FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

LV: Aktuelle Themen der IT

Cloud Systeme

(Team: Kamil Glowinski / Christian Gossmann)

SS 2016

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

Inhaltsverzeichnis

FH Burgenland
UNIVERSITY OF APPLIED SCIENCES

1. Entwicklung von Computer zu Cloud Services

Cloud Systeme wurden schon in 1966 bereits von Douglas Parkhill im Buch „The Challenge of the Computer Utility"-Buch angedacht, wobei alle modernen Aspekte von Clouds darin angesprochen wurden. So war von unerschöpflichen Ressourcen und von öffentlicher (behördlicher) und privater Community die Rede. Die Entwicklung vollzog sich in groben Schritten folgendermaßen:

- ➔ Network-Computing
- ➔ Server-Cluster („einzelner starker Computer")
- ➔ Grid-Computer (Parallel-Computing)
- ➔ Utility-Computing, z.B. MS-Azure: nur das zahlen, wann und was wie lange gebraucht wird (=maßgeschneiderte Lösung je nach Geldbeutel)
- ➔ Mobile Computing (im Sinne Verbindungen zu „xyz as a service" jederzeit und überall zu haben)

2. IaaS, PaaS, SaaS

- ➔ Infrastruktur (=das Rechenzentrum in Form von Hardware nach Bedarf [und Geld!]) → achten auf Service Level Agreements und wo die Server stehen (EU, USA, islamischer Staat, Nordkorea)
- ➔ Plattform (=die Middleware, also gewünschte Software und Datenbanken) und
- ➔ Software „as Services" = Infrastruktur und Plattform zusammen unter einem Dach

spezielle Unterformen

- ➔ DaaS: Desktop (speziell zugeschnittene Umgebungen, Nutzung meist mit Thin-Clients)
- ➔ IDaaS: Identity (Benutzerauthentifizierung ausgelagert)
- ➔ DICaaS: Data-intensiv-Computing (z.B. Spezialanwendung Crashtests simulieren)
- ➔ HuaaS: Human (die Intelligenz des Menschen und nicht der Algorithmus steht im Vordergrund → der Mensch bedient also das „Hilfsmittel Computer" – Freelancer vermitteln über Börsen (www.mturk.com)
- ➔ Storage as Service

Letztere sind dabei heute am bekanntesten, da diese gemeinhin vom Tablet über Smartphones bis zu Implementierungen in Unternehmen verwendet werden. Wesentlich ist bei allen Systemen Augenmerk auf die Gewährung von Datenschutz und Datensicherheit zu legen. Konkret geht es darum, wo die Server stehen, auf denen die Files, bzw. Dienste gehostet werden, d.h. also welches Recht hier zum Tragen kommt. Andererseits gilt es auch sicherzustellen, wer die Clouds verwaltet und entsprechende Schulungen für Mitarbeiter in Unternehmen hält.

3. Einteilung der Clouds

- ➔ public (öffentlich nutzbar für jeden, auch den islamischen Staat / Nordkorea)
- ➔ privat (interne Bereitstellung in Behörden, sog. Government Clouds / Unternehmen)
- ➔ hybrid (je nach Anforderung: z.B. Werbung und PR öffentlich, Lohndatenbanken & Co. privat)

4. Möglichkeiten der Cloud(-Systeme) für modern ausgerichtete Unternehme (ausdrücklich NICHT NUR IT):

- ➔ Abhilfe bei interner Kommunikation, läuft sie schlecht, z.B. Urlaubsvertretung oder jemand krank, dann sind- Dokumente gesperrt
- ➔ Dokumente nur in lokalen PCs und / oder Zweigniederlassungen, die nicht global oder nur unzureichend vernetzt sind
- ➔ Dokumente sollen ALLE vorhanden sein und nicht ein Teil dort und da verstreut UND sie sollen aktuell sein
- ➔ Kosten sparen (eigene Cloud-System-Infrastruktur bedingt Updates vor Ort, Hardware, Räumlichkeiten und Sicherheitsmanagement, Backup-Konzepte, etc… und damit erhöhte Kosten)

5. Ziele der Clouds

- ➔ HPC-Infrastruktur (high performance)
- ➔ Plattformunabhängigkeit (Virtualisierung / Software Stacks)
- ➔ Trust Management
- ➔ Privacy / Copyright
- ➔ **Geld (einfacher) verdienen (sowohl für Cloud-Anbieter als auch Cloud-Nutzer)**

6. Herausforderungen

➔ Verfügbarkeit

➔ Datenschutz und Sicherheit

Verschlüsselung (symmetrisch → nicht so gut, Asymmetrisch mittels Public / Private Key-Verfahren). Generell hängt alles von der Key-Länge ab und den Zertifikatstypen: eigenes http-Zertifikat selbst signiert (und Owncloud)

→ Fehlermeldungen, aber trotzdem sicher für eigene Zwecke

→ für Drittanbieter: gekauftes Zertifikat mit Risiko, wer noch Zugriff darauf hat (besseres Image beim Kunden???)

