# …und jetzt wird es cloudy…

**Angela Espinosa**
**Deutsche Lufthansa AG**
**Frankfurt am Main**

**Schlüsselworte**
Cloud, Security, Stakeholder, SaaS, IaaS, PaaS, Compliance, Strategie

**Kurzbeschreibung**
Dieser Vortrag betrachtet das Thema Cloud. Ein Thema, das alle Unternehmen in gewisser Weise bewegt. Doch wie geht man es an? Was ist Cloud? Ist das eher schlecht oder gut? Welche Vorteile gibt es, was muss man bedenken, wenn man in eine Cloud geht und Unternehmensdaten dort ablegt. Darf man das überhaupt?

**Einleitung**
Die fortschreitende Mobilität und Flexibilität im privaten Bereich hält nun auch Einzug in die Fachabteilungen der Unternehmen. Der Kunde steht immer mehr im digitalen Fokus. Denn hier steigt die Erwartungshaltung an die Unternehmen, ein durchgängiges digitales Erlebnis und individualisierte Services für den Kunden zu erschaffen und damit die Kundenbindung zu stärken. Durch die Mobilität werden zusätzlich eine Menge an Daten erzeugt, die es zu verarbeiten gilt.

Fachabteilungen befinden sich in Innovationszwang. Auch die Hersteller reagieren auf diese Veränderung und „zwingen“ die Unternehmen durch Kosten- und Lizenzeinsparungen, Entwicklung und Weiterentwicklung von „Cloud“-Softwaren zunehmend in die Cloud.

Zusätzlich kommt hinzu, dass Unternehmen deren Kerngeschäft nicht die IT ist, aber die Geschäftsprozesse durch IT gestützt werden, sich nicht immer leisten können, ein eigenes Rechenzentrum aufzubauen oder zu mieten. Eine Cloud-Lösung bietet den Vorteil, Kosten für Hardware, Software, Infrastruktur und deren Administration zu sparen. Ressourcen und Services werden nach Nutzen bezahlt und können flexibel hinzugebucht werden. Außerdem kann man Applikationen in aller Welt verfügbar machen und Latenzzeiten verringern, wenn der Cloud Anbieter weltweit mi Rechenzentren vertreten ist. Der Cloud Anbieter kümmert sich auch darum, Hard- und Software aktuell zu halten. Verfügbarkeiten (SLAs) sollte man vereinbaren, jedoch werden Pönale Zahlungen oft als weitere Nutzungszeit zugestanden.

Vor einer Prüfung des Cloud Dienstes weiß man nicht, wo die Daten gespeichert und verarbeitet werden. Eine Prüfung kann allemal mittels Zertifikaten und SOC2 Berichten erfolgen, denn meist ist es sehr schwierig bis gar nicht möglich das Auditrecht beim Cloud Anbieter durchzusetzen.
Als Unternehmen begibt man sich in die Abhängigkeit eines Cloud Anbieters. Daten hineinzupumpen ist leicht getan, aber diese bei Insolvenz des Anbieters oder Unzufriedenheit mit dem Anbieter wieder herauszubekommen und zu einem anderen Anbieter zu migrieren ist fragwürdig. Gigabyte von Daten als csv-Datei ausgeliefert zu erhalten, bringt nicht wirklich viel Spaß. Zudem kann es vorkommen, dass die Daten ohne die Software gar nicht verwendbar sind. Der zentralisierte Ansatz wirkt sich zwar positiv auf die Nachhaltigkeit (Umweltbilanz) aus, jedoch sind meist mehrere Unternehmen bei dem gleichen Cloud Anbieter und damit sind bei Ausfall viele betroffen. Solche Ausfälle können auch zu Datenverlusten führen. Ein Cloud Anbieter versucht so weit wie möglich standardisiert zu arbeiten. Dabei geht ein Stück weit Flexibilität verloren, die man ggf. als Unternehmen braucht.

Wenn Unternehmen respektive Fachabteilungen auf die Idee kommen, Cloud Dienste zu nutzen, sollte dies kontrolliert geschehen. Dafür sind einige Stakeholder und Rahmenbedingungen notwendig, um entscheiden zu können, ob der Dienst in Frage kommt, genutzt werden darf oder nicht.

