf die Virtualisierungsschicht durchgeführt werden. Eine größere Anzahl an Personen hat Zugriff auf die virtuellen Maschinen und die zugehörigen Netze, so dass das Risiko des unautorisierten Zugriffs signifikant höher als in traditionellen IT-Umgebungen ist. | | | | | | | |
| **Maßnahmen** | | | | | | | |
| In einer Cloud-Umgebung sollen administrativer und produktiver Datenverkehr voneinander getrennt, der Zugang zum Management Interface beschränkt und streng kontrolliert werden. Der Zugriff von virtuellen Maschinen aus darf nicht möglich sein. Die Verwendung von starken Authentisierungsverfahren und sicheren Protokollen (SSHv2, HTTPS) für den Zugriff auf das Management Interface wird empfohlen. | | | | | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | | | | | |
| IaaS | ☑ | PaaS | ☑ | SaaS | ☑ | | |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | | | | | |
| Private Cloud | ◑ | Community Cloud | ◑ | Hybrid Cloud | ● | Public Cloud | ● |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | | | | | |
| Vertraulichkeit | ☑ | Integrität | ☑ | Verfügbarkeit | ☑ | | |
| **Wahrscheinlichkeit** | | | | **Vergleich zu traditioneller IT** | | | |
| niedrig | | | | höher | | | |
| **Schadenshöhe** | | | | **Vergleich zu traditioneller IT** | | | |
| hoch | | | | höher | | | |
| **Einstufung Gesamtrisiko** | | | | | | | |
| mittel | | | | | | | |

### 4.2.4 Distributed Denial of Service (DDoS)

| **Definition** | | | | | |
|---|---|---|---|---|---|
| Eine Distributed Denial of Service (DDoS) Attacke tritt auf, wenn mehrere Systeme durch einen gemeinsamen Angriff gezielt die Ressourcen eines Zielsystems blockieren und damit die Verfügbarkeit negativ beeinflussen. Symptomatisch sinkt hierdurch die Ausführungsgeschwindigkeit des Zielsystems bis hin zur völligen Nichtverfügbarkeit. | | | | | |
| **Cloud-Spezifika** | | | | | |
| Wird durch eine DDoS Attacke der Zugang zum Dienst in der Cloud behindert oder aber der Dienst selbst blockiert, ist eine Nutzung des Dienstes nicht mehr möglich. Die Verbindung zwischen Kunde und Cloud Provider ist hierbei häufig eine Schwachstelle ("Single Point of Failure"). | | | | | |
| **Maßnahmen** | | | | | |
| Die Verfügbarkeit kann am wirkungsvollsten durch eine Redundanz erhöht werden. Eine zweite Anbindung an das Internet erhöht die Verfügbarkeit signifikant. Eine Nutzung der Dienste mehrerer Cloud Provider schafft zusätzliche Redundanz, falls ein Provider nicht erreichbar ist. Prinzipiell sind auch die klassischen Maßnahmen der DDoS-Mitigation anzuwenden.[9] Wie in Kapitel 3.3 betrachtet, bietet Cloud Computing auch dadurch Vorteile, dass Ressourcen dynamisch skalieren und zur Sicherstellung der Verfügbarkeit gezielt an andere Stellen der Cloud umverteilt werden können. | | | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | | | |
| IaaS | ☑ | PaaS | ☑ | SaaS | ☑ |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | | | |
| Private Cloud | ◑ | Community Cloud | ◑ | Hybrid Cloud | ● | Public Cloud | ● |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | | | |
| Vertraulichkeit | ☐ | Integrität | ☐ | Verfügbarkeit | ☑ |
| **Wahrscheinlichkeit** | | **Vergleich zu traditioneller IT** | | | |
| niedrig | | niedriger bis gleich | | | |
| **Schadenshöhe** | | **Vergleich zu traditioneller IT** | | | |
| hoch | | gleich | | | |
| **Einstufung Gesamtrisiko** | | | | | |
| mittel | | | | | |

