
| | | |
|---|---|---|
| **Cloud Computing**<br>**Positionspapier 2016** | | **White Paper**<br>**CloudComp-Pos-1.1.3**<br>**Ergebnis der AG** |
| Kurzbeschreibung | Das vorliegende Positionspapier untersucht die Möglichkeiten des Einsatzes von Cloud Computing in der österreichischen öffentlichen Verwaltung. Das Positionspapier soll Grundlageninformationen für nötige strategische Entscheidungen bereit stellen bzw. wie man diese Entscheidungsgrundlagen erarbeitet und was man dabei beachten muss; es beinhaltet Begriffsdefinition, Marktsituation, rechtliche/strukturelle/wirtschaftliche/technische Aspekte (Geschäfts-prozesse), Auswirkungen, Chancen und Risiken sowie potentielle Anwendungen für klassische Rechenzentren, eine Private Cloud und Public Cloud als auch Beispiele und Prozesse für Migration. | |
| Autor(en): | Peter Reichstädter | Projektteam / Arbeitsgruppe:<br>AG-Cloud / BLSG |
| Beiträge von: | Reinhard Posch, Hanspeter Czermak, Mike Fandler, Christian Gebauer, Wolfgang Huber, Bernhard Karning, Thomas Kasa, Nicolas Knotzer, Roland Krenner, Jürgen Marek, Christian Panigl, Martin Petrak, Harald Pirker, Harald Reisinger, Alena Sirka-Bred, Günther Tschabuschnig, Klemens Urban, Norbert Weidinger, Gregor Schmied, Karin Luttenberger, Anna-Karina Hafner, Christian Schuller , Harald Stradal, Hannes Wittmann, Gregor Eibl | |

| | |
|---|---|
| Version 1.1.3 : **7.11.2016** | Zur Kenntnis: 4.4.2017 |

| | |
|---|---|
| Unter-Version ... : **TT.MM.JJJJ** | Fristablauf: **TT.MM.JJJJ** |
| Abgelehnt von: | *(Länderangabe bei ablehnender Stellungnahme)* |

| | |
|---|---|
| Detail-Version ... : **TT.MM.JJJJ** | Fristablauf: **TT.MM.JJJJ** |

| Anmerkungen: | *(Detailangaben zur Freigabe)* |
|---|---|

# 1. Inhaltsverzeichnis

# 2. Einleitung

Cloud Computing ist ein weiterer Schritt zur durchgängigen Virtualisierung von IKT-Infrastruktur und –Services. Viele Innovationsprojekte und eine erfolgreiche Kooperation der letzten Jahre haben das österreichische E-Government in das europäische Spitzenfeld gebracht. Die österreichische Verwaltung möchte das Ziel und den Weg für erfolgreiches E-Government der vergangenen Jahre in Zukunft weiterverfolgen - eine der möglichen Säulen dieses Weges kann das Potential von Cloud Computing sein.

Cloud Computing ist eine Form der flexibel am Ressourcenbedarf orientierten Nutzung von IT-Leistungen. Diese werden in Echtzeit als Service über das Internet bzw. Intranet bereitgestellt und nach Nutzung abgerechnet. Die Nutzer (also die internen IKT-Dienstleister der öffentlichen Verwaltung) müssen IT-Ressourcen nicht selbst anschaffen und betreiben, sondern nutzen die nötigen Kapazitäten für Daten, Rechenleistung und Anwendungen bei Anbietern als „Services aus dem Netz“. Damit ermöglicht Cloud Computing den Nutzern einen bedarfsgerechten Einsatz von Mitteln und eine Umverteilung von Investitions- zu Betriebsaufwand. Beides kann somit für hohe Flexibilität sorgen. Cloud Computing ist keine grundsätzlich neue Technologie, sondern kombiniert vorhandene Technologien und Verfahren für eine standardisierte Bereitstellung von Diensten (Services) und ist daher eine Weiterentwicklung des Outsourcing Modells; durch die Anforderungen des Cloud Computing wurden aber Technologien stark weiter entwickelt und auf eine neue Ebene im Bereich Skalierung, Flexibilität, Nutzungsgrad und geteilte Nutzung gebracht.

Cloud Computing ist eine Chance, birgt aber auch Risiken. Die Plattform Digitales Österreich hat in einer gemeinsamen Arbeitsgruppe (AG Cloud) der Bund/Länder/Städte/Gemeinden-Kooperation (kurz Kooperation-BLSG) das vorliegende Positionspapier mit Stand Juni 2011 erstellt, welches die Möglichkeiten des Einsatzes von Cloud Computing in der österreichischen öffentlichen Verwaltung untersucht. Das Positionspapier wurde im März 2016 um die rechtliche Checkliste der AG Resi ergänzt und mit September 2016 einer allgemeinen Aktualisierung unterzogen. Das Positionspapier soll Grundlageninformationen für nötige strategische Entscheidungen bereit stellen bzw. wie man diese Entscheidungsgrundlagen erarbeitet und was man dabei beachten muss; es beinhaltet Begriffsdefinition, Marktsituation, rechtliche/strukturelle/wirtschaftliche/technische Aspekte (Geschäftsprozesse), Auswirkungen, Chancen und Risiken sowie potentielle Anwendungen für klassische Rechenzentren, eine Private Cloud und eine Public Cloud als auch Beispiele und Prozesse für eine Migration. Im Kontext der BLSG-Strukturen der Behörden der Österreichischen Verwaltung geht es nicht nur um die Betrachtung von Public Cloud Angeboten, sondern auch um den Einsatz der Konzepte des Cloud Computing in den eigenen Infrastrukturbereichen (sog. Private Cloud) sowie künftige E-Government-Applikationen nach „Cloud-Prinzipien“ zu designen.

Um bei geringstem Risiko den höchsten Mehrwert für Bürgerinnen und Bürger und Verwaltung durch Cloud Computing zu erreichen, wäre Cloud-Nutzung, welche auf die Notwendigkeit österreichischer Behörden abgestimmt ist, eine Option (Private Cloud oder Hybrid Clouds). Dabei ist die strategische Abhängigkeit von einem einzelnen Cloud-Anbieter zu vermeiden, wozu die Nutzung mittlerweile etablierter Cloud-Standards (z.B. OpenStack-Architektur) beitragen kann. Darüber hinaus können und sollen Public Cloud-Angebote genutzt werden, wo dies die Rahmenbedingungen erlauben und die Wirtschaftlichkeit gegeben ist.

Die in diesem Zusammenhang zu betrachtenden Chancen und Risiken müssen in Bezug auf Wirtschaftlichkeit, verbesserte Reaktionszeit bei wechselndem Ressourcen-Bedarf, strategische Risiken „Wissens-/Skills Verlust“ und strategische Abhängigkeit vom „Cloud

Service Provider“ (CSP), Verletzlichkeit durch Angriffe sowie Abhängigkeit von einer Netzinfrastruktur bewertet werden.

Wenngleich der Trend „Cloud Computing“ schon einige Jahre andauert und nunmehr mit 2016 "Digitale Transformation" im Fokus steht, hat die Cloud nichts an ihrer Aktualität für die österreichische Verwaltung eingebüßt. Nicht zuletzt deshalb, weil Cloud Computing auch als Kernelement der Digitalen Transformation erkannt wurde, so ein IDC (siehe Grafik, Stand 2015).

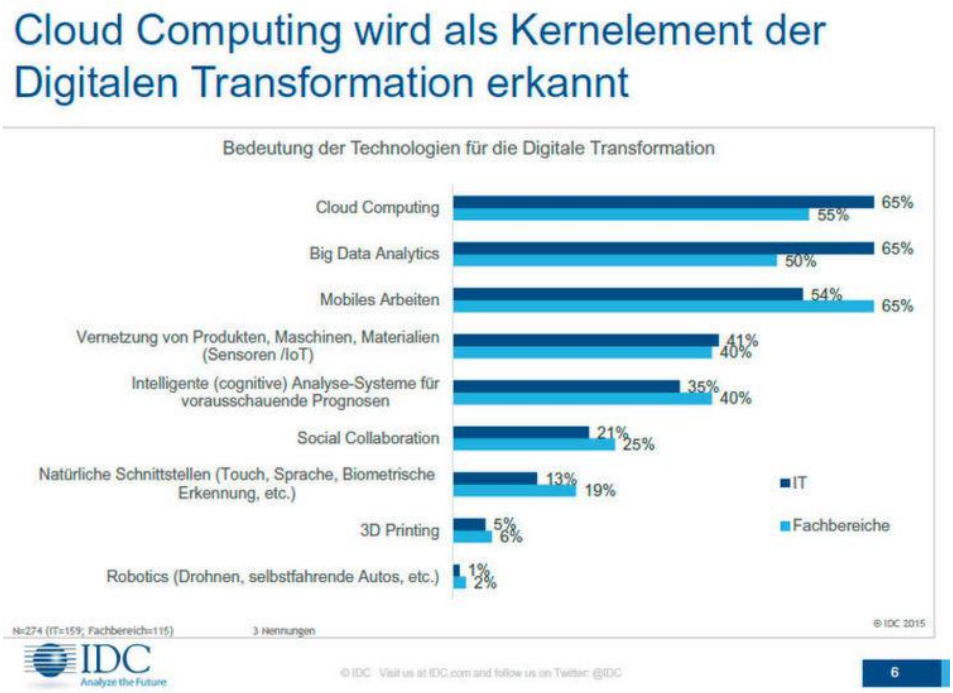


**Abbildung 1: Cloud Computing als Kerntechnologie der Digitalen Transformation**

Einige „Private Cloud“ - Lösungen sind mittlerweile in der österreichischen Verwaltung angekommen und man darf erwarten, dass durch die fortschreitende Digitalisierung Cloud Computing weiteren Auftrieb erhält.

# 3. Begriffsdefinition

Cloud Computing ist ein Begriff, der bereits seit ein paar Jahren die IT-Landschaft prägt. Dahinter verbergen sich zum Teil zwar altbekannte Architekturen und Konzepte, die aber Dank fortschreitender technischer Entwicklungen erstmals markttauglich umsetzbar sind. Einer der Schlüsselaspekte hinter dem breiten Interesse an Cloud Computing ist eine mögliche wirtschaftliche Effizienzsteigerung gegenüber traditionellen IT Verfahren. Dem zur Seite stehen Begriffe wie Kunden / Nutzer / Auftraggeber / Anwender, Organisation, IT-Organisation wobei im Zusammenhang mit Cloud Computing folgendes damit verstanden werden soll:

- Kunde - der gegenüber dem Cloud Service Provider (CSP) oder auch Cloud Anbieter auftretende Auftraggeber – Bsp. auf Ebene des Bundes wäre z.B. Ministerium

Hinter Cloud Computing steht ganz allgemein das Anbieten bzw. Nutzen von Ressourcen oder Diensten, die über Netzwerke zur Verfügung gestellt werden. Charakteristisch ist des Weiteren, dass Ressourcen oder Dienste nicht unbedingt dediziert einem Kunden zugeordnet, sondern auch dynamisch je nach Bedarf – und Vertragsmodell – zur Verfügung gestellt werden (shared services/resources).

Grob zusammengefasst versteht man darunter eine bedarfsgerechte und flexible Bereitstellung von IT-Ressourcen, deren tatsächliche Nutzung abgerechnet wird.

Das National Institute of Standards and Technology (NIST) kategorisiert Cloud Computing-Dienste anhand von Charakteristiken, Servicemodellen sowie Einsatzvarianten (vgl. [NIST09]).

### 3.1.1. Charakteristiken von Cloud Computing

- **On-Demand Self-Service / Self-provisioning of resources** (Ressourcenmanagement durch Nutzer/Kunde): Ein Kunde (s.o.) 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.
- **Massive Scalability** (Skalierbarkeit): Je nach Anforderungen können Ressourcen im entsprechenden Umfang dem Kunden zur Verfügung gestellt werden.

- **Rapid Elasticity** (Elastizität): 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. Dank der dynamischen Verteilung von Ressourcen und Diensten können bspw. Lastspitzen gut ausgeglichen werden.

- **Measured Service / Pay as you go** (verbrauchsorientiertes Bezahlmodell): 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 - Nutzer zahlen in der Regel nur für tatsächlich abgerufenen Ressourcen und Dienste (je nach Vertragsmodell).

- **Multitenancy** (Mehrmandantenfähigkeit): Ressourcen und Dienste werden zwischen allen Kunden/Nutzern dynamisch aufgeteilt.