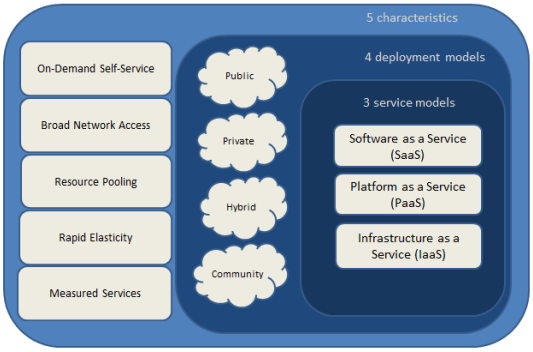
Erstmal angefangen damit, was Cloud bedeuten kann…

## Was ist überhaupt dieses Cloud?

Das NIST (National Institute of Standards and Technology) beschreibt Cloud Services durch fünf charakteristische Merkmale, vier Nutzungsmodelle und drei Servicekategorien.

## Cloud Computing Charakteristiken

Cloud Computing ermöglicht es den Cloud-Kunden, Ressourcen selbstständig zu bestellen (On-Demand Self-Service). Der Kunde soll von verschiedenen Endgeräten aus auf ein Netz zugreifen können, das die benötigten Dienste bereitstellt (Broad Network Access). Die Ressourcen werden „gepoolt“ und multimandantenfähig zur Verfügung gestellt (Resource Pooling).




Der Kunde kennt erstmal weder die spezifische Lokation der Ressourcen noch hat er die Kontrolle darüber. Entsprechend den Anforderungen der Anwendungen können die Ressourcen „elastisch“ zeitnah hoch oder herunter skaliert werden (Rapid Elasticity). Um die nutzungsabhängige Abrechnung möglich zu machen, wird ein Dienst angeboten, der die automatische Kontrolle und Optimierung der genutzten Ressourcen enthält (Measured Services).

## Nutzungsmodelle

Vier Nutzungsmodelle werden hier unterschieden.

### Private Cloud

Die Infrastruktur für eine **private Cloud** ist exklusiv für eine einzige Organisation vorgesehen, die aber mehrere Nutzer umfasst. Physikalisch kann eine private Cloud entweder direkt im Unternehmen angesiedelt sein, oder aber als virtuelle private Cloud (VPC) vom Betreiber realisiert sein. In der virtuellen Lösung des Betreibers werden die Server „logisch isoliert“ von den öffentlichen Servern betrieben und exklusiv von dem einen Kunden genutzt.

### Public Cloud

**Public Cloud**s sind geteilte Infrastruktur Plattformen, die von Dritten betrieben werden und größere Kosteneinsparungen darstellen. Aber da Daten in einer öffentlichen Cloud auf vielen physikalischen Orten gespeichert sein können, wird der Kunde gezwungen eventuell Ressourcen mit anderen Kunden zu teilen.

Öffentliche Cloud Services können kostenlos oder nach einem pay-per-usage Modell angeboten werden. Aus Sicherheitssicht sind meist gravierende Unterschiede zu Private Clouds bei den Services (Anwendungen, Speicher oder andere Ressourcen) feststellbar.

#### Community Cloud

Eine **Community Cloud** ist eine Mehrbenutzer Plattform die es mehreren Unternehmen erlaubt auf der gleichen Plattform zusammenzuarbeiten, vorausgesetzt dass sie gleiche Bedürfnisse und Einschränkungen haben. Es ist vergleichbar mit einer öffentlichen Cloud Umgebung, aber mit festen Ebenen von Sicherheit, Privatsphäre und sogar behördlicher Compliance einer privaten Cloud.

#### Hybride Cloud

Eine **hybride Cloud** Infrastruktur ist ein Zusammenschluss von zwei oder mehreren Cloud Infrastrukturen (Privat, Community oder Öffentlich), die zwar eindeutige Instanzen bleiben aber integriert sind um das Beste aus allen Welten zu bekommen. Zum Beispiel erlaubt der hybride Ansatz einem Unternehmen, den Vorteil der Skalierbarkeit und Kosteneffizienz einer öffentlichen Cloud Umgebung zu nutzen, ohne dabei geschäftskritische Anwendungen und Daten an dritte zu entblößen.