➔ Performance (wie viele User, wann? „Wann es denen halt einfällt" – 3 Uhr morgens, 12 Uhr mittags...)
→ Planbarkeit: Volllast, Risiko der Performance-Einbuße?

➔ Software-Fehler (Bugs → schwer zu debuggen, da unter Realbedingungen die Cloud selbst debuged werden muss, um unter realistisches Bedingungen zu testen → hohe Gefahr des Datenverlustes oder zumindest Performance-Verlust)

➔ Lizenzen (Windows-Systeme, Owncloud?)

➔ Skalierbarkeit, Interoperabilität, Standards

7. Risiken der Cloud(-Systeme)

➔ Kosten – beachten: Implementierungskosten / (UM-)Schulungskosten für Personal auch hinsichtlich Datenschutz, Buchführungs- und Aufbewahrungspflichten → Gefahr: ändert sich das Cloud System durch den Anbieter, bzw. Hersteller, ändern sich auch die gewohnten Workflows (ohne Cloud entscheidet Geschäftsführung und IT-Abteilung, wann, wie und ob überhaupt umgerüstet wird. (Stichwort: Change Management → man wird abhängig von Externen)

➔ Verfügbarkeit des jeweiligen Rechenzentrums vs. eigene Server → Gefahr der verstreuten Daten (obere Punkt 2 u. 3)

➔ Haftung? Aufbewahrungspflicht für Finanzamt. Was passiert z.B., wenn Daten futsch sind – wer trägt die Verantwortung für den Restore (wenn hoffentlich wo ein Backup vorher gemacht wurde UND greifbar ist → Zugriff auf Backup Cloud, interne Sicherung der Cloud-Daten, ansonsten ist das Unternehmen „erledigt" → Backup as a Service??? Sensible Daten, wem anvertrauen???)

- ➔ Verschlüsselung, bzw. Sicherheit vor neugierigen Blicken (korrupte(r) SysadminIn, NSA, KollegInnen)
- ➔ Support? 24/7? Kosten? → aktuell Salzburger Uni E-Mail-System
- ➔ Clients für Cloud-Nutzung sind trotzdem erforderlich und eine IT-Infrastruktur dafür, um diese zumindest aktuell zu halten → Server (WSUS, System Center, ...) und damit Lizenzen oder kompletter Umstieg auf Open Source → (Um-)schulungskosten, da Windows verbreiteter ist

Zu den genannten Möglichkeiten und Risiken ist zu sagen, dass hier sowohl Kostenersparnis als auch Kostenrisiken im Raum stehen. Die Ersparnis liegt für kleinere Unternehmen v.a. in der Infrastruktur, die billiger outgesourced werden kann als selbst im Unternehmen entsprechendes IT-Equipment vor Ort und Personal zu dessen Wartung im Einsatz zu haben. Teuer kann es jedoch werden, wenn die Clouds nicht erreichbar sind und das Unternehmen von diesen Systemen einen Grad der Abhängigkeit (von externen Dienstleistern) erreicht hat, an dem es schlichtweg nicht mehr betriebsfähig ist. Zu diesem Zwecke sollte ein optimaler Kompromiss gefunden werden zwischen Diensten, die in der Cloud genutzt werden, bzw. Diensten und Services die man vor Ort (möglicherweise nur auf einem „kleinen" Server laufen lässt – und sei es nur, um zumindest in den wichtigsten Unternehmensbereichen handlungsfähig zu bleiben). Gemeint sind damit die wichtigsten Dokumente und Datenbestände. Allerdings gilt es hier zu beachten, dass die Synchronisierung zuverlässig mit den Cloud Systemen läuft, um hier nicht unterschiedliche Datenbestände zu erhalten.

Neben den Kosten gilt es auch die einleitend erwähnte Sicherheit zu beachten. Clouds müssen gegen unbefugten Zugriff gesichert sein, da darauf eben zentrale Unternehmensdaten gespeichert sein können, deren Manipulation oder Verlust auch meist den Tod des Unternehmens bedeutet – sei es aus Imagegründen („die sind gehackt worden") und dem damit verbundenen Vertrauensverlust, sei es aus wirtschaftlichen Gründen, wenn Daten von wichtigen Geschäftspartnern verloren gegangen sind, die die Existenz des Unternehmens gefährden oder auch schlichtweg der Konflikt mit dem Gesetz – wenn z.B. Daten länger vorrätig gehalten werden als zulässig, Daten auf Servern in Rechenzentren liegen, auf die (auch ohne Wissen) durch deren Anbieter oder Geheimdienste auf einfachste Weise zugegriffen werden kann. Daten auf eigenen IT-Systemen im Unternehmen lassen sich hier wesentlich besser sichern.

Letztlich gilt es natürlich auch mittels Sicherungen und Backup- und Restoreszenarien für den Katastrophenfall vorbereitet zu sein. Die beste Cloud nutzt nichts, wenn die Zugangsdaten fehlen, die Systeme erst neu aufgesetzt werden müssen und eine Wiederherstellung aus der Cloud Tage oder Wochen dauert (je nach Bandbreite) – im Vergleich zum Restore von internen Speichersystemen.