### 3.1.2. Servicemodelle des Cloud Computings

Im Zusammenhang mit Cloud Computing existiert eine Klassifizierung der Services in drei unterschiedliche Modelle – eine Detaillierung bzw. Zuordnung ist in den folgenden Kapiteln nach Möglichkeit durchgeführt worden bzw. ist spätestens zum Zeitpunkt einer Überlegung der Nutzung in der Analyse des Services / der Anwendung anzustellen:

- **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.

Zusätzlich werden aktuell weitere Ebenen diskutiert:

- **Business Process as a Service (BPaaS):** geht aus der SaaS-Ebene hervor und wird durch eine stärkere Nähe zum Geschäftsprozess charakterisiert.
- **Data as a Service (DaaS)**
- **Network as a Service (NaaS)**

### 3.1.3. Ausprägungen von Cloud Computing

In der Praxis sind drei grundsätzliche Ausprägungen für Cloud Computing zu unterscheiden – die Unterscheidung wird nach Möglichkeit in den folgenden Kapiteln angewandt; sollte keine Unterscheidung angegeben sein, wäre trotzdem zum Zeitpunkt der Überlegung der Nutzung von Cloud Ausprägungen die Unterscheidung individuell anzuwenden bzw. hinsichtlich der Chancen und Risiken zu analysieren.:

- **Public Cloud:** Die Cloud-Infrastruktur ist öffentlich über Internettechnologien zugänglich und wird von einem CSP betrieben. In der Regel wird diese Ausprägung 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.
    - **Virtual Private Cloud:** ist eine spezifische Public Cloud Ausprägung, wobei mittels geeigneter Sicherheitsvorkehrungen dem Kunden eine abgekapselte IT-Infrastruktur zur Verfügung gestellt wird, die unter Verwendung von Secure VPN (Virtual Private Network) Technologie direkt mit dem Kunden-Netzwerk verbunden ist.
- **Private Cloud:** Die Cloud-Infrastruktur wird für einen einzelnen Auftraggeber bzw. vorgegebene Gruppe betrieben, die ausschließlichen Zugriff auf die Cloud hat. Sie kann die Infrastruktur selbst oder durch Dritte betreiben lassen. Skaleneffekte und Kosteneinsparungen werden reduziert, stärkere Individualisierungen der Dienste (d.h. Anpassung auf die Erfordernisse der Kunden) sind möglich, aus Sicht des Auftraggebers 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.

Zusätzlich kommen in der Literatur weitere Begriffe wie Enterprise Cloud, Exclusive Cloud, etc. vor. Diese lassen sich aber aufgrund deren Eigenschaften immer einer dieser drei Hauptmodelle unterordnen. Das der Cloud zu Grunde liegende Netzwerk ist in der Regel offen (bei Public Clouds ist dies meist das Internet). Selbst die in einer Cloud zur Verfügung gestellten Ressourcen und Dienste konzentrieren sich nicht auf einzelne, wenige Standorte. Vielmehr können die in einer Cloud angebotenen Dienste und Ressourcen global verteilt sein. Ein CSP entspricht daher nicht mehr zwingend dem Bild eines klassischen Rechenzentrumsbetreibers mit wenigen, überschaubaren Standorten (dies gilt insbesondere bei Public Clouds).

# 4. Marktsituation

Mit Cloud Computing werden global bereits Umsätze im zweistelligen Milliarden-Dollar-Bereich erzielt. Für das Jahr 2016 berechneten Analysten für das Segment Public Cloud Computing IaaS ein Marktvolumen (international) von 38 Mrd. US-Dollar, für SaaS und PaaS 12 Mrd. US$. Bis 2018 wird mit einem Anstieg des Marktvolumens für Cloud Computing auf bis zu 104 Mrd. US-Dollar (Quelle Statistica) gerechnet.

Das Marktwachstum für Cloud Computing entwickelt sich auch im deutschsprachigen Raum dynamisch. Beispielgebend dazu aus einer Bitkom/KPMG Veröffentlichung vom 12. Mai 2016 über den deutschen Markt:

„… Nach den Ergebnissen der Umfrage nutzten im **Jahr 2015 26 Prozent der Unternehmen Public Cloud Computing, im Jahr 2014 erst 16 Prozent**. Dagegen stabilisierte sich der Einsatz von Private Clouds bei 38 Prozent (Vorjahr: 39 Prozent). „Bislang installierten die Unternehmen vor allem Private Clouds, weil vielen die Nutzung über das öffentliche Internet zu unsicher schien. Das ändert sich jetzt“, sagte Pols. **„Das vergangene Jahr markiert den Durchbruch für Public Cloud Computing in der deutschen Wirtschaft.“** …“

Aufgrund der tatsächlichen und prognostizierten Wachstumsraten im Zusammenhang mit Cloud Computing versuchen sowohl neue Cloud Service Provider (CSP) als auch klassische IT-Anbieter mit zum Teil sehr unterschiedlichen und insbesondere in ihrer Nachhaltigkeit nicht immer leicht nachvollziehbaren Geschäftsmodellen am erwarteten Kuchen mitzumischen.

Es positionieren sich CSP wie Google oder Amazon, ausschließlich über "Public Cloud" Angebote, vielfach werbe- oder querfinanziert und mit somit noch nicht vertrauten Geschäftsmodellen und -bedingungen. Diese Public Cloud Angebote werden aber sukzessive für den Business/Enterprise Bereich durch Angebote erweitert.

Klassische Softwarehersteller versuchen mit vertrauten Produkt- und Lizenzmodellen in der Cloud einerseits ihren Bekanntheits- und Vertrauensvorteil auszuspielen und andererseits versuchen diese natürlich Kundenabwanderung in Richtung der neuen CSP zu verhindern. Vor allem Microsoft hat mit seiner „Microsoft-Cloud-First-Strategie“ aufhorchen lassen und positioniert die Azure Plattform für IaaS-Produkte und Office365 für SaaS-Produkte mit großen Wachstumsschüben, aber auch Oracle, IBM, CISCO, HP haben eine klare Cloud Ausrichtung gewählt. Hardwarehersteller wie z.B. IBM sind bemüht, den potentiellen Umsatzrückgang im reinen Hardwaregeschäft durch Private und Hybrid Cloud Ansätze und Angebote zu kompensieren. Und klassische Outsourcing Partner verpassen ihren zum Teil schon lange etablierten Angeboten und Services einfach einen Cloud „Anstrich“. Hinzu kommen noch Konsulenten und Lösungsanbieter mit unterschiedlichen (Eigen-) Finanzierungsmodellen. Eine objektive Gewichtung und Beurteilung der vielen Positionspapiere und Empfehlungen in Sachen Cloud Computing stellt daher nach wie vor eine große Herausforderung dar (es sei aber auch auf die dynamische Entwicklung hingewiesen, da in kurzen Abständen erhebliche Veränderungen stattfinden, die es laufend zu berücksichtigen gilt).

Ein Wachstumshemmnis, das besonders für den öffentlichen Sektor von großer Relevanz ist, liegt darin, dass die Nutzer der Cloud eher stark an einen Cloud Service Provider (CSP) gebunden sind. Aufgrund erst entstehender Standards im Bereich Cloud Computing sind viele Services oder Systeme der CSP (z.B. File-System, Nutzer- und Rechteverwaltung, etc.) proprietär. Der Transfer von einem CSP zu einem anderen ist nur bei bestimmten einfachen

Services (z.B. Object-Storage) oder innerhalb einer Technologie-Gemeinschaft (z.B. vCloud Community) einfach möglich. Bei einem Ausfall des CSP – nicht nur infolge technischer Gründe sondern auch infolge wirtschaftlicher Gründe (eDoS: economic Denial of Service) – könnte dadurch die Verfügbarkeit der Dienste und Daten gefährdet und auch eine Abhängigkeit des Kunden vom CSP erzeugt werden. Die Industrie hat diese Lock In Drohung erkannt und bietet im Enterprise Bereich nun zunehmend „Multi-Cloud-Fähigkeit“ ihrer eigenen Cloud-Stacks an. Teilweise werden auch Cloud-Brokerage-Softwarelösungen angeboten. Diese Entwicklung erfolgt auch vor dem Hintergrund, dass im Enterprise die Hybrid-Cloud Lösungen im Vormarsch sind und Unternehmen auch bei SaaS unterschiedliche Cloud-Lösungen selektiv einsetzen. In einer Studie (Rightscale 2016: State of the Cloud Report) geben 95 % der befragten Unternehmen an ein Multicloud Strategie zu verfolgen. Auch bei der Verteilung der Workload setzen Unternehmen über 1000 Mitarbeitern (im Gegensatz zu KMU’s) auf Hybrid-Lösungen, derzeit mit Schwerpunkt Private Cloud. 55% der befragten Unternehmen haben nur 20-40% der Arbeitslast in einer Public Cloud.

Eine wesentliche Veränderung des europäischen Cloudmarktes verfolgt die Deutsche Telekom bzw. T-System mit seinem neuen Produkt. T-Systems hat sich zum Ziel gesetzt, Cloud Computing mit der Sicherheit der europäischen Datenschutzbestimmungen und trotzdem preislich auf Augenhöhe mit den großen amerikanischen Anbietern (Hyperscale-Clouds) anzubieten. Dies 2016 in 2 verschiedenen Ausprägungen:

- Die Open Telekom Cloud:
  Primär fokussiert auf IaaS-Services und als europäische Alternative z.B. zu AWS positioniert

- Microsoft Azure und Office365 unter Eigenbetrieb der T-Systems in Deutschland und unter vertraglicher Zusicherung aller europäischen Datenschutzrichtlinien

Diese Entwicklung einer europäischen Alternative zu den amerikanischen Hyperscale-Clouds wird noch näher zu analysieren und zu beobachten sein. Für Microsoft Cloud Services ergibt sich damit eine datenschutzrechtlich klarere Alternative, wenn auch die Details noch zu bewerten sind.

Die mangelnde Reife des Cloud Marktes in Bezugs auf Standards und der Bedarf eines stärkeren Abgleichs von Marktangebot und Datenschutzrecht führen trotz der ökonomischen Vorteile einer Public Cloud dazu, dass europäische Verwaltungen derzeit eher konkrete Strategien und Umsetzungspläne in Richtung Private Cloud bzw. Community Cloud, also die Vernetzung und gemeinsame Nutzung der verwaltungseigenen Systeme und Ressourcen, konzipieren. So hat beispielsweise die britische Regierung ein eigenes Cloud-basiertes System für die öffentliche Verwaltung errichtet, in dem mehrere leistungsfähige Datenzentren zu einer Private Cloud (G-Cloud) vernetzt werden und die bisher genutzten Rechenzentren zum Teil ersetzen [EGCC10]. Durch die Private Cloud sollen wirtschaftliche Vorteile erschlossen werden, ohne Kompromisse in den Bereichen Datensicherheit und –verfügbarkeit eingehen zu müssen.

In zwei Bereichen werden diese Private Cloud Ansätze zu kurz greifen müssen:

- Ausreichende Elastizitäten für sehr stark schwankenden Ressourcenbedarf lassen sich durch rein verwaltungsintern geschaffene Private Clouds auch künftig kaum kostengünstig realisieren

- Die Nutzung von attraktiven Funktionen, die Software-Hersteller wie Microsoft nur über eine Anbindung an die Hersteller-Cloud als Hybride Cloud Service anbieten, sind in rein verwaltungsinternen private Clouds nicht verfügbar.

# 5. Rechtliche Aspekte

Das Kapitel 4 wurde mit der Rechtliche Checkliste zum Einsatz von Cloud Computing der AG Recht und Sicherheit aus dem Jahr 2015 ersetzt und die AutorInnen dieser Checkliste als MitautorInnen aufgenommen.

## *5.1. Datenschutz*

- Werden personenbezogene Daten verwendet?

Werden keine personenbezogenen Daten verwendet, dann ist keine weitere datenschutzrechtliche Prüfung erforderlich.

Wenn es sich hingegen um personenbezogene Daten handelt, dann sind bei der Wahl des Cloud Service Providers (CSP), welcher als Dienstleister[1] im Sinne des § 4 Z 5 DSG 2000 zu beurteilen ist, nachstehende Fragen zum Datenschutz zu prüfen. Alle Fragen sind vor der Auswahl eines Cloud-Dienstes stets mit „**Ja**“ zu beantworten:

### 5.1.1. Verarbeitungs- bzw. Speicherort von Daten (Storage)

Bestimmte Datenschutzbestimmungen verbieten den Transfer von Daten in andere oder bestimmte Länder, oder es ist die explizite Zustimmung durch jene Person, auf die sich die Daten beziehen, erforderlich. Eine dynamische Umverteilung im Laufe der Zeit ist mit zu beachten.