[9] siehe z. B. RFC 4732, http://tools.ietf.org/html/rfc4732

### 4.2.5 Fehlender Secure Software Development Life Cycle (SSDLC) Support

| **Definition** | | | |
|---|---|---|---|
| Die Software- und Systementwicklung findet häufig gemäß des Software Development Life Cycle (SDLC)-Prozesses statt. Die Entwicklung gemäß des Secure Software Development Life Cycle (SSDLC)-Prozesses berücksichtigt das Thema Sicherheit nicht erst nach, sondern schon während der Entwicklungsphase. So werden durch Schwachstellen verursachte aufwändige und kostenintensive Änderungen der Software oder gar der Softwarearchitektur im Nachhinein vermieden und die Integrität der Software sichergestellt. | | | |
| **Cloud-Spezifika** | | | |
| Die Entwicklung von Software und Systemen ist zentraler Bestandteil zahlreicher PaaS- Angebote. Der SSDLC-Ansatz ist relativ neu und wird noch nicht von allen Anbietern unterstützt. Der Verzicht auf die Entwicklung von Software und Systemen gemäß SSDLC führt zu potenziell unsicherer Software, die nach der Entwicklung angepasst und ergänzt werden muss, so dass sie den Sicherheitsanforderungen genügt. Da die Entwicklungsschritte nicht integriert und parallelisiert ablaufen, ist mit einer längeren Entwicklungsdauer und somit höheren Kosten zu rechnen. | | | |
| **Maßnahmen** | | | |
| Wird keine SSDLC-Unterstützung angeboten, muss die Umsetzung geforderter Sicherheits-maßnahmen während oder nach der Entwicklungsphase sichergestellt werden. Ein Provider, der die Entwicklung gemäß SSDLC unterstützt, ist bei der Auswahl u. U. zu bevorzugen. | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | |
| IaaS ☐ | PaaS ☑ | SaaS ☐ | |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | |
| Private Cloud ● | Community Cloud ● | Hybrid Cloud ● | Public Cloud ● |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | |
| Vertraulichkeit ☑ | Integrität ☑ | Verfügbarkeit ☐ | |
| **Wahrscheinlichkeit** | | **Vergleich zu traditioneller IT** | |
| mittel | | gleich | |
| **Schadenshöhe** | | **Vergleich zu traditioneller IT** | |
| niedrig | | gleich | |
| **Einstufung Gesamtrisiko** | | | |
| niedrig bis mittel | | | |

### 4.2.6 Nutzerauthentisierung, Rollen- und Rechteverwaltung

| **Definition** | | | | | | | |
|---|---|---|---|---|---|---|---|
| Die Authentisierung der Nutzer und die Möglichkeit der Vergabe verschiedener Rollen und Rechte sind für den sicheren Betrieb und zur Gewährleistung der Vertraulichkeit und Integrität eines Cloud-Dienstes unerlässlich. | | | | | | | |
| **Cloud-Spezifika** | | | | | | | |
| Ein Cloud Computing-Dienst wird i. d. R. von verschiedenen Nutzern mit unterschiedlichen Rollen und Rechten genutzt. Der Zugang zu den Ressourcen darf nur authentisierten Nutzern ermöglicht werden. | | | | | | | |
| **Maßnahmen** | | | | | | | |
| Der Cloud Computing-Anbieter muss Authentisierungsdienste sowie ein Rollen- und Rechtemodell unterstützen. Abhängig von der Rolle und den Rechten des Nutzers erhält dieser einen mehr oder weniger beschränkten Zugriff auf den Dienst. Darüber hinaus müssen von einer entsprechenden Plattform Funktionalitäten für die Rollen-, Rechte- und Benutzerverwaltung und die Definition einer Passwort-Richtlinie (Policy) zur Verfügung gestellt werden. Diese administrativen Funktionalitäten stehen nur besonderen Nutzern mit erweiterten Rechten zur Verfügung. | | | | | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | | | | | |
| IaaS | ☑ | PaaS | ☑ | SaaS | ☑ | | |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | | | | | |
| Private Cloud | ● | Community Cloud | ● | Hybrid Cloud | ● | Public Cloud | ● |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | | | | | |
| Vertraulichkeit | ☑ | Integrität | ☑ | Verfügbarkeit | ☐ | | |
| **Wahrscheinlichkeit** | | | | **Vergleich zu traditioneller IT** | | | |
| mittel | | | | höher | | | |
| **Schadenshöhe** | | | | **Vergleich zu traditioneller IT** | | | |
| niedrig | | | | gleich | | | |
| **Einstufung Gesamtrisiko** | | | | | | | |
| mittel | | | | | | | |

## 4.3 Compliance

Unter Compliance wird in diesem Zusammenhang der Einklang von Cloud Computing mit regulatorischen und rechtlichen Rahmenbedingungen verstanden. Aufgrund der Verteilung von Daten und Anwendungen, teilweise über nationale Grenzen hinweg, ist es notwendig, die Einhaltung der geltenden gesetzlichen Rahmenbedingungen sicherzustellen und diese in wiederkehrenden Intervallen zu überprüfen.

Die Herausforderungen der Compliance in einer Cloud-Umgebung konzentrieren sich auf den Datenschutz, Gesetze (Finanzen) und Regulierungen, z. B. Health Insurance Portability and Accountability Act (HIPAA), sowie branchenspezifische Standards, wie z. B. Payment Card Industry Data Security Standard. Datenschutz, vor allem im internationalen Umfeld, ist ein komplexes Thema, da jedes Land seine eigenen Datenschutzrichtlinien besitzt, die für die jeweils lokalen Datenzentren gelten.

Konformität mit regulatorischen Rahmenbedingungen wird in den meisten Fällen durch Audits nachgewiesen, die in der Regel durch externe Dritte vorgenommen werden. Audits in einer Cloud-Umgebung sind allerdings nicht einfach durchzuführen, u. a. auch wegen des Mangels an Standards zwischen verschiedenen Anbietern.