Damit eine solche Lösung effektiv sein kann, muss eine Management Strategie für einen hybriden Cloud Einsatz die Punkte Konfigurationsmanagement, Change Control, Sicherheit, Fehlermanagement und Kostengestaltung umfassen.

### Servicekategorien

NIST definiert drei Servicekategorien (Fertigungstiefen).

#### Software as a Service (SaaS)

Hierunter fallen sämtliche Anwendungen, die den Kriterien des Cloud Computing entsprechen. Dem Benutzer wird der Zugang zu den Applikationen und Datenbanken durch das Internet bereitgestellt. Typische Standard-Anwendungen sind ERP, CRM und Backoffice. Die Provider verwalten und betreiben die Infrastruktur und die Plattformen auf denen die Anwendungen laufen. Beispiele dafür sind: Office365, Oracle Marketing Cloud, Salesforce, uvm.

#### Platform as a Service (PaaS)

Der Cloud Service Provider (CSP) stellt in diesem Modell eine komplette Infrastruktur bereit und bietet dem Kunden auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So können dort Software Lösungen bereitgestellt werden, ohne Kosten und Komplexität für die Anschaffung und Verwaltung der zu Grunde liegenden Hard- und Software. Beispiele sind hier die Datenbanken, Entwicklungsumgebungen, etc.

#### Infrastructure as a Service (IaaS)

In diesem (Basis) Modell werden IT-Ressourcen wie z.B. Rechenleistung, Datenspeicher oder Netze als Dienst angeboten. So werden auf einer virtuellen Operating Plattform mehrere Gast-Betriebssysteme zur Verfügung gestellt, die sich die virtualisierten Hardware Ressourcen teilen. Um die Anwendungen zu nutzen, können Cloud Kunden die Betriebssystem Images und die Anwendungssoftware auf der Cloud Infrastruktur installieren. Beispiele für dieses Modell sind: Amazon Webservices, Microsoft Azure IaaS.

**Stakeholder**

Mit welchen Stakeholdern hat man es beim Cloud-Thema zu tun.

Hersteller
Die Hersteller oder auch Cloud Service Provider zwingen die Kunden durch Lizenzänderungen (Kostenanpassungen) und Weiterentwicklungen von Cloud-Softwaren dazu, umzudenken.

Cloud Service Provider
Diesen Stakeholder wird es immer geben. Er stellt immer das Infrastrukturfundament bereit. Das heißt, Gedanken um die Hardwarelösung muss man sich als Kunde keine mehr machen. Die ganzen Themen, die sich darum ranken, Rechenzentrum, Strom, Brandschutz, Alarmanlage, Netzwerkinfrastruktur, Orchestrierung der Ressourcen werden durch den Cloud Service Provider übernommen.

Managed Service Provider
Je nach Konstrukt der Cloud Anwendung, kann es sein, dass noch ein weiterer Player ins Spielfeld tritt. Er kümmert sich um die Wartung/Betrieb der Ressourcen, die in der IaaS Lösung beispielsweise aufgebaut werden. In einer PaaS oder SaaS Welt, würde sich der MSP als Integrator und Administrator präsentieren.

Der Fachbereich, kleine Unternehmen
Dieser Stakeholder möchte den Kundenanforderungen gerecht werden. Die digitale Business Transformation zwingt ihn dazu flexibel und zukunftsfähig zu bleiben, damit auch unnötige Kosten für Infrastruktur und Hardware einzusparen.

Einkauf
Im Einkauf werden die Verträge mit den Cloud Anbietern also CSP und/oder MSP geschlossen.

DSB Datenschutzbeauftragter
Für jede Cloud Dienst Betrachtung ist der Datenschutzbeauftragte hinzuzuziehen, um Compliance Fragen hinsichtlich des Datenschutzes sicherzustellen. Es kann sein, dass Auftragsdatenverarbeitungen abgeschlossen werden müssen.