Bestehende Regelungen, wonach Daten ausschließlich im Inland gespeichert werden dürfen (z.B. im Zusammenhang der umfassenden Landesverteidigung), schließen CSP außerhalb Österreichs aus!

- Werden die Daten ausschließlich im europäischen Wirtschaftsraum oder in Ländern, die in der Datenschutzangemessenheits-Verordnung angeführt sind, verarbeitet? [2]

[1] Es wird angemerkt, dass der Auftraggeber bei der Auswahl seines Dienstleisters die freie Wahl hat, jedoch muss dieser die auch die Dienstleisterpflichten einhalten. Der Auftraggeber hat weiters seine Auftraggeberpflichten einzuhalten bzw. sicherzustellen, dass sein Dienstleister dies tut. Die Verantwortung für die Einhaltung dieser Auftraggeber- und Dienstleisterpflichten verbleibt jedoch letztlich beim Auftraggeber. Im Einzelfall kann die Abgrenzung der Rolle des Auftraggebers und des Dienstleisters schwierig sein. Im Zweifel ist jedoch anzunehmen, dass die Behörde als Auftraggeber angesehen wird.

[2] § 12 DSG 2000: Übermittlung und Überlassung an Empfänger im Europäischen Wirtschaftsraum ist keinen Beschränkungen unterworfen. Weiters bedarf der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz keiner Genehmigung gemäß § 13 (vgl. auch Datenschutzangemessenheits-Verordnung).

§ 13 DSG 2000: Sofern die Datenübermittlung ins Ausland nicht genehmigungsfrei gemäß § 12 ist, so ist eine Genehmigung der Datenschutzbehörde vor der Übermittlung einzuholen.

- Wenn nein, liegt eine Genehmigung der Datenschutzbehörde oder liegen Standardvertragsklauseln[3] für die Übermittlung personenbezogener Daten in Drittländer (2001/497/EG) vor?

### 5.1.2. Datensichersicherheitsmaßnahmen

- Stellt der Dienstleister die Maßnahmen zur Datensicherheit gemäß § 14 DSG 2000 sicher?
- Trifft der Dienstleister insbesondere Maßnahmen zum Schutz vor zufälliger und unrechtmäßiger Zerstörung?
- Trifft der Dienstleister insbesondere Maßnahmen gegen den Verlust oder unbefugtem Zugriff auf die Daten?
- Trifft der Dienstleister insbesondere Maßnahmen zur Protokollierung der Zugriffe?

### 5.1.3. Betroffenenrechte (Auskunfts-, Richtigstellungs-, Löschungs- und Widerspruchrecht) gemäß §§ 26 bis 28 DSG 2000

Zugriff auf Daten (Access): Die Person, auf die sich Daten beziehen (d.h. der/die Betroffene im Sinne des DSG), kann sowohl Auskunft über, als auch Korrektur oder das Löschen dieser Daten verlangen.

- Ist daher sowohl die Einsichtnahme als auch die Richtigstellung bzw. das Löschen der Daten der Betroffenen in der Cloud gemäß den rechtlichen Vorgaben gewährleistet und durchführbar?
- Gibt es ein Regelwerk das das Verfahren zur Wahrung der Rechte der Betroffenen in einem Informationsverbundsystem klar regelt?

### 5.1.4. Verbleib und Vernichtung von Daten (Retention/Destruction)

Am Ende der Haltezeit von Daten müssen diese geeignet gelöscht werden.

- Gibt es ein Regelwerk zur Umsetzung der Skartierung von Daten (Retention-Policy)?
- Gibt es ein Regelwerk zur Skartierung von Protokolldaten einschließlich Verkehrs- und Metadaten?
- Werden die Daten tatsächlich gelöscht (und nicht nur die Zugriffsrechte entzogen)?
- Ist dabei sichergestellt, dass keine Kopien der Daten (z.B. Back-Up) erhalten bleiben?

[3] http://www.dsb.gv.at/site/6208/default.aspx

- Gibt es ein Regelwerk, wonach die Zurückstellung (inkl. Löschung der Daten beim CSP) an den Auftraggeber nach Beendigung des Vertragsverhältnisses erfolgt?

### 5.1.5. Datenschutzverletzungen (Privacy Breaches):

- Ist bei Datenschutzverletzungen ein Meldeprozess bei Auftraggeber und Dienstleister etabliert?

## *5.2. Vertragsrecht*

Sollte immer auf den Einzelfall abgestimmt sein. Folgende Punkte könnten jedoch Inhalt einer vertraglichen Regelung sein:

- Zusicherung der Einhaltung der datenschutzrechtlichen Anforderungen;
- Informationsverfahren bei datenschutzrechtlichen Verletzungen;
- Gewährung eines Kontrollzugriffs durch den Auftraggeber;
- Dienstleistervereinbarungen (abhängig von der Anzahl der Dienstleister bzw. Sub-Dienstleister die in Anspruch genommen werden);
- Art der Leistung (Leihe, Miete, Werk- oder Dienstleistung);
- Haftung und Gewährleistungsansprüche;
- Service-Level-Agreement (SLA);
- Sonstige Vereinbarungen (z.B. ISO 27001, Informationssicherheitsmanagementsystem (ISMS);
- Einhaltung referenzierter Konvention (internationale Standards, BLSG-Konventionen);
- Migrierbarkeit der (Daten-)Standards im Fall des Betreiberwechsels, Unternehmensübergang oder im Insolvenzfall;

## *5.3. Vergaberecht*

- Cloud Service Provider sind meist international tätig und stellen ihre Leistungen unter Standard-AGB zur Verfügung. Es ist daher zu prüfen, ob sich diese CSP überhaupt an einem formellen Ausschreibungsverfahren beteiligen würden und sich Abweichungen von den AGB mit dem jeweiligen CSP vereinbaren lassen.

## *5.4. Strafprozessrecht*

Innerstaatliche Auskunftspflichten gegenüber österreichischen Strafverfolgungsbehörden sind zu beachten (z.B. Verkehrsdaten)

# 6. Organisatorische Aspekte

Im folgenden Abschnitt werden Chancen und Risiken aus der organisatorischen Perspektive dargestellt und mögliche Auswirkungen von Cloud Computing auf die IT-Organisation der öffentlichen Verwaltung erläutert. Im Fokus der Betrachtungen steht dabei das Modell „Public Cloud“, da sich hier die größten organisatorischen Änderungen in der IT-Struktur ergeben. Wesentliche Teile der Überlegungen gelten jedoch auch für die Modelle „Private Cloud“ und „Community Cloud“.

Cloud Computing kann organisatorische Vorteile durch Standardisierung bieten. Organisatorische Nachteile und Risiken inkludieren eine erschwerte Steuerung des IT-Einsatzes, strukturelle Abhängigkeit aufgrund von Lock-in-Effekten gegenüber Cloud-Anbietern sowie die Notwendigkeit der Kontrolle der Einhaltung von Governance-Regeln [DSCC10]. Cloud Computing stellt die organisatorische Steuerung der IT in der öffentlichen Verwaltung vor zahlreiche Herausforderungen:

- *Standardisierung:* Prinzipiell bietet Standardisierung in der IT neben der Kostenreduktion auch mehrere mögliche organisatorische Vorteile (Vereinfachung von Prozessen, Integration externer Partner, Flexibilität und Agilität). Cloud Computing ist, sofern richtig eingesetzt, eine Möglichkeit, Standardisierung zu fördern und entsprechende Vorteile zu generieren. Falsch eingesetzt kann Cloud Computing jedoch auch zu gegenteiligen Ergebnissen führen. Bei den Standardisierungen im E-Government Umfeld soll Rücksicht genommen werden, dass Cloud nicht prinzipiell ausgeschlossen wird.

- *Organisatorische Aufspaltung:* Cloud Computing kann zu „Silo-Lösungen“ führen, wenn die Zusammenhänge zwischen Anwendungen und Prozessen bei Entscheidungen nicht berücksichtigt werden. Dann kann sich der Datenaustausch zwischen Anwendungen (bei „Silo-Lösungen“) als schwierig erweisen, was die Service-Qualität aus der Perspektive des Auftraggebers reduziert.

- *Strukturelle Abhängigkeit:* Durch zu starke Bindung an einen bestimmten CSP oder einen Service können Abhängigkeiten bis zu Lock-in-Effekten entstehen, die einen Wechsel zu einem anderen Dienstleister oder einen internen Service erschweren. Potentielle Abhängigkeiten und Migrationskosten sollten deshalb stets berücksichtigt werden.

- *Potentielle Steigerung des Verarbeitungsvolumens:* Bei einem Einsatz von Cloud Computing werden grundsätzlich sinkende Kosten erwartet. In der Praxis kann es aber aufgrund gesteigerter Nutzung entsprechender Services zu höheren Verbrauchsmengen und damit in weiterer Folge schnell zu unerwartet steigenden Kosten kommen.

- *Fehlender Kostenvergleich:* In der öffentlichen Verwaltung sind die internen Kosten bei fehlender Kostenrechnung oft nicht exakt bekannt. Ein aussagekräftiger Vergleich der Kosten zwischen einer Cloud-Lösung und einer internen Lösung ist dann oftmals nicht oder nur schwierig möglich.

- *Vereinbarungen:* Oftmals ist in einer traditionell strukturierten internen IT-Abteilung wenig Erfahrung mit Dienstleistern und entsprechenden Vereinbarungen vorhanden.

Gerade sorgfältig ausgearbeitete Bestimmungen in den Dienstleister- bzw. Betriebsvereinbarungen sind für einen erfolgreichen Einsatz von Cloud Computing aber von großer Bedeutung. Zu berücksichtigende Aspekte beinhalten u.a. Service Level Agreements (SLA), Verfügbarkeit, Change Management, Notfallmanagement, Qualitätssicherung. Auch die Kontrolle dieser Vereinbarungen muss organisatorisch berücksichtigt werden.

Um die Risiken des Cloud Computing zu minimieren bzw. die Potentiale bestmöglich auszuschöpfen, ist eine ausführliche Voranalyse über Ziele und Anforderungen erforderlich. Idealerweise wird dabei ein Vorgehensmodell zur Einführung von Cloud Computing eingesetzt [PCEC09]. Ein Beispiel dafür ist das fünfstufige Vorgehensmodell von Reeves und Santos [BSCA10].

1. Projektvorbereitung: Formierung eines Kernteams zur Entwicklung einer Cloud-Strategie, Definition von Geschäftszielen und Darlegung der Migrationsgrundsätze, Entwicklung einer Migrations-Roadmap

2. Analyse des Geschäftsfeldes sowie der bestehenden IT-Anwendungen: Identifizierung der Risiken und der Einflüsse im Falle eines Ausfalls der Cloud, Analyse der Anforderungen und Abhängigkeiten der IT-Anwendungen, Kostenvergleich Cloud vs. „interner“ Betrieb der IT-Anwendungen, Analyse der Änderung der internen organisatorischen Abläufe sowie generelle Auswirkungen auf die Organisation, Erarbeitung von Richtlinien zur Bestimmung des passenden Cloud-Modells (Software as a Service, Hardware as a Service, Infrastructure as a Service) bzw. der Ausprägung (Private, Public oder Hybrid).

3. Auswahl des Cloud-Anbieters: Analyse des Leistungsvermögens sowie des Risikopotenzials der Cloud-Anbieter anhand der ermittelten Anforderungen und den vorliegenden Angeboten, Entscheidung nach Einsatz von geeigneten Evaluierungsverfahren.

4. Vermeidung bzw. Reduzierung der Risiken durch Planung einer Exit-Strategie (Vertragsgestaltung, Verwendung offener Datenformate)

5. Planung des laufenden Betriebes: Erarbeitung von Governance-Regeln (Management von unerwarteten Ausgaben, Budgetplanung, ungeplante Auswirkungen)

Von zentraler Bedeutung ist während der Projektplanung (Punkt 2) im Zusammenhang mit dem Einsatz von Cloud Computing die Analyse der „*Cloud-Fähigkeit*“ von IT-Anwendungen. Aus organisatorischer Perspektive sind (bei Cloud Computing) folgende Aspekte zu berücksichtigen [BSCA10]:

- Auswirkungen auf die Kontinuität der Geschäftstätigkeit: Wann ist eine IT-Anwendung zu geschäftskritisch, um in die Cloud ausgelagert zu werden?

- Informationssicherheit: Werden Daten verarbeitet, die aufgrund gesetzlicher Bestimmungen oder nach der Einschätzung der Organisation nicht für die Nutzung von (Public-)Cloud Computing geeignet sind?