Die durch den Anbieter eingesetzten Sicherheitsmaßnahmen sind der Schlüssel zur Einhaltung der gesetzlichen Anforderungen und dienen der nachweisbaren Erfüllung der Informationspflichten gegenüber Wirtschaftsprüfern, Gesellschaftern und zuständigen Behörden (z.B. Bankenaufsicht, FTC, SEC). Die Nachweisbarkeit der Sicherheitsmaßnahmen wird durch Standards wie ISO 27001 und 27002, sowie den SAS 70 Reports (insbesondere Type II Reports) unterstützt.

### 4.3.1 Datenlokation

| **Definition** | | | | | |
|---|---|---|---|---|---|
| Unter der Datenlokation versteht man den geografischen Ort, an dem die Daten gespeichert werden, sowie die Zuordnung der Daten zu einer bestimmten geografischen Region. Die Lokation der Daten ist oftmals durch Regularien vorgegeben. Besonders für die EU gelten hier besondere Vorschriften, so dass Daten in bestimmten Fällen zwingend innerhalb der EU gespeichert werden müssen. In bestimmten Ländern, wie z. B. Frankreich, ist eine Speicherung von Finanzdaten sogar nur im eigenen Land erlaubt, so dass die Infrastruktur des Cloud Providers zwingend im jeweiligen Land vorhanden sein muss. Allerdings ist auch für gesetzliche Auflagen die Frage der Datenlokation von größter Bedeutung, da in manchen Ländern Behörden im Rahmen geheimdienstlicher Recherchen sehr einfach Zugriff auf Daten erlangen können, was gerade bei streng vertraulichen Daten ein sehr hohes Risiko darstellt. | | | | | |
| **Cloud-Spezifika** | | | | | |
| Viele Cloud Provider betreiben weltweit verteilt Rechenzentren und Cloud Computing-Ressourcen. Nicht alle Provider garantieren, dass Daten innerhalb einer bestimmten geografischen Lokation gespeichert werden. Die Einschränkung auf geografische Teilbereiche der Cloud würde gewissermaßen auch dem Grundgedanken des Cloud Computing widersprechen. | | | | | |
| **Maßnahmen** | | | | | |
| Sollten für Daten entsprechende Regularien gelten oder will man vor der Verbreitung der Daten in andere Länder aus Geschäftssicht Abstand nehmen, ist dies bereits bei der Auswahl des Cloud Providers zu berücksichtigen. Der Provider muss in diesem Fall vertraglich verpflichtet werden, die Daten nur in festgelegten geografischen Regionen zu speichern. Um sicherzustellen, dass für relevante Daten entsprechende Maßnahmen umgesetzt werden können, müssen die Daten klassifiziert werden. | | | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | | | |
| IaaS | ☑ | PaaS | ☑ | SaaS | ☑ |

| Relevanz in den Cloud Computing Einsatzvarianten | | | |
|---|---|---|---|
| Private Cloud ◑ | Community Cloud ● | Hybrid Cloud ● | Public Cloud ● |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | |
| Vertraulichkeit ☑ | Integrität ☑ | Verfügbarkeit ☑ | |
| **Wahrscheinlichkeit** | **Vergleich zu traditioneller IT** | | |
| mittel | höher | | |
| **Schadenshöhe** | **Vergleich zu traditioneller IT** | | |
| hoch | höher | | |
| **Einstufung Gesamtrisiko** | | | |
| mittel bis hoch | | | |

### 4.3.2 Nachforschungen

| Definition |
|---|
| Es ist sicherzustellen, dass Daten zur Verfolgung von illegalen oder unsachgemäßen Aktivitäten zur Verfügung stehen und einwandfrei rekonstruiert werden können. Hierzu gehören nicht nur die Daten an sich, sondern ebenfalls weitere Meta-Daten wie Log-Dateien, die die Bearbeitungen und Wege der Daten nachvollziehbar machen und eindeutig aufzeigen. |
| **Cloud-Spezifika** |
| Als Hürde erweist sich der Umstand, dass Daten verteilt auf mehreren Servern, in mehreren Rechenzentren, im Extremfall sogar in unterschiedlichen Ländern mit eigenen Jurisdiktionen liegen (siehe auch Kapitel 4.3.1). |
| **Maßnahmen** |
| Es muss mit dem Cloud Provider vertraglich vereinbart werden, entsprechende Nachforschungsmöglichkeiten sicherzustellen. Hier ist besonders darauf zu achten, dass der genaue Inhalt der Nachforschungsmöglichkeiten, z.B. die Aufbewahrungsdauer der Daten, a priori exakt per Dienstgütevereinbarung (SLA) festgelegt wird. |

| Zuordnung zu den Cloud Computing Servicemodellen | | | |
|---|---|---|---|
| IaaS ☑ | PaaS ☑ | SaaS ☑ | |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | |
| Private Cloud ◑ | Community Cloud ● | Hybrid Cloud ● | Public Cloud ● |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | |
| Vertraulichkeit ☑ | Integrität ☑ | Verfügbarkeit ☑ | |
| **Wahrscheinlichkeit** | **Vergleich zu traditioneller IT** | | |
| mittel | höher | | |
| **Schadenshöhe** | **Vergleich zu traditioneller IT** | | |
| mittel | höher | | |
| **Einstufung Gesamtrisiko** | | | |
| mittel | | | |

## 4.4 Lock-In

Unter Lock-In versteht man die gezielte Bindung eines Kunden an ein Unternehmen, um den Wechsel zu einem Mitbewerber zu erschweren. Der Wechsel zu einem Konkurrenten wird i. d. R. vom Kunden nur vollzogen, wenn die Vorteile den mit dem Wechsel verbundenen Aufwand übersteigen.