ISO Information Security Officer oder Sicherheitsexperte
Der ISO ist daran interessiert, dass die Compliance- und Sicherheitsregeln des Unternehmens auch in Cloud-Diensten abgebildet werden können. Falls nicht, muss entschieden werden, ob bestimmte Risiken für das Unternehmen tragbar sind oder nicht.

Lieferanten des Managed oder Cloud Service Provider
Diese Gruppe ist vor allem für Compliance Themen wichtig zu kennen und zu verstehen. Zum Beispiel fordert das BDSG, dass alle Lieferanten bekannt sein müssen und ggf. ADVen mit denjenigen geschlossen werden.

Betriebsratsgremien in großen Firmen
In großen Firmen gibt es die Betriebsräte, die in wichtige Entscheidungen einbezogen werden. Wenn man also mit offenen Karten spielt und auch diese Stakeholder einfängt, kann man das Spiel eventuell gewinnen.

**Datenklassifizierung**

Welche Daten kommen überhaupt in Frage, um in einer Cloud Umgebung verarbeitet oder gespeichert zu werden.

Dafür muss sich das Bewusstsein entwickeln, wie Daten im Unternehmen zu klassifizieren sind.
Das Bundesdatenschutzgesetz kann Anhaltspunkte liefern, Hier werden personenbezogene Daten der besonderen Art (Religion, Ethnische Herkunft, Gesundheit, Sexualleben, etc.) beispielsweise als besonders schützenswert angesehen. Doch noch viele andere Gesetze und Compliancevorgaben erfordern den besonderen Schutz der Daten. Wenn diese Vorgaben nicht greifen, liegt es dennoch am Schutzbedarf der Daten, wie damit umzugehen ist und wie sie einzustufen sind.
Dazu zählt auch, wenn die Vertraulichkeit (eingeschränkter Kreis der Empfänger) und die Integrität (also Unveränderlichkeit) der Daten sichergestellt werden müssen.
Der Fachbereich (das Business) kann hier entscheiden, welches Risiko dahinter steckt, würden Daten missbraucht, verändert oder verloren gehen. Welcher Schaden würde entstehen. Denn auch Intellectual Property ist ein hoch schützenswertes Gut (Datum). Also nicht nur offensichtlich schützenswerte Daten.
Der Faktor der Verfügbarkeit darf auch nicht vernachlässigt werden.

Wenn Anwendungen und damit Daten in die Cloud migriert oder Dienste aus der Cloud genutzt werden sollen, ist es ein entscheidendes Kriterium, erstmal zu wissen, welche Daten dort verarbeitet und gespeichert werden sollen. Dann ist zu überlegen, wie diese einzustufen sind. Daraus ergeben sich technische und organisatorische Maßnahmen, die die Cloud Lösung anbieten muss. Organisatorisch können auf Kundenseite Anforderungen entstehen.

Es ist hilfreich, eine Obergrenze der Klassifizierung zu definieren.
Bspw. können öffentlich bekannte Daten in die Cloud gehen und hoch schützenswerte nicht. Entsprechende Sicherheitsmaßnahmen sind immer zu ergreifen oder beim Cloud Service Provider zu erfragen, denn in bestimmten Servicekategorien wie SaaS hat man wenig Einfluss auf die Gestaltung der Sicherheit.

**Compliance und Governance**
Natürlich spielt nicht nur die Datenklassifizierung eine Rolle, sondern auch die Anforderungen, die durch Gesetze oder anderen Vorgaben kommen.
Wenn es um rechnungslegungsrelevante Daten geht z.B. muss Testierung nach Prüfungsstandards wie ISAE3402 oder IDW PS951 erfolgen.
Bei der Verarbeitung buchführungsrelevanter Daten müssen bestimmte Aufbewahrungsfristen (z.B. von bis zu 10 Jahren bei GOBS-Relevanz) eingehalten werden.
Bei personenbezogenen Daten hingegen ist die Löschung und Datensparsamkeit eine ganz wichtige Geschichte.
Hinzu kommt, dass nach dem Bundesdatenschutzgesetz jeder Cloud Service Provider, Managed Service Provider und Unterauftragnehmer nach § 11 Abs. 2 BDSG entsprechend vertraglich zu verpflichten ist. Eine ADV-Vereinbarung mit allen Unterauftragnehmern muss vorgelegt werden, wenn diese den Zugriff auf personenbezogene Daten erlangen können.
PCI DSS kommt zum Tragen sofern Kreditkartendaten verarbeitet werden.