- Risikotoleranz: Sind die Risiken eines Ausfalls der IT-Anwendung für eine Organisation tragbar? Gibt es einen Schwellenwert, der durch SLAs nicht garantiert werden kann?

- Interdependenz von IT-Anwendungen: Hat eine IT-Anwendung zu viele Abhängigkeiten mit bestehenden Services um sinnvoll in eine Cloud ausgelagert zu werden?

- Migrationsaufwand: Was ist der maximal tolerierbare Aufwand für die Migration eines Services in die Cloud? Steht dies in Verhältnis zu den erwarteten Einsparungen (Kosten-Nutzen Analyse)?

Generell gilt es, die Cloud-Fähigkeit von neuen IT-Anwendungen bereits in der Architekturphase und Vergabephase zu prüfen und bei positiver Einschätzung weitere Schritte zu setzen bzw. eine entsprechende Analyse durchzuführen (z.B. durch das skizzierte fünfstufige Vorgehensmodell). Umfangreiche und aktuelle Sammlungen von zu berücksichtigenden Aspekten für einen erfolgreichen Einsatz von Cloud Computing finden sich bei Bedarf auch an verschiedenen Quellen im Internet und in Fachzeitschriften, z.B. unter [ÜRCC].

# 7. Wirtschaftliche Aspekte

Noch befindet sich Cloud Computing in der frühen Phase der Marktdurchdringung. Mittel- bis langfristig ist anzunehmen, dass ein erheblicher Anteil traditioneller IT-Dienstleistungen durch Cloud-basierte Services ersetzt wird. Das Wirtschaftlichkeitsargument – also das Potential IT-Kosten nachhaltig zu senken – wird in diesem Zusammenhang als wichtigster Treiber für den Wandel in Richtung Cloud gesehen.

Die Cloud Service Provider (CSP) realisieren die Kostenvorteile vor allem durch das Standardisieren von Services, das Bündeln von IT-Ressourcen und Automatisierung von Abläufen. Auf Anbieterseite ermöglicht das Cloud-Konzept weitreichende Skaleneffekte. So sinken mit zunehmender Auslastung auf Anbieterseite die (Betriebs-)Kosten (Strom – GreenIT/CO2 Reduktion, Sicherheit, etc.) pro Server. Gleichzeitig können die Overhead-Kosten auf eine größere Zahl von Nutzern aufgeteilt werden. Der Kunde profitiert zudem durch ein höheres Maß an Flexibilität und budgetärem Planungsspielraum, da er die Ressourcen des CSP exakt seinem Bedarf entsprechend – also auch kurzfristig – in Anspruch nehmen kann. Investitionskosten zum Abdecken von Auslastungsspitzen können entfallen.

Für die Verwaltung bedeutet Cloud Computing aus wirtschaftlicher Sicht:

- Standardisierte IT-Infrastruktur und –Dienste sind unter den Rahmenbedingungen einer Cloud-Architektur und eines Cloud -Geschäftsmodells wirtschaftlicher zu beziehen bzw. zu erbringen. Die Anwendungen sind jedoch umfassend zu betrachten.

- Die Kostensituation bei funktionalen Anpassungen von Cloud-Services oder deren Integration in bestehende Geschäftsprozesse ist im Vergleich zu den Adaptionskosten herkömmlicher Architekturen weitgehend unbekannt (bzw. muss man im Detail unterscheiden für IaaS, PaaS und SaaS). Aufgrund des hohen Automatisierungsgrads der Cloud Services sind diese Kosten aber tendenziell höher anzusetzen.

- Massiv skalierende Public Cloud Services scheinen zumindest derzeit nicht anpassbar zu sein. Hier sind den Kostenvorteilen im Einkauf etwaige Effizienzverluste in der Nutzung der Standardservices ohne Anpassungen für die Verwaltung gegen zu rechnen. IT-Anwendungen sind als Werkzeug ja nicht nur aus einer Kostensicht im Einkauf sondern vor allem auch hinsichtlich ihres Beitrags zur Effizienzsteigerung der Geschäftsprozesse der Verwaltung zu beurteilen; für dieses Umfeld ungeeignete Prozesse können auch zu Kostensteigerungen führen.

- Zusätzlich zu den zu erwartenden Kostenvorteilen verändert sich bei Public Cloud Services für den Auftraggeber des Cloud Services auch die Kostenstruktur grundlegend. Durch die nutzungsbedingte Verrechnung werden Investitionskosten durch Betriebskosten ersetzt, was entsprechende Auswirkungen auf die Budgetplanung hat. Für Private Cloud Services gilt dieses Argument unabhängig von der Größenordnung der Private Cloud bzw. Community Cloud nicht. Der Private Cloud Anbieter für eine große Organisation selbst muss investieren. Die Zusammenfassung von mehreren internen Kunden in einer Private Cloud bringt in

Summe mehr Investitionssicherheit für den Cloud Anbieter bei gleichzeitig hoher Flexibilität für die einzelnen Kunden.

Für die Verwaltung bedeutet Cloud Computing aus wirtschaftlicher Sicht: Die IT-Infrastruktur und –Dienste können unter Einhaltung der Rahmenbedingungen einer Cloud-Architektur und Cloud-Geschäftsmodells wirtschaftlich bezogen bzw. erbracht werden. Zusätzlich zu den zu erwartenden Kostenvorteilen verändert sich für den Auftraggeber auch die Kostenstruktur grundlegend, falls bisher kein nutzungsabhängiges Verrechnungsmodell implementiert war.

Die zu Grunde liegenden wirtschaftlichen Parameter sind aufgrund der zum Teil fehlenden Transparenz des technischen und organisatorischen Modells der CSP schwer zu beurteilen. Abgesehen von entsprechenden vertraglichen Vereinbarungen und SLAs sollten diese Bedenken rund um das Spannungsfeld zwischen Profit und Sicherheit mit in eine Vorab-Klassifizierung über die „Cloud-Fähigkeit“ von Bereichen bzw. Daten einfließen. Natürlich muss auch die bestehende Infrastruktur in den Wirtschaftlichkeitsüberlegungen berücksichtigt werden. Die bestehende bzw. für sensible Bereiche auch künftig notwendige Infrastruktur führt zwangsläufig zu Investitionen und Fixkosten, die nicht vermeidbar sind und zusätzlich zu den Kosten der Cloud Services anfallen (Unit costs). Somit können die Vorteile einer Public Cloud nicht 1:1 auf eine Mischform bzw. mögliche Private Clouds bzw. Community Clouds der heimischen Verwaltung übertragen werden.

Eine Vorstudie zu Cloud Computing in Schweizer Behörden zeigt auf, dass es sich insbesondere für größere Organisationen – so auch für die Behörden der heimischen Verwaltung – nicht nur aufgrund der Risikominimierung sondern auch aus wirtschaftlichen Überlegungen anbietet, die Bereitstellung der IT-Services über Private Clouds bzw. Community Clouds anzugehen.

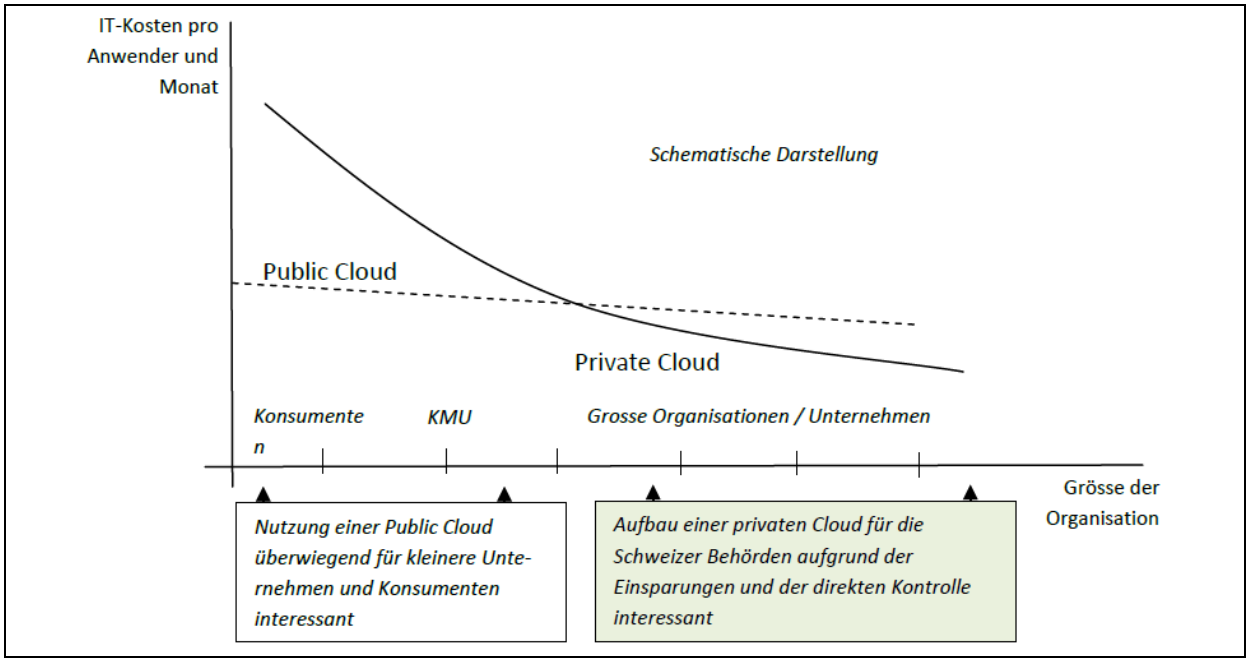


**Abbildung 2: Public vs. Private Cloud – wirtschaftliche Überlegungen (schematische Darstellung)**

# 8. Technische Aspekte und Sicherheit

Technische Aspekte wie Virtualisierung, Provisioning, gemeinsame Nutzung von Ressourcen und Ausgleichen von Lastspitzen sowie Externalisierung von Investitionskosten sind Grundeigenschaften, die Cloud Computing ausmachen.

## *8.1. Technische Aspekte*

Bei der Beschreibung von Cloud Computing-Systemen haben sich u.a. folgende technische Aspekte etabliert.

### 8.1.1. Standardisierung

IT-Anwendungen haben eine Vielzahl von Schnittstellen bzw. unterhalten Schnittstellen zu anderen Anwendungen. Sind diese Schnittstellen standardisiert, ist ein Wechsel eines Anbieters einfacher, da der Anpassungsaufwand gering sein müsste; von einer breiten Standardisierung sind wir allerdings noch weit entfernt - jedenfalls sind Projektaufwände zu kalkulieren.

Chance: Durch standardisierte Cloud-Umgebungen kann sich technisch gesehen ein Wettbewerb etablieren der den Wechsel zwischen Anbietern einfacher macht. Die Standards der Schnittstellen bilden daher ein wichtiges Kriterium um nicht in eine Abhängigkeit (Lock-In) zu kommen. Für die Standardisierung gibt es bereits eine Reihe von Standards (z.B. OVF, SAML, SPML, XACML, LIAF) die durch die Cloud-Anbieter unterstützt werden sollten.

- Open Virtualization Format (OVF)
- Security Assertion Markup Language (SAML)
- OAuth, OpenID Connect
- Service Provisioning Markup Language (SPML)
- Extensible Access Control Markup Language (XACML)
- Liberty Identity Assurance Framework (LIAF)
- Breitere Aktivitäten:
    - NIST Cloud Standard Roadmap, Reference Architecture
    - ETSI TC Cloud
    - OASIS Cloud TCs
    - DMTF Cloud Standards
    - ITU Cloud Standard roadmap

Mehr Informationen zu Standardisierungsaktivitäten finden sich im Cloud Standards Wiki[4].

[4] http://cloud-standards.org/wiki/index.php?title=Main_Page

### 8.1.2. Skalierbarkeit / Elastizität

Unter Skalierbarkeit versteht man die (automatische) Anpassbarkeit von Ressourcen an die – sich ändernden - Leistungsanforderungen von Auftraggebern / Kunden auch bei Lastspitzen (z.B. Dienstbeginn, Tagesabschluss, Monatsabschluss, Volkszählung, Wahlvorbereitung, Volksbefragung, ...).

Chance ist hier der Lastausgleich über mehrere Kunden oder Mandanten in der Cloud, da die Grundarchitektur dafür geeignet ist. Gleichzeitig kann es zum Risiko werden, wenn nicht ausreichend Ressourcen vorgehalten werden und damit alle Kunden oder Mandanten beeinträchtigt werden.