### 4.4.1 Daten- und Code-Portabilität

<table>
<tr><th colspan="4">Definition</th></tr>
<tr><td colspan="4">Daten und Quellcode sollten im Idealfall vollständig portabel sein, d. h. problemlos zwischen verschiedenen Providern oder zurück in das eigene Unternehmen portiert werden können.</td></tr>
<tr><th colspan="4">Cloud-Spezifika</th></tr>
<tr><td colspan="4">Bei Cloud Computing-Angeboten wird ein umfassender Teil einer IT-Dienstleistung durch einen einzelnen Anbieter erbracht. Momentan fehlen im Umfeld von Cloud Computing noch Standards, Schnittstellen und Protokolle, die einen einfachen Wechsel von einem Cloud Provider zu einem anderen oder die Re-Migration ins eigene Unternehmen ermöglichen. Dies verursacht hohe Migrationskosten und kann zu einer ungewollten Bindung an den Anbieter führen.</td></tr>
<tr><th colspan="4">Maßnahmen</th></tr>
<tr><td colspan="4">Vor einer Migration ist festzulegen, welche Prozesse und Standards eingesetzt werden. Bei der Bewertung eines Cloud Providers sind sowohl technische als auch ökonomische Dimensionen zu berücksichtigen, um den Aufwand einer Migration bzw. Rückführung in das eigene Unternehmen zu bewerten. Eine Strategie besteht darin, den Dienst von unterschiedlichen Cloud Providern zu beziehen. Des Weiteren bietet sich die vertragliche Vereinbarung der Datenherausgabe durch den Anbieter, sowie u. U. die Nutzung von spezialisierten Daten- und Quellcodetreuhändern an.</td></tr>
<tr><th colspan="4">Zuordnung zu den Cloud Computing Servicemodellen</th></tr>
<tr><td>IaaS ☑</td><td>PaaS ☑</td><td colspan="2">SaaS ☑</td></tr>
<tr><th colspan="4">Relevanz in den Cloud Computing Einsatzvarianten</th></tr>
<tr><td>Private Cloud ◔</td><td>Community Cloud ◑</td><td>Hybrid Cloud ◑</td><td>Public Cloud ●</td></tr>
<tr><th colspan="4">Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit</th></tr>
<tr><td>Vertraulichkeit ☐</td><td>Integrität ☐</td><td colspan="2">Verfügbarkeit ☑</td></tr>
<tr><th colspan="2">Wahrscheinlichkeit</th><th colspan="2">Vergleich zu traditioneller IT</th></tr>
<tr><td colspan="2">hoch</td><td colspan="2">höher</td></tr>
<tr><th colspan="2">Schadenshöhe</th><th colspan="2">Vergleich zu traditioneller IT</th></tr>
<tr><td colspan="2">mittel</td><td colspan="2">gleich</td></tr>
<tr><th colspan="4">Einstufung Gesamtrisiko</th></tr>
<tr><td colspan="4">mittel bis hoch</td></tr>
</table>

### 4.4.2 Proprietäre Entwicklungstools und Application Programming Interfaces (APIs)

| **Definition** | | | |
|---|---|---|---|
| Bei einem Plattform-Dienst werden dem Nutzer Entwicklungs-Frameworks, Middleware-Funktionalitäten sowie Datenbanken und APIs zur Verfügung gestellt. | | | |
| **Cloud-Spezifika** | | | |
| Die zur Verfügung gestellten Entwicklungswerkzeuge und APIs sind an die Cloud- Plattform angepasst. Um sie zu nutzen, ist auf Kundenseite das entsprechende Know-How aufzubauen. Somit verstärkt sich die Bindung an den Cloud Provider. | | | |
| **Maßnahmen** | | | |
| Es ist bereits im Vorfeld einer möglichen Nutzung eines PaaS Angebotes zu prüfen, welcher zeitliche und monetäre Aufwand für die Nutzung der proprietären Tools und APIs anfällt und wie stark die eingesetzten Verfahren von etablierten Standards abweichen. Je näher der Anbieter sich an Standards orientiert, offene Schnittstellen verwendet etc., desto geringer sind Aufwand und Bindung an den Anbieter. Die Entwicklung des Marktes und das Verhalten einzelner Anbieter hinsichtlich Standards, z. B. Open Virtualization Format (OVF), sind aufmerksam zu beobachten. | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | |
| IaaS ☐ | PaaS ☑ | SaaS ☐ | |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | |
| Private Cloud ● | Community Cloud ● | Hybrid Cloud ● | Public Cloud ● |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | |
| Vertraulichkeit ☐ | Integrität ☐ | Verfügbarkeit ☑ | |
| **Wahrscheinlichkeit** | **Vergleich zu traditioneller IT** | | |
| hoch | höher | | |
| **Schadenshöhe** | **Vergleich zu traditioneller IT** | | |
| niedrig | gleich | | |
| **Einstufung Gesamtrisiko** | | | |
| mittel | | | |

## 4.5 Finanzen

Unter finanziellen Risiken werden Risiken verstanden, die einen direkten finanziellen Schaden für das betroffene Unternehmen nach sich ziehen können.