Der Patriot Act ist ein Gesetz, das unsere Daten direkt betrifft. Das Safe Harbour Abkommen zum Austausch von personenbezogenen Daten vom 26. Juli 2000 wurde im Oktober 2015 gekippt und damit das Datenschutzniveau der US-Unternehmen als nicht ausreichend eingestuft.

Das 2001 in den USA erlassene Patriot Act Gesetz wurde nach den Terroranschlägen auf das World Trade Center verabschiedet, um es US Behörden legal zu erlauben ohne richterliche Anordnung auf die Server von US-Unternehmen zuzugreifen. Wichtig ist hierbei der Fakt, dass dies auch für ausländische Tochterunternehmen gilt, selbst wenn lokale Gesetze dies verbieten.

EU Datenschutz Grundverordnung tritt ab 2018 in den Fokus. Hierbei wird der Datenschutz innerhalb der EU vereinheitlicht. Bußgelder werden erhöht. Im Extremfall sind bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens möglich. Biometrische und genetische Daten wurden aufgenommen und zählen als besonders schützenswert.
Um das Schutzniveau beurteilen zu können, muss vorher der Schutzbedarf ermittelt werden. Daraus ergeben sich technische und organisatorische Maßnahmen und eine Bewertung hinsichtlich des Risikos, dass eventuell eingegangen werden muss, falls Maßnahmen nicht umgesetzt würden. Hinzu kommt bei der DS-GVO, dass zusätzlich Risiken bezüglich des Betroffenen bewertet werden müssen.
Technische Aspekte der Datenverarbeitung, die bislang eher unter „IT-Sicherheit“ anzusiedeln waren, bekommen durch die DS-GVO eine höhere Bedeutung für Datenschutzverantwortliche als es bislang durch das BDSG abgebildet wurde. In den nächsten Jahren müssen hierfür jedoch auf europäischer Ebene objektive Kriterien und Methoden festgelegt werden, um künftig geeignete Maßnahmen auszuwählen.

Deshalb ist es wichtig, vorher darüber nachzudenken, welche Anforderungen nicht nur aus der Klassifizierung der Daten, sondern auch aus der Art der Daten zusätzlich erwachsen können.

**Anforderungen an die Cloud-Umgebung**

Entsprechend der Datenklassifizierung und der Datenart kommen Sicherheitsmechanismen/-anforderungen in Frage, die in der Cloud gegeben sein müssen.
Entscheidend ist auch, welche Fertigungstiefen in Anspruch genommen werden: IaaS, PaaS oder SaaS und in welcher Ausprägung diese implementiert werden sollen.
Es gibt Anforderungen auf verschiedensten Ebenen. Das fängt bei Prozessen an und hört bei der Härtung eines Systems auf.
Zuerst einmal verschafft man sich einen Eindruck des Cloud Service Provider. Man darf nicht vergessen, dass dieser das Infrastruktur-Fundament zur Verfügung stellt. Mit dem Fundament steht und fällt alles. Ich würde mein Haus auch nicht auf einem sumpfigen Untergrund bauen. Also ist es wichtig, sich zu informieren. Dazu zählt auch die Frage der Lokation des Fundaments. Hier hat man oft die Wahl den Standort zu bestimmen.
Auf den Webseiten der großen Provider findet man Informationen rund um die zahlreichen Testate/Zertifizierungen (mittels eines SOC 2 Berichts), die erworben wurden. Diese sollte man genauestens prüfen. Selten ist man als Kunde berechtigt, Audits bei einem Cloud Service Provider durchzuführen. Entweder man vertraut dem Cloud Service Provider ein Stück weit und schätzt das Risiko ein oder man lässt es. Bei der genaueren Betrachtung der Zertifizierungen muss man auf den Scope und von wem das Zertifikat ausgestellt wurde.
Betrachtenswert sind Sicherheitsmaßnahmen wie Verschlüsselung, Sicherheitsinfrastruktur (Firewall, WAF, etc.), Administration der Komponenten, Ablage/Transport/Speicherung/Backup/Verarbeitung der Daten, Nachvollziehbarkeit durch Monitoring und Protokollierung, Identitäten-Verwaltung, Anbindung an das Rechenzentrum.
Es gilt herauszufinden, was uns die Cloud Lösung an Sicherheitsmaßnahmen bietet (Sicherheit von der Cloud) und was man selbst noch dazu tun kann (Sicherheit in der Cloud), um das eigene Sicherheitsverständnis/-niveau zu verstärken. Cloud Service Provider bieten sogenannte Security Pattern an, an denen man sich orientieren kann.