### 8.1.3. ID- und Rechtemanagement

Die Identitäts- und Rechteverwaltung ist wesentlicher Baustein der Zugangskontrolle in Cloud Computing-Systemen. Um die bestehenden Sicherheitsbedenken auszuräumen, ist daher die Lösung des CSP genau zu hinterfragen wie er damit umgeht, dass **fremde Administratoren Zugang zu Unternehmensdaten** haben. Es muss die sichere Identifikation der Kunden der Cloud selbst wie auch die der Administratoren des CSP ermöglichen. Besonders auf die Absicherung der privilegierten Benutzerprofile des CSP muss geachtet werden. Hier muss es dem Kunden der Cloud ermöglicht werden regelmäßige Audits (Zugriffe, Zugriffsprofile) durchführen zu können. Es sollten generell für die Authentisierung nur starke Verfahren für Kunden und CSP verwendet werden. Die Connectivity zu einem lokalen IDM (Identity Management) des Kunden ist sicherzustellen, da sonst erhebliche Zusatzaufwände und auch Risiken entstehen.

Das ID- und Rechtemanagement kann auch bei einem Drittanbieter angesiedelt sein.

### 8.1.4. Mandantenfähigkeit

Zu den Grundeigenschaften einer Cloud-Architektur zählt die Mandantenfähigkeit. Die sichere Mandantenfähigkeit in der Cloud soll die Partitionierung einer virtualisierten Shared IT Infrastructure ermöglichen, wie sie auch bei Server-Virtualisierung im modernen Rechenzentrum bereits eingesetzt wird. Dadurch ergibt sich die Chance verschiedene Anwendungsszenarien (z.B.: Produktions- und Testbetrieb) abzubilden.

### 8.1.5. Sicherheitsstruktur

Um die Ressourcen der Kunden oder Mandanten (Daten, Anwendungen, Netze, …) zu schützen, ist eine durchgängige Sicherheitsarchitektur zu implementieren. Da Cloud-Systeme mandantenfähig (multi-tenancy) sein müssen, ist eine sichere Trennung der Ressourcen von Kunden oder Mandanten in der Architektur abgebildet.

### 8.1.6. Cloud Management

Um den Betrieb von Cloud-Services zu gewährleisten, sind vom CSP IT-Managementfunktionen und Prozesse anzubieten, die sowohl die Einrichtung wie auch den Betrieb unterstützen. CSPs offerieren für ihre Services Werkzeuge in Form von Webportalen, die die Funktionen zur Verfügung stellen. Typischer Weise sind folgende Funktionen inkludiert:

- Steuerung von Services - dazu zählen z.B.
    - das Starten,
    - Stoppen oder
    - Reboot

- Überwachung von Services - um die Leistungsfähigkeit/Leistungsdaten des CSP zu erheben.
- Sicherheit von Services - umfassen den sicheren Zugriff auf Services, Transparenz von Zugriff und die sichere Identifikation von Kunden und Administratoren des CSP.

Wünschenswert wären zudem Werkzeuge, mit denen die Cloud Ressourcen und die lokalen on-premise Ressourcen gleich verwaltet werden können.

### 8.1.7. Technische Revision

CSP müssen zum Durchsetzen von kundenspezifischen Sicherheitspolitiken dafür geeignete Prozesse anbieten. Es muss dem Kunden möglich sein, im Rahmen der Umsetzung seiner Sicherheitspolitik die benötigten Informationen/Zugriffe auf z.B. LOG-Dateien oder Zugriffslisten zu haben, um die eigene Compliance zu gewährleisten.

### 8.1.8. Patch Management

Unter Patch Management wird die Planung und Installation von Patches (Software-Updates) zusammengefasst. Wichtig ist hier, dass Patches über die gesamte Umgebung zu definierten Zeitpunkten eingespielt werden.

Durch die standarisierte Cloud-Infrastruktur ergibt sich die Chance, das Patch Management bei höherem Effizienzgrad mit geringeren Ausfallzeiten zu bewerkstelligen. Als Schwierigkeit ist der Test der Verträglichkeit bzw. Kompatibilität von SW-Updates mit kundenspezifischen Anwendungen zu sehen.

Die wichtigsten Erkenntnisse aus den vorigen Punkten finden sich überblicksmäßig in der folgenden Zusammenfassung:

### 8.1.9. Zusammenfassung der technischen Aspekte:

| | Chance | Risiken |
|---|---|---|
| Standardisierung | Wettbewerb, Wechsel zwischen Anbietern | Ohne Standard Abhängigkeit von den CSP-Anbietern |
| Skalierbarkeit | Vorstellung nahezu grenzenloser Ressourcen durch CSP | Gleichzeitige Lastspitzen können im schlechtesten Fall zum Stillstand führen. |
| Identity- und Rechtemanagement | | Sicherheitsbedenken bei der Umsetzung der CSP, vor allem bei den privilegierten Benutzerkennungen (Administratoren) |
| Mandantenfähigkeit, Sicherheitsstruktur | Ist eine Kernanforderung an CSP und sollte damit „state of the art“ | |

| | | |
|---|---|---|
| | durchgeführt werden. | |
| Cloud Management | Standarddienste (&einheitliche Administrationskonsolen) werden durch komfortable Webportale zur Verfügung gestellt. | Einbindung der Werkzeuge an CSPs in kundenspezifische Prozesse noch nicht erprobt. |
| Technische Revision | | Auftrennung der kunden-spezifischen Daten (Log-Dateien etc.) muss vertraglich geregelt werden. Derzeit noch keine standardisierten Angebote (allerdings z.B. bei PaaS bereits eine Frage des Designs der Applikation) |
| Patch Management | Schnelles standardisierten Ausrollen von Patches durch vereinheitlichte Infrastruktur | Schwierigkeit des Testens der Kompatibilität von Patches, Rücksichtnahme auf kundenspezifische Anforderungen. |

## *8.2. Sicherheit*

### 8.2.1. Anforderungen / Schutzziele

Risiken, die bei konventionellen Web-Diensten oder Services entstehen können, sind bei Cloud-Services ebenfalls zu berücksichtigen.

Zu erreichende Schutzziele sollen individuell in Abhängigkeit von Klassifizierungsstufen, Datenschutzrichtlinien und rechtlichen Aspekten definiert und in Kraft gesetzt werden. Die Festlegung und Einhaltung dieser organisatorischen und technischen Maßnahmen seitens der Anbieter, Auftraggeber und Nutzer von Cloud-Services trägt zur Gewährleistung der Informationssicherheit bei.

Cloud-basierte Dienste müssen wie andere IT-Dienste die Sicherheitsaspekte in Bezug auf Datenschutz, Informationsschutz, Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, … beachten und stehen denselben Bedrohungen gegenüber.

### 8.2.2. Datenschutz

Insbesondere im Hinblick darauf, dass die Daten unter Umständen von einem externen Dienstleister verarbeitet werden, der seinen Rechtssitz im Ausland hat, sind spezielle Vereinbarungen erforderlich. Diese Fragestellungen werden in Kapitel Rechtliche Aspekte behandelt.

### 8.2.3. Informationsschutz

Die Verarbeitung, Speicherung und Übertragung von Informationen muss derart gestaltet sein, dass die Schutzziele der zugehörigen IKT-Services eingehalten werden. Dabei sind auch die spezifischen Risiken zentralisierter Infrastruktur mit zu betrachten.

### 8.2.4. Vertraulichkeit

Informationsvertraulichkeit ist dann gegeben, wenn keine unautorisierte Informationsgewinnung möglich ist. Das erfordert die Festlegung von Berechtigungen und Kontrollen der Art, dass sichergestellt ist, dass Subjekte nicht unautorisiert Kenntnis von Informationen erlangen. Das umfasst sowohl gespeicherte Daten (data at rest), als auch Daten, die über ein Netzwerk übertragen werden (data in transit). Berechtigungen zur Verarbeitung dieser Daten müssen prinzipiell von entsprechenden Administratoren vergeben und entzogen werden können und es müssen Verfahren vorhanden sein, die eine Einhaltung dieser Rechte durchsetzen und überprüfbar machen.

Daten sollen daher zu jedem Zeitpunkt verschlüsselt übertragen bzw. ausgetauscht werden. Die Speicherung soll verschlüsselt erfolgen, um technisch das missbräuchliche Lesen von Daten zu verhindern. Dies ist insbesondere bei der Nutzung von Public Cloud erforderlich. Dies benötigt eine Infrastruktur kryptographischer Dienste, ein entsprechendes Schlüsselmanagement, sowie geeignete Kryptographie-Komponenten. Bis zu einer produktionsreifen Entwicklung der Vollverschlüsselung (Homomorphe Verschlüsselung - Berechtigte Veränderung des Inhaltes von verschlüsselten Dateien ohne diese zu entschlüsseln) bieten derzeitige Verschlüsselungssysteme und -algorithmen keinen ausreichenden Schutz für ausgelagerte sensible Daten.

Durch die CSP wird nicht immer garantiert, dass die Daten verschlüsselt auf einem Speichermedium vorliegen. In den Geschäftsbedingungen der meisten CSP gibt es keine Zusicherungen darüber, wo die Daten gespeichert werden und wie ihre Vertraulichkeit geschützt wird. Häufig ist es dem Kunden selbst überlassen, entsprechende Sicherheitsverfahren anzuwenden.

Die notwendigen Skaleneffekte eines CSP können nur durch einen sehr effizienten IT Management-Prozess erreicht werden. Aus diesem Grund muss die Administration der virtuellen Server per Zugriff 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.

Aus Optimierungsgründen haben CSP die Möglichkeit, Daten und Services auch zu anderen CSP auszulagern. Dadurch entstehen neue Abhängigkeiten und Risiken, die bewertet werden müssen.

Die Vertraulichkeit der Daten muss für den gesamten Daten-Lebenszyklus sichergestellt werden: von der Erfassung der Daten über deren Nutzung und Archivierung bis hin zum Löschen. Da die Daten in beliebigen Teilsystemen einer Cloud gehalten werden, ist nur sehr schwer nachvollziehbar, ob die ausgelagerten Daten in der Cloud vollständig gelöscht sind (Backupkopien, Replikationen beim Anbieter)

### 8.2.5. Integrität

Ein System gewährleistet die Datenintegrität, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren. Die Integrität von Daten,

Nachrichten und Informationen bezeichnet deren Unverfälschtheit bzw. Vertrauenswürdigkeit.

Dieses Ziel sollte nicht nur der Cloud-Service selbst erfüllen, sondern auch alle weiteren beteiligten Komponenten eines Cloud Computing-Systems. Der CSP ist für die Integrität des Systems und der Services vollinhaltlich verantwortlich, und soll vertraglich festgehalten werden.

Gespeicherte Daten müssen vor nicht autorisierten Manipulationen geschützt werden. Fehler in der System-Konfiguration des Anbieters können zu einer Integritätsverletzung führen.

Die Daten in Cloud Computing-Systemen sollten immer mit einer kryptografischen Prüfsumme versehen werden, wobei die Originalprüfsumme bei einem vertrauenswürdigen Dritten zum Vergleich hinterlegt werden kann. Diese sollte bei jedem Zugriff auf Daten in Cloud Computing-Systemen überprüft werden, bedeutet jedoch einen zusätzlichen Kommunikationsaufwand.

Neben der Datenintegrität sind in Cloud-Systemen auch die Softwareintegrität, Konfigurationsintegrität und Nachrichtenintegrität wichtig.

- Softwareintegrität stellt sicher, dass die eingesetzte Software, um ein Cloud Computing-System zu betreiben, intakt vom Softwarehersteller geliefert wurde und beispielsweise keine Hintertüren und ähnliche Verfälschungen aufweist.
- Konfigurationsintegrität stellt sicher, dass die Konfiguration einer Cloud-Ressource oder eines Cloud-Services nur durch autorisierte Personen geändert werden kann. Dies ist in Cloud-Systemen besonders wichtig, da meist eine Cloud-Umgebung automatisiert über Konfigurationsskripte aufgesetzt und verwaltet wird.
- Nachrichtenintegrität ist eine weitere wichtige Anforderung, die sowohl innerhalb einer Cloud als auch zwischen verschiedenen Clouds und den Systemen des Benutzers sichergestellt werden muss. Neben der Nachrichtenintegrität bedürfen auch Verwaltungs- und Steuerinformationen besonderem Schutz, da auch diese Nachrichten häufig über ein öffentliches Netzwerk transportiert werden.