### 4.5.1 Economic Denial of Service (EDoS)

| **Definition** | | | |
|---|---|---|---|
| Bei einer Economic Denial of Service (EDoS)-Attacke werden finanzielle Mittel eines Kunden missbräuchlich von Dritten verwendet. Durch die Verletzung der Vertraulichkeit entsteht dem Kunden ein finanzieller Schaden, im Extremfall bis hin zur Zahlungsunfähigkeit. | | | |
| **Cloud-Spezifika** | | | |
| Bei Cloud Computing-Geschäftsmodellen erfolgt die Abrechnung nach dem Pay-per-Use- Prinzip. Nach erfolgtem Identitätsdiebstahl kann ein Angreifer das Benutzerkonto sowie seine Ressourcen verwenden und ihm somit finanziellen Schaden zufügen. | | | |
| **Maßnahmen** | | | |
| Im einfachsten Fall sollten Sicherheitsmaßnahmen den Ressourcenverbrauch begrenzen. Hierfür sind sinnvolle Obergrenzen zu definieren, so dass auf der einen Seite der potenzielle finanzielle Schaden kalkulierbar bleibt, auf der anderen Seite aber auch die Nutzung des Dienstes nicht eingeschränkt wird. Des Weiteren sind sichere Verfahren der Nutzerauthentisierung einzusetzen. | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | |
| IaaS ☐ | PaaS ☑ | SaaS ☐ | |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | |
| Private Cloud ● | Community Cloud ● | Hybrid Cloud ● | Public Cloud ● |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | |
| Vertraulichkeit ☑ | Integrität ☐ | Verfügbarkeit ☐ | |
| **Wahrscheinlichkeit** | | **Vergleich zu traditioneller IT** | |
| mittel | | höher | |
| **Schadenshöhe** | | **Vergleich zu traditioneller IT** | |
| hoch | | gleich | |
| **Einstufung Gesamtrisiko** | | | |
| mittel bis hoch | | | |

### 4.5.2 Zukunftsfähigkeit des Providers

| **Definition** | | | | | |
|---|---|---|---|---|---|
| Durch die Auslagerung von Daten und Diensten in die Cloud wird dem Provider eine große Verantwortung übertragen, da meist geschäftskritische Daten oder Dienste betroffen sind. Würde der Provider Insolvenz anmelden oder von einem anderen Unternehmen übernommen werden, so besteht das Problem darin, beim Provider vorhandene Daten und Services zurück zu bekommen und diese wieder in das eigene Unternehmen zu integrieren. | | | | | |
| **Cloud-Spezifika** | | | | | |
| Das Risiko der Zukunftsfähigkeit ist natürlich nicht auf Cloud Computing-Anbieter beschränkt. Doch angesichts des neuen Geschäftmodells Cloud Computing und den damit fehlenden Erfahrungen über die Beständigkeit am Markt ist hier besondere Vorsicht angebracht. | | | | | |
| **Maßnahmen** | | | | | |
| Von zentraler Bedeutung ist es, dass der auszuwählende Provider ein auf längere Sicht robustes Geschäftsmodell vorweist. Es ist ratsam, mit dem Anbieter die Herausgabe von Daten, ggfs. sogar Quellcode, vertraglich zu vereinbaren. | | | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | | | |
| IaaS | ☑ | PaaS | ☑ | SaaS | ☑ |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | | | |
| Private Cloud | ◔ | Community Cloud | ◑ | Hybrid Cloud | ◑ | Public Cloud | ● |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | | | |
| Vertraulichkeit | ☐ | Integrität | ☐ | Verfügbarkeit | ☑ |
| **Wahrscheinlichkeit** | | **Vergleich zu traditioneller IT** | | | |
| niedrig | | höher | | | |
| **Schadenshöhe** | | **Vergleich zu traditioneller IT** | | | |
| mittel | | gleich | | | |
| **Einstufung Gesamtrisiko** | | | | | |
| niedrig bis mittel | | | | | |

## 4.6 IT-Governance

IT-Governance hat die Aufgabe, durch die Etablierung geeigneter Führungs- und Organisationsstrukturen sowie über Prozesse sicherzustellen, dass die IT die definierten Unternehmensziele und die Geschäftsstrategie unterstützt. Wesentliches Ziel von IT-Governance ist auch die Minimierung der IT-Risiken.