Betriebliche Aspekte sind auch zu berücksichtigen hinsichtlich Verfügbarkeit d.h. Disaster Recovery Lokation/Konzept, Prozesse wie Incidentmanagement, Kontaktpersonen sind zu definieren.

**Anwendungsaspekte**

Es gibt eine Vielfalt an Applikationen, die cloud-ifiziert werden können.
Angefangen bei Office Anwendungen (Mail, Telefonie, Word), die intern genutzt werden über Kundenplattformen, Marketing und Big Data Analyse Plattformen.

Wenn man mit eigens entwickelten Anwendungen in die Cloud gehen möchte, heißt das nicht immer, dass die Anwendung an sich auch cloudfähig ist.
Es ist natürlich möglich, erstmal alles in der Cloud so nachzubilden wie es bisher ist, doch das bringt nicht unbedingt die erhoffte Flexibilität und spart schlussendlich keineswegs Geld. Die Architektur der Applikation muss entsprechend aufgebaut/verändert werden.

**Strategie**

Wie integriert man das Thema in ein Unternehmen.
Ein Unternehmen entwickelt Unternehmensziele und leitet daraus Strategien für die jeweiligen Bereiche ab. Somit erhält auch der IT-Bereich eine Strategie. Diese IT-Strategie dient dazu, eine Cloud-Strategie zu entwickeln und beinhaltet auch die IT-Sicherheitsstrategie.
Wenn eine Cloud-Strategie im Unternehmen existiert, kann man damit beginnen, zu überlegen, welche Anwendungen in die Cloud wandern könnten.
Um diese Entscheidung zu treffen, sollten Cloud Leitfaden für die Nutzung der Cloud, Regelungen und Vorgaben hinsichtlich der Cloudlösungen und eine Entscheidungsmatrix unterstützen. Cloud Design Patterns helfen bei der Umsetzung einer geeigneten Lösung.
Wichtig ist es, den Schutzbedarfs der Daten festzustellen und eine entsprechende Risikoanalyse durchzuführen. Und das bei jedem neuen Cloud-Dienst.
Den Fachbereich selbst entscheiden zu lassen, wäre zu kurz gedacht. Es braucht mindestens den Datenschutzbeauftragten und den Informationssicherheitsbeauftragten dazu als Hilfestellung für den Bereich der IT-Sicherheit und Compliance.
Es ist ratsam, jemanden dazu zu holen, der sich mit dem Thema Cloud genauer befasst hat und wenn es ein externer Berater sein muss. Um Schatten-IT zu verhindern, sollten man den Fachbereichen vorgefestigte Lösungsrahmen zur Verfügung stellen. Bei IaaS könnte man zum Beispiel einen Sicherheits- und vertraglich abgesicherten Rahmen implementieren, damit darin flexibel Ressourcen aufgebaut und genutzt werden können.

**Kontaktadresse:**
Angela Espinosa
Deutsche Lufthansa AG
Airportring 1
D-60546 Frankfurt am Main

Telefon: +49 (0) 69-696 91904
E-Mail angela.espinosa@dlh.de
Internet: www.lufthansa.com