### 8.2.6. Verfügbarkeit

Die Verfügbarkeit gibt an, dass Funktionen eines IKT-Services ständig bzw. innerhalb einer vorgegebenen Zeit, die von Service zu Service unterschiedlich sein kann, zur Verfügung stehen. Dazu zählen logische Schutzmaßnahmen wie Zugriffsrechte ebenso wie technische Maßnahmen wie beispielsweise Redundanzen oder auch Schutz vor gezielten Sabotageversuchen Dritter. Cloud Computing bietet den Vorteil, dass standardisierte Ressourcen dynamisch skalieren und zur Sicherstellung der Verfügbarkeit gezielt an andere Stellen der Cloud umverteilt werden können. Dabei wird die Netzwerkverfügbarkeit immer wichtiger.

### 8.2.7. Authentizität

Authentizität ist die Echtheit, Zuverlässigkeit und Glaubwürdigkeit eines Objekts. Dadurch wird sichergestellt, dass die Herkunft des Objekts zweifelsfrei nachgewiesen werden kann. Eine Möglichkeit für den Nachweis ist die digitale Signatur.

Cloud Computing bietet besonders für die IT-Sicherheit erhebliche Chancen, aber auch ungleich viel mehr Risiken. Positive Effekte sind dabei Standardisierung und Skalierbarkeit, demgegenüber stehen unter anderem die negativen Effekte wie Datenlokation, Trennung des Datenverkehrs verschiedener Nutzer, Kontrollverlust von Daten etc. Um einen

langfristigen Erfolg von Cloud Computing sicherzustellen, ist die Betrachtung kritischer Erfolgsfaktoren, allen voran das Thema Sicherheit, besonders bedeutsam.

Der Einsatz von Cloud-Services verändert traditionelle IT-Infrastrukturen. So ist die skalierbare, flexible und zentrale Bereitstellung von Sicherheitsfunktionen und Sicherheitsmaßnahmen möglich und schafft auf diese Weise die Voraussetzung zur bedarfsgesteuerten Erfüllung differenzierter Sicherheitsanforderungen – ich kann aber z.B. keine Verschlüsselung zur Anwendung bringen.

Je nach Servicemodell muss von unterschiedlichen Bedrohungsszenarien ausgegangen werden. Diese sollen in gesonderten Risikoanalysen betrachtet werden:

- Infrastruktur-Provider **(IaaS)** bieten Sicherheitsfeatures lediglich auf Hardware bzw. Infrastrukturebene an. Für das Management und die Umsetzung der darüber hinausgehenden Sicherheitsmaßnahmen ist der Kunde verantwortlich.
- Bei **PaaS** zeichnet der Anbieter für Sicherheitsfunktionen von Plattformdiensten, wie z. B. Datenbanken und Middleware, verantwortlich.
- **SaaS** Provider regeln Details der Applikationsnutzung vertraglich, beispielsweise geltende Service Level, Sicherheit und Compliance

## 8.2.8. Bedrohungen

Bedrohungsszenarien betreffen traditionelle IT-Konzepte und Cloud Computing Modelle zu gleichen Teilen. Die hier skizzierten Bedrohungen stellen die häufigsten Gefahren dar, ohne den Anspruch auf Vollständigkeit zu haben. Es muss daher im konkreten Fall eine spezifische Bedrohungsanalyse erstellt werden.

Bedrohungen werden grob in zwei Punkte eingeteilt: Daten/Informationen und Services. Daten werden nach Informationssicherheitsgesetz (InfoSiG) in Klassifizierungsstufen[5] (unklassifiziert, eingeschränkt, vertraulich, geheim, streng geheim) eingeteilt, und müssen je nach Stufe einer unterschiedlichen Behandlung zugeführt werden. Informationen, welche als z.B. geheim klassifiziert werden, sind von einer Bearbeitung in einer Public Cloud ausgeschlossen, da eine lückenlose Kontrolle des Zugriffs nicht mehr gewährleistet ist. Diese Kontrollen sind besonders im militärischen Bereich unerlässlich.

Services die von einem Cloud-Anbieter angeboten werden (XaaS), unterliegen einer ständigen potentiellen DoS-Gefahr (Denial of Service) sowie der Gefahr des unberechtigten Datenabflusses durch Dritte.

Social Engineering ist eine der größten Gefahren. Nutzer mit Administratorenrechten werden dazu verleitet, Zugangsdaten-, verfahren, o.ä. preiszugeben. Es sind Ansprechpersonen und Prozesse zu definieren, um bei einem Sicherheitsvorfall sowohl strukturierte Abläufe zu haben, als auch Zuständigkeiten abgrenzen zu können.

## 8.2.9. Trennung von verschiedenen Sicherheitsebenen

Dokumente welche nach InfoSiG klassifiziert sind, dürfen nur mehr in einer Private Cloud bzw. Community Cloud verarbeitet werden. Hierbei ist besonders zu berücksichtigen, dass die Trennung nur mehr vertraulich und geheim umfasst. Streng geheime Daten nach InfoSiV §9(2) dürfen nur mehr auf nicht vernetzten und abstrahlungsarmen Geräten verarbeitet werden.

[5] http://www.a-sit.at/de/sicherheitsbegleitung/sicherheitshandbuch/

### 8.2.10. Standards und Normen

Zurzeit sind Cloud-Service-Provider kaum nach einschlägigen Normen zertifiziert (z.B.: ISO2700X, ISO 27018, ISO 27019, BSI Grundschutz, BASEL III). Bei der Einholung von Angeboten von CSP wäre also auf derartige Zertifizierungen besonders Wert zu legen.

Auditing-/Zertifizierungsinitiativen und Tools im Cloud Bereich sind bspw.:

- CloudAudit/Cloud Controls Matrix (Cloud Security Alliance)
- StarAudit (EuroCloud)
- ISACA Cloud Computing Management Audit/Assurance Program
- NIST SP 800-53, NIST SP 800-144, SP 800-30
- Cloud Auditing Data Federation (DMTF)
- Deloitte Cloud Computing Risk Intelligence Map
- Federal Risk and Authorization Management Program - (FedRAMP)

## 8.2.11. Zusammenfassung der vorigen Punkte in der Sicherheitsmatrix

rot – hohes Risiko, orange – überschaubares Risiko, gelb – geringes Risiko

| Risikogruppe | Beschreibung des Risikos | Mögliche Maßnahmen | Public-Cloud | Trad. IT / Private-Cloud |
|---|---|---|---|---|
| Datenschutz | Interne Daten werden von einem externen Dienstleister verwendet | Untersuchung rechtliche Aspekte, vertragliche Regelungen | 🔴 | 🟡 |
| | Daten/Dienste werden an Subunternehmer weitergegeben | vertragliche Regelungen | 🔴 | 🟡 |
| Vertraulichkeit | Unautorisierte Personen greifen auf interne Informationen zu | Identitätsmanagement, Rechteverwaltung | 🔴 | 🟠 |
| | Daten werden über externe Netzwerke übertagen | Verschlüsselung, Schlüsselmanagement | 🔴 | 🟡 |
| | Zugriffe der Administratoren / Mitarbeiter des Providers | Genaue vertragliche Reglementierung | 🔴 | 🟠 |
| | Daten werden an einen Subunternehmer ausgelagert | Genaue vertragliche Reglementierung | 🔴 | 🟡 |
| | Löschung der Daten an allen Speicherorten | Genaue vertragliche Reglementierung | 🔴 | 🟡 |
| Integrität | Unbemerkte Manipulation von Daten | Kryptografische Prüfsummen | 🔴 | 🟠 |
| | Fehler in der Systemkonfiguration verändern Daten | Genaue vertragliche Reglementierung, Kryptografische Prüfsummen | 🔴 | 🔴 |
| | Die Infrastruktur des Providers enthält Hintertüren | Genaue vertragliche Reglementierung, Abwehrmaßnahmen | 🔴 | 🟡 |
| | Konfigurationsänderungen des Anbieters beeinflussen Services | Genaue vertragliche Reglementierung | 🔴 | 🟡 |
| | Verwaltungs- und Steuernachrichten werden manipuliert | Verschlüsselung, Rechteverwaltung | 🔴 | 🟠 |
| | Daten sind an unterschiedlichen geografischen Orten, und unterliegen daher auch unterschiedlichen | Genaue vertragliche Reglementierung, Verschlüsselung | 🔴 | 🟡 |
| Verfügbarkeit | Das Service steht nicht immer zur Verfügung | Rechteverwaltung<br>Abwehr von Sabotageversuchen | 🔴 | 🟠 |
| | Insolvenz des Providers | | 🔴 | 🟡 |
| | „Beschlagnahmung“ von Hardware | | 🔴 | 🟡 |
| | Verlängerte Responsezeiten von Anwendungen | Stärke Datenleitungen, genaue vertragliche Regelung | 🔴 | 🟠 |
| Authentizität | Die Echtheit eines Objektes wird nicht sichergestellt | Digitale Signatur | 🟠 | 🟠 |
| Angriffe | Serviceattacken | Sicherungsmaßnahmen | 🔴 | 🟡 |
| | Sabotageversuche | Abwehrmaßnahmen | 🔴 | 🟠 |
| | Erpressungsversuche | | 🔴 | 🟠 |
| Abhängigkeit | Abhängigkeit von einem Provider | Auf offene Standards setzen | 🔴 | 🟠 |

# 9. Prozesse (Geschäftsprozesse) – Aspekte

Cloud Computing als IT-Betriebsmodell ist nicht nur für IT-Abteilungen von Bedeutung, sondern für Unternehmen und die öffentliche Verwaltung insgesamt eine relevante Herausforderung. Durch den Einsatz von Cloud Computing kann eine ganzheitliche Änderung von Unternehmensstrategien und -strukturen erforderlich werden. Die Auslagerung von Teilen der eigenen Geschäftsprozesse an einen Dritten (CSP) ist mit signifikanten Änderungen in diesen Prozessen verbunden. Eine mögliche Folge ist die Notwendigkeit der Umverteilung von Rollen und Kompetenzen und damit Prozessen.

Die Zusammenarbeit von internen Prozessen und den Prozessen des CSP sind in einem Cloud Compliance Regelwerk (im Rahmen einer Dienstleistervereinbarung) transparent festzulegen und zu kontrollieren. Im Sinne der Aufgabendefinition und –überwachung wird auch in diesem Zusammenhang auf die Notwendigkeit des Abschlusses ausreichender Service Level Vereinbarungen (SLAs) und Operational Level Vereinbarungen (OLAs) verwiesen.

## *9.1. Strategische Aspekte der Prozessveränderung durch Cloud Computing*

Prinzipiell verfügen viele bestehende Anwendungen, auch in der öffentlichen Verwaltung, die nicht als Cloud-Service bezeichnet werden, über die typischen Anforderungen und Charakteristika von Cloud-Services (z.B. gemeinsame Nutzung von Ressourcen über Vernetzung, Lizenzgebühren statt Investitionen für die Nutzer, Standardisierung). Bestehende Erfahrungen aus der Nutzung solcher Anwendungen, speziell im Zusammenhang mit Betrieb und Datenspeicherung über einen Dienstleister und bei Anpassungen von Prozessen können auch bei der Evaluierung von potentiellen Cloud-Services genützt werden.

Standardisierung ist der wesentlichste Faktor für Kostenersparnisse beim Einsatz von Cloud Computing. Spezifische Cloud-Anwendungen sind ein Werkzeug zur effizienten Umsetzung dieser Standardisierung. Gerade Public Cloud-Service unterliegen einem sehr hohen Standardisierungszwang, der bei einem Private Cloud-Service nicht immer gegeben ist. Entsprechend dem Grad der Standardisierung der gewählten Cloud-Lösung ist mit Änderungen in den Geschäftsprozessen und unterschiedlichen Kosten und Finanzierungsrisiken zu rechnen. Bei einem Einsatz von Cloud-Services unterschiedlicher Dienstleister muss Interoperabilität zur Sicherstellung der Unabhängigkeit von einem bestimmten Anbieter in den Prozessen berücksichtigt werden. Bei Nutzung standardisierter Cloud-Lösungen sollte durch den flexiblen Einsatz von Rechenleistung schnell auf Änderungen in den Geschäftsprozessen reagiert werden können.

Compliance- und Governance-Prozesse werden in Unternehmen und der öffentlichen Verwaltung mit steigendem Einsatz von Cloud-Services externer Dienstleister durch die Notwendigkeit der Sicherstellung und Kontrolle der Einhaltung von Datensicherheit und Rechtskonformität an Bedeutung gewinnen. Neben der gründlichen Ausarbeitung von SLAs zur Abdeckung der Anforderungen bei der Nutzung eines Cloud-Services müssen auch die dazugehörigen Kontrollprozesse ausreichend definiert und umgesetzt werden.