### 4.6.1 Kontrollverlust

<table>
<tr><th colspan="4">Definition</th></tr>
<tr><td colspan="4">Ein Kontrollverlust ist die Abgabe der Kontrollhoheit über einen oder mehrere Bereiche an einen externen Dritten. Der Nutzer gibt hierbei evtl. auch die Steuerung von Bereichen aus der Hand, die die Sicherheit betreffen.</td></tr>
<tr><th colspan="4">Cloud-Spezifika</th></tr>
<tr><td colspan="4">Bei der Nutzung von Cloud Computing wird immer auch Kontrolle vom Nutzer an den Cloud Provider abgegeben. Der Kontrollverlust kann sich z.B. auf Daten, Software oder Quellcode beziehen. Branchenspezifische Anforderungen an Sicherheitsüberprüfungen (Audits) sind unter Umständen nur sehr schwer zu erfüllen.</td></tr>
<tr><th colspan="4">Maßnahmen</th></tr>
<tr><td colspan="4">Es besteht die Möglichkeit, die Kontrolle nur für gewisse Bereiche an den Cloud Provider zu übertragen. Die sicherheitskritischen Bereiche bleiben beispielsweise unter eigener Kontrolle. Das Vertrauen in den Provider sollte mit Hilfe von SLA-Vereinbarungen gestärkt werden.</td></tr>
<tr><th colspan="4">Zuordnung zu den Cloud Computing Servicemodellen</th></tr>
<tr><td>IaaS ☑</td><td>PaaS ☑</td><td colspan="2">SaaS ☑</td></tr>
<tr><th colspan="4">Relevanz in den Cloud Computing Einsatzvarianten</th></tr>
<tr><td>Private Cloud ○</td><td>Community Cloud ◑</td><td>Hybrid Cloud ◑</td><td>Public Cloud ●</td></tr>
<tr><th colspan="4">Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit</th></tr>
<tr><td>Vertraulichkeit ☑</td><td>Integrität ☐</td><td colspan="2">Verfügbarkeit ☑</td></tr>
<tr><th colspan="2">Wahrscheinlichkeit</th><th colspan="2">Vergleich zu traditioneller IT</th></tr>
<tr><td colspan="2">hoch</td><td colspan="2">höher</td></tr>
<tr><th colspan="2">Schadenshöhe</th><th colspan="2">Vergleich zu traditioneller IT</th></tr>
<tr><td colspan="2">mittel</td><td colspan="2">höher</td></tr>
<tr><th colspan="4">Einstufung Gesamtrisiko</th></tr>
<tr><td colspan="4">mittel bis hoch</td></tr>
</table>

### 4.6.2 Skalierbarkeit

| **Definition** | | | | | | | |
|---|---|---|---|---|---|---|---|
| Unter Skalierbarkeit versteht man, dass Anwendungen und Systeme bei höherer Last, die gewünschte Leistung, z. B. in Form von Reaktions- und Bearbeitungszeiten, stabil erbringen. Dies bedeutet, dass die Qualität des zu erbringenden Dienstes unabhängig von der zu bewältigenden Last ist (vgl. Kapitel 3.3). | | | | | | | |
| **Cloud-Spezifika** | | | | | | | |
| Skalierbarkeit kann Chance und Risiko zugleich sein. Zwar verspricht das Cloud Computing-Modell - zumindest in der Theorie - eine generelle Skalierbarkeit. Doch es ist entscheidend, dass Cloud Provider genügend Ressourcen vorhalten, um auch extreme Lastspitzen abfangen und die Dienste durchgehend leistungsfähig anbieten zu können. Da die Ressourcen von mehreren Nutzern geteilt werden, können bei großer Homogenität der Nutzer Lastspitzen im schlechtesten Fall gleichzeitig auftreten und die Skalierbarkeit der Cloud-Infrastruktur an ihre Grenzen bringen. | | | | | | | |
| **Maßnahmen** | | | | | | | |
| Es sind entsprechende Dienstgütemerkmale (SLA) der Provider als Absicherung zu nutzen, um ein Interesse des Anbieters an einer genügend großen Ressourcendecke sicherzustellen. Darüber hinaus kann es sinnvoll sein, sich eine Übersicht über die Nutzer des Providers zu verschaffen. Bei vielen Kunden aus der gleichen Branche ist die Gefahr von Kapazitätsengpässen höher als bei einer sehr homogenen Nutzerbasis. | | | | | | | |
| **Zuordnung zu den Cloud Computing Servicemodellen** | | | | | | | |
| IaaS | ☑ | PaaS | ☑ | SaaS | ☑ | | |
| **Relevanz in den Cloud Computing Einsatzvarianten** | | | | | | | |
| Private Cloud | ● | Community Cloud | ● | Hybrid Cloud | ◑ | Public Cloud | ◑ |
| **Zuordnung zu Vertraulichkeit, Integrität und Verfügbarkeit** | | | | | | | |
| Vertraulichkeit | ☐ | Integrität | ☐ | Verfügbarkeit | ☑ | | |
| **Wahrscheinlichkeit** | | | | **Vergleich zu traditioneller IT** | | | |
| niedrig | | | | niedriger | | | |
| **Schadenshöhe** | | | | **Vergleich zu traditioneller IT** | | | |
| mittel | | | | gleich | | | |
| **Einstufung Gesamtrisiko** | | | | | | | |
| niedrig bis mittel | | | | | | | |