8. Cloud Dienste als Speicherplatz

Grundsätzlich sind 2 Möglichkeiten vorhanden, Speicherung der Daten (Filehosting) auf einem eigenen Server oder auf einem Externen der jeweiligen Cloud Anbieter Firma.

Wichtige Kriterien

- ➔ Standort der Server → Rechtsicherheit
- ➔ Schnittstellen
- ➔ Kosten
- ➔ Verschlüsselung / Datenschutz

One Drive

- ➔ Hoher Sicherheitsstandard
- ➔ Viele nützliche Office- und Teilfunktionen
- ➔ Weltweite Serverstandorte
- ➔ Keine WebDav[1] Unterstützung
- ➔ Keine FTP-Schnittstelle

Dropbox – Pionier unter den Speicherdiensten

- ➔ Unkomplizierte Bedienung
- ➔ Hoher Sicherheitsstandard
- ➔ Schneller Support in dt. Sprache
- ➔ Viele Funktionen zum Teilen
- ➔ Serverstandort außerhalb EU
- ➔ (Noch) Keine Office Funktionen
- ➔ Keine externe Schnittstellen (ftp[2], WebDAV)

---

[1] WebDAV (***Web**-based **D**istributed **A**uthoring and **V**ersioning*) ist ein offener Standard zur Bereitstellung von Dateien im Internet. Dabei können Benutzer auf ihre Daten wie auf eine Online-Festplatte zugreifen.

[2] Das **File Transfer Protocol** Netzwerkprotokoll zur Übertragung von Dateien über IP-Netzwerke.

Google Drive

- ➔ Viel Speicher für wenig Geld
- ➔ Sehr gute Benutzeroberfläche
- ➔ Google Docs erstellen u. bearbeiten
- ➔ Unbegrenzt Versionen speichern
- ➔ OCR Texterkennung
- ➔ Kein Serverstandort in der EU
- ➔ Kein Email-Support
- ➔ "Nur" 128bit Verschlüsselung

ownCloud

Speicherung von Daten auf eigenen Server, wurde 2010 durch ehemalige KDE Entwickler ins Leben gerufen um eine freie Alternative zu kommerziellen Anbietern eines Cloud-Service zu schaffen. Im Gegensatz zu kommerziellen Speicherdiensten kann ownCloud auf einem privaten Server oder Webspace ohne Zusatzkosten installiert werden. Somit können gerade bei sensiblen Daten die Bedenken gegenüber einer Datenweitergabe und der damit einhergehenden Abgabe der Kontrolle über die Daten zerstreut werden. Verschlüsselung der Daten auf dem Server sowie eine verschlüsselte Übertragung per SSL/TLS

Alle modernen Cloud Dienste die sich mit Datensicherung beschäftigen haben sogenannte Sync-Clients (Desktop Clients) die eine Automatisierten Upload und nahezu einen Live Sync-Vorgang bereitstellen. Jedoch sind Up- und Down Load über eine Webschnittstelle ebenfalls jederzeit möglich.

SEAFILE

Seafile ist eine freie Software, um Dateien zentral auf einem eigenen Server zu speichern. Benutzer können auf ihre Daten über eine Webschnittstelle zugreifen oder über Desktop-Clients synchronisieren. Der Hauptunterschied zu bekannte Online-Dienste liegt darin, dass Seafile als Open-Source-Software auf dem eigenen Server installiert werden kann.

9. Cloud Dienste als Rechenleistung:

Infrastructure-as-a-Service (IaaS) Die Nutzer erhalten über das Internet direkten Zugriff auf einzelne virtuelle Ressourcen im Netz, z. B. Speicher oder Rechenleistung.

Generell wir es durch „*Virtualisierung*“ realisiert. Damit wird das Betreiben eines „virtuellen Computers“ auf einer (fremden) Hardware gemeint. Dabei erfolgt eine logische Trennung eines Programms vom Betriebssystem des genutzten Rechners.

Anbieter von Public Clouds sind die ganz großen globalen IT-Unternehmen, u.a. Amazon (EC2), Google, Microsoft, IBM oder Hewlett-Packard (zusammen mit Intel und Yahoo). Diese verarbeiten die Daten auf weltweit verteilten Servern bzw. Serverfarmen, die einem oder auch unterschiedlichen Anbietern gehören.

10.Quellenangaben und verwendete Literatur

Bücher

- Thomas Erl (u.a.): Cloud Computing, 2013
- Dr. Tobias Höllwarth (Hrsg.): Der Weg in die Cloud, Hemsbach, 2011
- Kai Hwang (u.a.): Distributed and Cloud Computing, Waltham, 2013

Internet-Links

- https://de.wikipedia.org/wiki/OwnCloud
- https://www.vetalio.de/cloud-speicher
- https://**onedrive**.live.com/about/de-at/
- www.**dropbox**.com/
- https://**owncloud**.org/
- https://www.**google**.com/intl/de_at/**drive**/
- https://seafile.de/
- https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html