## *9.2. Cloud Compliance*

Das hohe Maß an Abhängigkeit zwischen Cloud Anbietern und Nutzern und die dadurch verzahnten Prozesse und Verantwortlichkeiten erfordern ein stabiles Regelwerk, das vielfach unter „Cloud Compliance“ [BITK10] zusammengefasst wird. Cloud Compliance hat zum Ziel, Transparenz und Sicherheit für alle Anspruchsgruppen (Stakeholder) zu schaffen und bietet damit eine wichtige Basis, um alle Vorteile von Cloud Computing für Anbieter, Nutzer und Provider vollumfänglich nutzbar zu machen.

Der Begriff Cloud Compliance bezeichnet die nachweisbare Einhaltung von Regeln zur Nutzung oder Bereitstellung von Cloud Computing. Zur Bestätigung der Cloud Compliance können sich Anbieter zertifizieren lassen. Zu den verschiedenen Zertifikaten/Gütesiegeln zählen das Gütesiegel SaaS von EuroCloud, Trusted Cloud, CSA STAR, TÜV Trust IT und das IT-Grundschutz-Zertifikat des BSI. Eine Zertifizierung allein reicht jedoch nicht für eine abschließende Beurteilung eines Cloud-Anbieters oder –Angebots in Hinblick auf die Anforderungen der Cloud Compliance aus.

Die berücksichtigten Kriterien sind vom Zertifikat abhängig und können sich von den Kriterien für die Verwaltung bzw. den konkreten Anwendungsfall unterscheiden.

# 10. Potentielle Anwendungen für RZ-, Private Cloud und Public Cloud (Kategorie A, B, …)

Anwendungen für Cloud Computing werden in durchaus unterschiedlicher Weise in den Studien diskutiert:

- Zum einen sind es die unter größtem Anbieter-Druck der Marktführer (Microsoft, Google, Amazon, IBM, etc.) am Markt platzierten Standardservices wie virtuelle Server, Storage, Mailboxen, Collaboration Services primär für Private wie für kleinere und mittlere Unternehmen, die als aussichtsreichste Domain von Cloud Computing gelten. Für diese Services werden auch Business Modelle mit hohem Kostenersparnispotential gerechnet und präsentiert.
- Zum anderen führt die Standardisierungsnotwendigkeit für Cloud Computing dazu, dass spezialisierte Applikationen und Services sowie Prozessoptimierungen in der Nutzung und Steuerung von IT-Services eher weniger sinnvoll in einer Cloud und hier wiederum insbesondere kaum in einer Public Cloud angesiedelt werden. Dies gilt vor allem für Großunternehmen.

## *10.1. Entscheidungskriterien zur Auswahl von Cloud-affinen Anwendungen / Services*

Für Forrester [FORR] spannen die beiden Parameter „Level of Sharing“ und „Business-Value“ den wichtigsten Entscheidungsraum auf, der „Cloud-affine“ und „Cloud-averse“ Applikationen trennt. Neben der Identifikation eines Services als „grundsätzlich Cloud-geeignet“ ist auch die Organisationsform der Cloud Nutzung zwischen Private und Public zu entscheiden. Hier zeigt sich nach [BITK10] eine Abhängigkeit von der Unternehmensgröße:

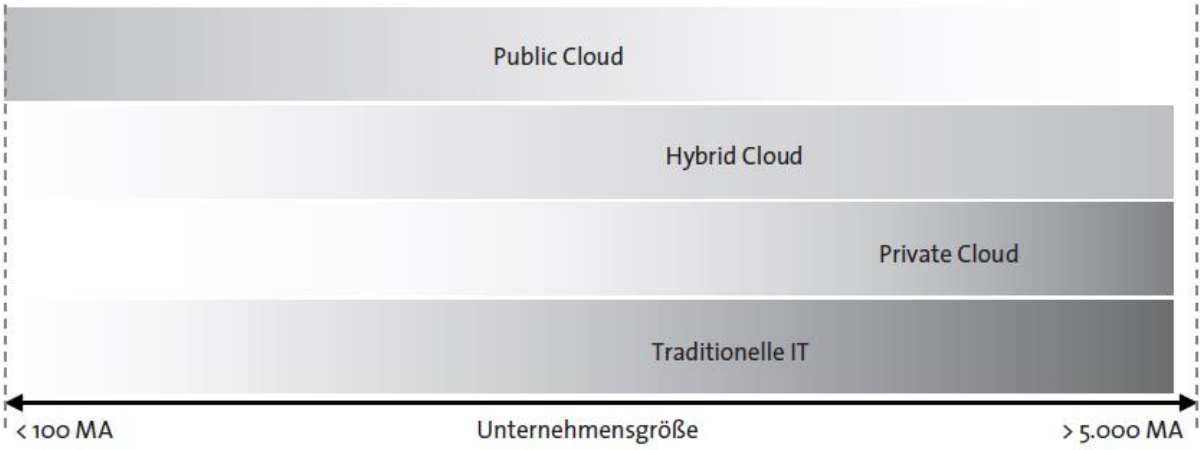


Abbildung 3: Nutzungsschwerpunkte – Typen von Clouds – Unternehmensgrößen

**Abbildung 3: Nutzungsschwerpunkte – Typen von Clouds - Unternehmensgrößen**

Unbedingt zu beachten ist, dass die Betrachtung der Unternehmensgröße nur einen einzigen Parameter in einer Vielzahl von Entscheidungsparametern darstellt. So sind für die Verwaltung strategische Überlegungen und Sicherheitsverpflichtungen unter Umständen wesentlicher als in der Wirtschaft für die Entscheidung **„Was ist auslagerbar und was nicht?**“ - dieser Punkt verdient generell hohe Bedeutung (z.B. kann in einer Hybriden Architektur die ‚Cloud' auch das Ausfallrechenzentrum im Desaster Fall sein.

Zusätzliche Parameter zur Auswahl der geeigneten Cloud-Organisationsform bietet z.B. [BITK10] in der folgenden Bewertungsstruktur an:

| 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

**Abbildung 5: Bewertung der Cloud-Typen**

Die Integrationsfähigkeit von Cloudservices in eine Gesamtorganisation und Gesamt-IT-Landschaft ist eine der wesentlichsten Entscheidungskriterien. Dies wird durch das Ergebnis einer von Forrester präsentierten Umfrage unterstrichen, die bei jenen Entscheidungsträgern, die bereits mit Cloud-Services vertraut sind, das Thema „Integration“ als größte Herausforderung identifiziert hat.

Die Herausforderung der Gesamtoptimierung darf auch bei scheinbar simplen Applikationen nicht unterschätzt werden. Einen sehr interessanten Hinweis liefert dazu die Gartner Studie „Can E-mail Be a Utility?“, die in Q4 2010 Großunternehmen und Organisationen der öffentlichen Hand befragte. Die zentrale Empfehlung dieser Studie spricht sich aus Integrationsgründen gegen ein voll standardisiertes eMail-Service für Großunternehmen aus:

*Do Not Treat E-mail as a Utility:*

*In the enterprise, e-mail is a critical communications channel. Treating e-mail as a utility is part of the siren song of SaaS e-mail, but the reality is that for most enterprises, following this song will lead into the rocks. E-mail, for most enterprises, is significantly more complex than a utility. E-mail requires numerous moving parts and integrations*.

Einen wichtigen Spezialfall stellt die Nutzung von Cloud Computing für Desktop-Services (z.B. Office, …) dar: 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. (BITKOM)

## *10.2. Mögliche Cloud Services im Behördenbereich*

Die Studie „E-Government und Cloud Services“ gibt exemplarisch Anregungen für mögliche Cloud Services im Umfeld öffentlicher Behörden, welche in den folgenden Paragraphen zitiert sind:

- **Infrastructure-as-a-Service (IaaS):**
  - Archivierung von Daten
  - Backup von Daten
  - Rechenleistung und Speicherbedarf
  - Virtuelle Server

- **Platform-as-a-Service (PaaS):**
  - Plattform für das Abbilden von behördeninternen und/oder bürgerorientierten Prozessen (eFormularen)
  - Plattform zum einfachen Erstellen von Web-Applikationen; diese Plattform bindet über einfache Module (APIs) die E-Government Infrastruktur mit ein (z.B. Zustellung, Payment, Bürgerkarte, SZRServices, etc.)
  - Datenbanken

- **Software-as-a-Service (SaaS):**
  - Desktop-Software der öffentlichen Verwaltung wird als cloudbasierter Dienst angeboten – Zugriff erfolgt bspw. über Web-Browser.
  - Workflow Management System, wie bspw. elektronische Aktensysteme.
  - Collaboration Suite
  - Identity-Management-as-a-Service: die Bürgerkartenanmeldung wird nach dem Muster eines Identity Providers als „zentrale“ Infrastruktur angeboten.
  - Security-as-a-Service: Mail-Filter (Filtern auf SPAM und Malware etc.) kann performant als Cloud-basierter Dienst angeboten werden.“

## *10.3. Analyse-Logik für die Auswahl von Services, die in eine Cloud-Form migriert werden können*

Völlig generell spiegeln (auch nach der Fraunhofer Cloud Studie) die vier Bestimmungsfaktoren-Gruppen für das Outsourcing von Leistungen

- rechtliche Aspekte (siehe dazu Kapitel 4),
- (wirtschaftliche) Vorteilhaftigkeit,
- Steuerbarkeit und
- Risikobeherrschbarkeit

die Gestaltungs- bzw. Handlungsebenen wider, die für Entscheidungen öffentlicher Institutionen über die Nutzung von Cloud Computing relevant sind.

Unter Berücksichtigung dieser generellen Grundsätze und der diskutierten Vor- und Nachteile von Cloud-Services bietet sich die Entscheidungsmatrix (siehe Anhang) für die Erprobung und Adoption von Cloud-Services im öffentlichen Dienst an.

Zum Beispiel sind IaaS und PaaS für Test- und Entwicklungsserver sowohl für Private wie für Public Cloud Lösungen die am einfachsten einzuführenden Services (allerdings immer unter der Gesamtbetrachtung der Sinnhaftigkeit, Wirtschaftlichkeit und der verwendeten Testdaten). Ein anderes Beispiel wäre die öffentliche Publikation von unkritischen Daten/Inhalten über das Internet: Auch hier könnten IaaS oder PaaS Cloud Services genutzt werden.

Vertikale Services mit Cloud Potential bzw. mit bereits Cloud-ähnlicher Realisierung wie SAP HV oder SAP PV können auf ihre technische Realisierung hin überprüft werden: Sind alle technischen Trends moderner Cloud Services sinnvoll aufgenommen?

Horizontale branchenunabhängige Service Kandidaten bedürfen der Evaluierung auf Integrationsbedarf, um bestehende Service-Integrationen und Prozessoptimierungen nicht zu verlieren und sie bedürfen einer politischen Willensbildung, ob sie „betriebskritisch“ für die jeweilige Behörde sind und auf Grund dieser Kritikalität ein Auslagern zu einem bestimmten Public oder Private Cloud Anbieter politisch erwünscht ist.

Allen Varianten gemeinsam ist die nötige kritische Gesamtkostenbeurteilung zur letztgültigen Entscheidungsfindung, ob ein Cloud Service sinnvoll genutzt werden kann oder eben nicht.

Ergänzend zu dieser Logik konnten in den Studien hilfreiche Fragen zur Entscheidungsfindung gefunden werden wie 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?

# 11. Gesamtbeurteilung

Der technische Ansatz Cloud Computing kann als ‚massive Standardisierung charakterisiert werden

Cloud Computing ist keine Modeerscheinung der IKT-Branche, sondern vereint als nächsten Entwicklungsschritt die technischen und wirtschaftlichen Möglichkeiten, die konsequente Standardisierung bedingt. Daher erfordert diese Entwicklung massive Maßnahmen im rechtlichen und organisatorischen Bereich.

Die IT-Industrie drängt aufgrund eines klaren Businessmodells zum Einsatz von Cloud Computing und sieht damit eine Forcierung des Rollouts von E-Services. Durch geringere Einstiegshürden in Bezug auf Zeit und Ressourcen erhofft man sich ein erhöhtes Nutzungsvolumen der Public Cloud und damit höhere Gewinne.

Vor dem Einsatz muss man dennoch einige Punkte bedenken. Je nach gewähltem Modell (Private Cloud, Public Cloud, Hybrid Cloud) stellen sich die Auswirkungen des Veränderungsprozesses unterschiedlich dar. Im nächsten Kapitel sind alle Fragestellungen aus Sicht des Auftraggebers, die in dem Positionspapier identifiziert wurden, zusammengefasst.