# 5 Sicheres Cloud Computing umsetzen

Sicherheit ist der am meisten genannte Erfolgsfaktor für Cloud Computing (vgl. Kapitel 2.6) und spielt deshalb bei der Umsetzung von Cloud Computing-Vorhaben eine zentrale Rolle. Ein entsprechendes Vorgehen umfasst im Allgemeinen vier Phasen: Planung, Verhandlung, Migration und Betrieb.

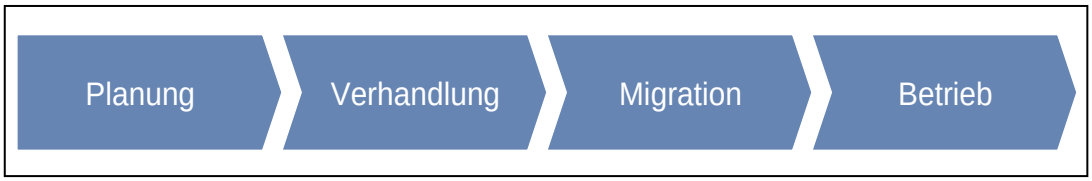


Abbildung 6: Vorgehen für sicheres Cloud Computing

In der **Planungsphase** entwickelt das Management eine Strategie, die vor allem vorgibt, für welche Geschäftsbereiche und -prozesse Cloud Computing grundsätzlich in Frage kommt sowie welche Risiken unbedingt zu vermeiden sind. Zudem werden in dieser Phase die Sicherheitsanforderungen definiert, die Schutzziele bestimmt, zu schützende Zielobjekte (Daten, Anwendungen etc.) identifiziert und Sicherheitsmaßnahmen erarbeitet. Anhand eines definierten Kriterienkatalogs werden die Einsatzvariante und darauf aufbauend mögliche Cloud Provider ausgewählt. Von Beginn an werden hierbei sämtliche Stakeholder wie der Datenschutzbeauftragte, der Sicherheitsbeauftragte, die Rechtsabteilung, die Fachabteilungen, der Betriebsrat etc. mit in die Planungen einbezogen. Des Weiteren wird auch die Beendigung des Cloud Computing-Betriebs bzw. der Wechsel zu einem anderen Provider geregelt. Hierbei ist vor allem zu klären, wie die Löschung und Übertragung der Daten gewährleistet wird.

Die Sicherheitsanforderungen fließen in die **Verhandlung** der Verträge mit ein. In diesem Rahmen werden Dienstgütevereinbarungen (SLA) und messbare Kennzahlen (KPI), die auch die Überwachung der Sicherheit ermöglichen, mit dem potenziellen Cloud Provider definiert. Weiterhin werden in den Verträgen Auditrechte festgeschrieben, die den Pflichten des Nutzers gegenüber seinen Kunden und Behörden gerecht werden.

Zu Beginn der **Migrationsphase** erstellen Provider und Nutzer gemeinsam auf Basis der Sicherheitsanforderungen die notwendigen Sicherheitskonzepte. Diese bilden die Grundlage für die eigentliche Umsetzung des Migrationsvorhabens und müssen ständig aktuell gehalten werden. Im Rahmen der Migration erfolgt die Übertragung der Kontrolle an den Cloud Provider und die Erbringung der Services. Außerdem werden die in der Planungsphase festgelegten organisatorischen und technischen Maßnahmen umgesetzt.

Für den sicheren **Betrieb** des Cloud Computing-Dienstes ist die Festlegung der Verantwortlichkeiten von entscheidender Bedeutung. Hierfür ist ein Sicherheitsbeauftragter zu benennen, der den Betrieb des Cloud-Dienstes verantwortet.

# 6 Lektüreempfehlungen


- BITKOM: Cloud Computing — Evolution in der Technik, Revolution im Business, 2009
- BSI: IT-Grundschutz und Cloud Computing, 2009
- Claus, Thorsten: Future of Cloud; DMR – The Magazine for Management and Technology, 2010
- CSA: Security Guidance for Critical Areas of Focus in Cloud Computing, Version V2.1, 2009
- Eikmeier, Christoph; Rieger, Volker; Weber, Erwin: Flexibilität aus der Wolke — Cloud Computing – die zukünftige Form der ICT; DMR — Das Magazin für Management und Technologie, 2009
- ENISA: Cloud Computing — Benefits, risks and recommendations for information security, 2009
- Jeske, Martin; Claus, Thorsten: Der Himmel reißt auf – Geteilte Märkte und differenzierte Geschäftsmodelle: Wie Cloud Computing erwachsen wird, DMR — Das Magazin für Management und Technologie, 2010
- Jeske, Martin; Pracht, Dirk: Stark bedeckt oder wolkenlos?; DMR — Das Magazin für Management und Technologie, 2010
- Kallerhoff, Philipp; Slamka, Christian: Sicherheit in grünen Wolken; digma — Zeitschrift für Datenrecht und Informationssicherheit, 2009
- Mather, Tim; Kumaraswamy, Subra; Latif, Shahed: Cloud Security and Privacy, 2009
- NIST: The NIST Definition of Cloud Computing, Version 15, 2009
- Ponemon Institute: Security of Cloud Computing Users - A Study of Practitioners in the US & Europe, 2010