Der Cloud-Monitor hat 2015 bereits das vierte Jahr die Cloud-Nutzung von deutschen Unternehmen betrachtet. Folgende vier zentrale Erkenntnisse aus Anwendersicht wurden gezogen: Die Cloud-Nutzung steigt langsam, aber stetig. Private Clouds sind das bevorzugte Modell. Die Erfahrung mit Cloud-Computing ist überwiegend positiv. Sicherheitsbedenken und rechtliche Unklarheiten bremsen die Marktdynamik. Aufgrund fehlender Statistiken im Verwaltungsumfeld sind diese Erkenntnisse die beste Orientierung für die Entwicklung von Cloud in der Verwaltung.

Ein Strategiestatement für eine gemeinsame Verwaltungscloud bzw. gemeinsamen Cloud-Lösungen ist zu erstellen (Bund / Länder getrennt / gemeinsam, D-A-CH Cloud, EU-Initiativen, EU Cloud Large Scale Pilot).

Ähnlich dem Modell Portal-Verbund sollten künftige Entwicklungen im Hinblick auf den Investitionsschutz "Cloud-fähig" umgesetzt werden. Damit ist die Entscheidung, ob der Betrieb eines IT-Services in der Cloud oder klassisch im Rechenzentrum erfolgt, offen und kann jederzeit getroffen werden. Standardisierungen sollen der Cloud-Fähigkeit nicht entgegenstehen. Die Erkenntnisse aus diesem Dokument sind zu berücksichtigen.

# 12. Entscheidungsfindungsprozess

Bevor man eine Entscheidung für die Nutzung von Cloud Computing trifft oder ein spezielles Modell auswählt, muss man in der Verwaltung die erforderlichen Grundlagen schaffen. In diesem Zusammenhang sind jedenfalls folgende Punkte zu klären:

| Organisatorische Anforderungen |
|---|
| Ab wann ist eine IT-Anwendung zu geschäftskritisch, um in die Cloud ausgelagert zu werden? Wann ist der Schwellenwert für Ausfallzeiten erreicht? |
| Welche Daten disqualifizieren eine IT-Anwendung aufgrund der besonderen Sensitivität? |
| Welche Risiken sind für eine Organisation aufgrund von Service-Ausfällen tragbar? |
| Hat eine IT-Anwendung zu viele Abhängigkeiten um sinnvoll in eine Cloud ausgelagert zu werden? |
| Was ist der maximal tolerierbare Aufwand für die Migration eines Verfahrens in die Cloud? Steht dies in Verhältnis zu den erwarteten Einsparungen? |
| Wie hoch ist die Dauer des Return on Investment inkl. der Transitionskosten? |

| Rechtliche Anforderungen |
|---|
| Werden personenbezogene Daten verwendet? |
| |
| Werden die Daten ausschließlich im europäischen Wirtschaftsraum oder in Ländern, die in der Datenschutzangemessenheits-Verordnung angeführt sind, verarbeitet? |
| Werden Subauftragnehmer beauftragt und gilt für diese Gleiches wie für den Dienstleister? |
| Stellt der Dienstleister die Maßnahmen zur Datensicherheit gemäß § 14 DSG 2000 sicher? |
| Trifft der Dienstleister insbesondere Maßnahmen zum Schutz vor zufälliger und unrechtmäßiger Zerstörung? |
| Trifft der Dienstleister insbesondere Maßnahmen gegen den Verlust oder unbefugtem Zugriff auf die Daten? |
| Trifft der Dienstleister insbesondere Maßnahmen zur Protokollierung der Zugriffe? |
| Ist sowohl die Einsichtnahme als auch die Richtigstellung bzw. das Löschen der Daten der Betroffenen in der Cloud gemäß den rechtlichen Vorgaben gewährleistet und durchführbar? |
| Gibt es ein Regelwerk das das Verfahren zur Wahrung der Rechte der Betroffenen in einem Informationsverbundsystem klar regelt? |
| |
| Gibt es ein Regelwerk zur Umsetzung der Skartierung von Daten (Retention-Policy)? |
| Gibt es ein Regelwerk zur Skartierung von Protokolldaten einschließlich Verkehrs- und Metadaten? |
| Werden die Daten tatsächlich gelöscht (und nicht nur die Zugriffsrechte entzogen)? |
| Ist dabei sichergestellt, dass keine Kopien der Daten (z.B. Back-Up) erhalten bleiben? |
| Gibt es ein Regelwerk, wonach die Zurückstellung (inkl. Löschung der Daten beim CSP) an den Auftraggeber nach Beendigung des Vertragsverhältnisses erfolgt? |
| |
| Ist bei Datenschutzverletzungen ein Meldeprozess bei Auftraggeber und Dienstleister etabliert? |
| Können innerstaatliche Auskunftspflichten gegenüber österreichischen Strafverfolgungsbehörden erfüllt werden? |

| Technische Anforderungen |
| --- |
| Werden die im Einsatz befindlichen Schnittstellen unterstützt? |
| Werden starke Identifizierungsverfahren für Cloud Kunden und Administratoren genutzt? |
| Ist eine durchgängige Sicherheitsarchitektur implementiert? |
| Können die für die Umsetzung der eigenen Sicherheitspolitik benötigten Zugriffe (z.B. Log Dateien, Zugriffslisten) gewährt werden? |
| Können Patches getestet werden und aus Kompatibilitätsgründen zurückgehalten werden? |
| Stellen kryptografische Methoden die Integrität der Daten sicher? |
| Welche Verfügbarkeiten können garantiert werden? |
| Wie skaliert die Cloud-Lösung? |
| Wie wird der Wechsel von einem Cloud-Anbieter zu einem anderen ermöglicht? |

# A. Revision History

| Version | Datum | Autor(en) | |
|---|---|---|---|
| 1.0.0 | 4.17.2011 | Peter Reichstädter (BKA) | Erstellt |
| 1.0.1 | 28.02.2012 | Peter Reichstädter (BKA) | Umformatierung auf neue CI Layout-Style<br><br>Sprachliche Detaillierungen bzw. editorielle Ergänzungen |
| 1.1.1 | 04.03.2016 | Gregor Eibl (BKA) | Erste Aktualisierungen, Tausch des Kapitel 4 mit der rechtlichen Checkliste der AG Resi |
| 1.1.2 | 04.11.2016 | Gregor Eibl (BKA) | Konsolidierung der Anmerkungen der eingelangten Änderungsvorschläge |
| 1.1.3 | 7.11.2016 | Gregor Eibl (BKA) | Anmerkungen der Cloud-AG wurden eingearbeitet |

# B. Referenzen


| | |
|---|---|
| [BITK10] | BITKOM-Leitfaden-CloudComputing_Web<br><br>Cloud Computing – „Was Entscheider wissen müssen“, BITKOM, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., Albrechtstraße 10 A, 10117 Berlin-Mitte, Dr. Mathias Weber, Arbeitskreis Cloud Computing und Outsourcing, www.bitkom.org, bitkom@bitkom.org, 2010 |
| [CCIS10] | Cloud Computing in Schweizer Behörden<br><br>„Vorstudie zu Cloud Computing in Schweizer Behörden“, Heck Uwe, Müller Willy, Oktober 2010 |
| [ECON10] | EU Public Sector Cloud Economics<br><br>„THE ECONOMICS OF THE CLOUD FOR THE EU PUBLIC SECTOR“, Microsoft, Rolf Harms (rolfh@microsoft.com) or Michael Yamartino (michael.yamartino@microsoft.com), November 2010 |
| [EGCC10] | E-Government und Cloud Computing<br><br>„E-Government und Cloud Computing“, E-Government Innovationszentrum, Dr. Thomas Rössler, thomas.roessler@egiz.gv.at, https://demo.egiz.gv.at/plain/content/download/678/3913/file/E-Government%20und%20 Cloud Computing.pdf, September 2010 |
| [SRGC11] | Security and Resilience in Governmental Clouds<br><br>„Security and Resilience in Governmental Clouds – Making an informed decision“, ENISA, Catteddu Daniele, Jänner 2011 |
| [WKIC10] | Wer klaut in der Cloud<br><br>„Wer klaut in der Cloud – Chancen und Risiken des Cloud Computing“, Detecon Consulting, Juli 2010 |
| [DHRA10] | Der Himmel reißt auf<br><br>“Der Himmel reißt auf” Thorsten Claus, Martin Jeske, Detecon Consulting, Februar 2010 |
| [SWIS10] | Messmer_IT-Trends<br><br>“IT Megatrends und Ihre Bedeutung für Geschäft und Gesellschaft” Bruno Messmer, Swisscom IT Services AG, September 2010 |

| | |
|---|---|
| [CCMA10] | Cloud_Computing_Mindestsicherheitsanforderungen<br><br>„BSI-Mindestsicherheitsanforderungen an Cloud Computing-Anbieter“ Bundesamt für Sicherheit in der Informationstechnik, Bonn, E-Mail: cloudsecurity@bsi.bund.de, September 2010 |
| [TVSR10] | kuppinger_ca_virtualization_security_report<br><br>„CA Technologies Virtualization Security“, Martin Kuppinger, KuppingerCole, service@kuppingercole.com, 2010 |
| [GITC10] | government_in_the_clouds_200519<br><br>„Government in the Clouds“, GARTNER Industry Research, Andrea Di Maio, Massimiliano Claps, Mai 2010 |
| [CCÖV10] | Fraunhofer cloud_studie_vorabversion_20101129<br><br>„Cloud Computing für die öffentliche Verwaltung“, ISPRAT-Studie, Dr. Peter H. Deussen, peter.deussen@fokus.fraunhofer.de, November 2010, |
| [BSCA10] | BURTON GROUP - Building a Solid Cloud Adoption Strategy: Success by Design<br><br>“Building a Solid Cloud Adoption Strategy: Success by Design”, Drue Reeves, dreeves@burtongroup.com, Mai 2010 |
| [CCTR10] | BURTON GROUP - Cloud Computing: Transforming IT<br><br>Cloud Computing: Transforming IT, Drue Reeves, dreeves@burtongroup.com, April 2010 |
| [CCSE09] | BURTON GROUP - Computing Security in the Enterprise<br><br>Cloud Computing Security in the Enterprise Cloud, Dan Blum, dblum@burtongroup.com, Juli 2009 |
| [DCCS10] | BURTON GROUP - Developing a Cloud Computing Security Strategy<br><br>“Developing a Cloud Computing Security Strategy”, Dan Blum, dblum@burtongroup.com, Mai 2010 |
| [PCEC09] | BURTON GROUP - Planning Considerations for Externalization and Cloud Computing<br><br>Planning Considerations for Externalization and Cloud Computing, Mike Rollings, mrollings@burtongroup.com, Oktober 2009 |

| | |
|---|---|
| [DSCC10] | BURTON GROUP - The Dark Side of Cloud Computing<br><br>“The Dark Side of Cloud Computing”, Drue Reeves, dreeves@burtongroup.com, Mai 2010 |
| [SDCC10] | BURTON GROUP - Using Encryption to Protect Sensitive Data in Cloud Computing Environments<br><br>“Using Encryption to Protect Sensitive Data in Cloud Computing Environments”, Dan Blum, dblum@burtongroup.com, Mai 2010 |
| [MACC10] | BSI Mindestanforderungen Cloud Computing - ENTWURF – 20100927<br><br>“BSI-Mindestsicherheitsanforderungen an Cloud Computing-Anbieter“, Bundesamt für Sicherheit in der Informationstechnik, cloudsecurity@bsi.bund.de, September 2010 |
| [CCSR] | ENISA Cloud Computing Security Risk Assessment<br><br>„Cloud Computing“, ENISA, Daniele Catteddu and Giles Hogben , Daniele.catteddu@enisa.europa.eu, giles.hogben@enisa.europa.eu, November 2009 |
| [CCDS] | Cloud Computing und Datenschutz<br><br>T. Weichert: Cloud Computing und Datenschutz, Unabhängiges Landeszentrum für Datenschutz Schleswig-Hohlstein. Abgerufen aus dem WWW am 15. Februar 2011 unter http://www.datenschutzzentrum.de/ Cloud Computing |
| [LCCR] | Leitfaden Cloud Computing Recht, Datenschutz & Compliance<br><br>EuroCloud Deutschland_eco e. V., Leitfaden Cloud Computing Recht, Datenschutz & Compliance, 22-27. abrufbar unter http://www.eurocloud.de/dokument/ |