# 7 Die Autoren

**Bernd Jaster** ist bei Detecon in Bonn als Consultant in der Competence Practice Information Technology tätig. In zahlreichen Projekten sammelte er Erfahrung in der Bewertung und Einführung von strategischen Technologien. Seine Themenschwerpunkte liegen in den Bereichen Cloud Computing und ICT Innovation Management.

Er ist erreichbar unter +49 228 700 1941 oder Bernd.Jaster@detecon.com

**Joao Collier de Mendonca** ist bei Detecon in Bonn in der ICT Risk and Security Management-Gruppe der Competence Practice Information Technology tätig. Sein Fokus liegt im Bereich Innovation für IT-Sicherheit. Er arbeitet überwiegend an multinationalen Projekten der IT-Sicherheit, der Compliance und des Datenschutzes.

Er ist erreichbar unter +49 228 700 1927 oder Joao.Mendonca@detecon.com

**Dr. Christian Slamka** ist bei Detecon im Schweizer Büro in Zürich im Security, IT Efficiency & IT Compliance -Team innerhalb des Information and Communication Technology-Bereichs tätig. Seine umfangreichen Erfahrungen sammelte der in Betriebswirtschaft promovierte Informatiker bisher vor allem in Projekten zu IT-Sicherheit und IT-Effizienz. Sein Themenschwerpunkt liegt im Cloud Computing.

Er ist erreichbar unter +41 79 6943488 oder Christian.Slamka@detecon.com

**Dr. Mike Radmacher** ist bei Detecon in Bonn in der Competence Practice Strategie und Marketing mit dem Schwerpunkt Product Innovation, tätig. In einer Vielzahl von Projekten sammelte er Erfahrungen in der Entwicklung innovativer Ideen, Konzepte und Produkte im ICT-Umfeld. Dazu gehörten neben der strategischen Portfolioentwicklung auch IT-Sicherheit und Identitätsmanagement. Nicht nur die reine Entwicklung der Konzepte, sondern ebenso die Begleitung bei deren Umsetzung stand dabei im Vordergrund.

Er ist erreichbar unter +49 170 9178317 oder Mike.Radmacher@detecon.com

# 8 Das Unternehmen

**We make ICT strategies work**

Detecon ist ein Beratungsunternehmen, das klassische Managementberatung mit einem hohen Technologieverständnis vereint.

Unsere Unternehmensgeschichte beweist dies: Detecon International ging aus der Fusion der 1954 gegründeten Management- und IT-Beratung Diebold und der 1977 gegründeten Telekommunikationsberatung Detecon hervor. Unser Leistungsschwerpunkt besteht demnach in Beratungs- und Umsetzungslösungen, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien, engl. Information and Communications Technology (ICT), ergeben. Weltweit profitieren Kunden aus nahezu allen Branchen von unserem ganzheitlichen Know-how in Fragen der Strategie und Organisationsgestaltung sowie beim Einsatz modernster Technologien.

Das Know-how der Detecon bündelt das Wissen aus erfolgreich abgeschlossenen Management- und ICT-Beratungsprojekten in über 160 Ländern. Wir sind global durch Tochter- und Beteiligungsgesellschaften sowie Projektbüros vertreten. Detecon ist ein Tochterunternehmen der T-Systems International, der Geschäftskundenmarke der Deutschen Telekom. Als Berater profitieren wir daher von der weltumspannenden Infrastruktur eines Global Players.

**Know-how und Do-how**

Die rasante Entwicklung von Informations- und Telekommunikationstechnologien beeinflusst in immer stärkerem Maße sowohl die Strategien von Unternehmen als auch die Abläufe innerhalb einer Organisation. Die daraus folgenden komplexen Anpassungen betreffen dementsprechend nicht nur technologische Anwendungen, sondern auch Geschäftsmodelle und Unternehmensstrukturen.

Unsere Dienstleistungen für das ICT-Management umfassen sowohl die klassische Strategie- und Organisationsberatung als auch die Planung und Umsetzung von hochkomplexen, technologischen ICT-Architekturen und -Anwendungen. Dabei agieren wir herstellerunabhängig und sind allein dem Erfolg des Kunden verpflichtet.

Detecon International GmbH
Oberkasselerstr. 2
53227 Bonn
Telefon: +49 228 700 0
E-Mail: info@detecon.com
Internet: www.detecon.com