

Cloud Computing – ein Hype-Thema ohne Zukunft?

Wolfgang Sidler

An vielen IT-Veranstaltungen wird über das neue, unbekannte «Cloud Computing» gesprochen und verkündet, dass Cloud Computing die Zukunft sei. Wie war das mit dem Outsourcing vor einigen Jahren? Wieso haben heute viele Unternehmen plötzlich Zweifel am Nutzen des Outsourcings und beginnen mit dem Insourcing? Wurden die Erwartungen an die Kosten, Dienstleistungsqualität und Funktionalität nicht erfüllt? Oder wurde man vom Outsourcer abhängig und verlor das eigene teure interne Know-how? Wieso heizen die Software-Giganten wie Amazon, Google und Microsoft dieses Thema so auf? Sehen sie hier ihre Wachstumschancen? Oder ist im Moment die «Wirtschaftskrise» der Motor für solche Überlegungen – wie im Jahr 2001 als Outsourcing boomte?

Viele Fragen. Darf man sich darüber Gedanken machen, oder soll man einfach mit dem Mainstream mitmachen – wird ja schon gut gehen. Oder glaubt man, mit Cloud Computing sind alle IT-Probleme gelöst?

Wie sieht es mit der Sicherheit und dem Datenschutz aus? Werden diese Systeme nicht alle im Ausland, in den USA gehostet?

Ein Beispiel: Sie als Unternehmer haben strategisch entschieden, die IT mit einem Cloud-Anbieter zu outsourcen. Sie unterschreiben einen Service Level Agreement (SLA) und gehen davon aus, dass alle vereinbarten Punkte und alle notwendigen Sicherheitsvorkehrungen getroffen und eingehalten werden. Einen Monat später, das Cloud-Projekt wurde abgeschlossen und

Ist Cloud Computing nicht der Wunsch eines jeden IT-Managers? Auslagern der gesamten IT inklusive Hardware, Programme und Daten – klingt doch ganz genial. Aber wo bleiben die Sicherheit und der Schutz der Daten? Ist Cloud Computing einfach eine erweiterte Version des bekannten Outsourcings oder des Software as a Service? Möchte das Management nun mit dieser Lösung sogar die Verantwortung des IT-Betriebs auslagern?

ihre Programme mit den «vertraulichen» Firmendaten laufen nun in der Wolke (Cloud). Nun entscheidet der Cloud-Provider, ohne bei ihnen ihr Einverständnis einzuholen, die Festplatten-Kapazität des Systems zu vergrössern, indem der Cloud-Provider Festplatten-Kapazität zum Beispiel in China zu einem viel günstigeren Preis einkauft. Der Cloud-Provider verschiebt ihre «vertraulichen Daten» von den USA nach China. Doch beim kopieren ist ein Fehler passiert, und eine beträchtliche Menge ihrer Daten wurde nicht kor-

zialsoftware wie Customer-Relationship-Management (CRM) oder Business Intelligence) wird durch den Anwender nicht mehr selbst betrieben/bereitgestellt, sondern über einen oder mehrere Anbieter bezogen. Die Anwendungen und Daten befinden sich nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der (metaphorischen) Wolke (engl. cloud), die üblicherweise das Internet in gängigen Netzwerkdiagrammen repräsentiert. Der Zugriff auf die entfernten Systeme

Wer von uns würde ein Auto fahren, bei dem die Bremsen nur zeitweise funktionieren oder ihren Dienst beliebig verweigern?

rekt kopiert und eine Wiederherstellung der Daten war nicht mehr möglich. Fazit: Sie haben viele Daten verloren. Sie haben kein Backup bei ihnen, da sie ja dachten, der Cloud-Provider hat ein Backup – was bedeutet dieser Datenverlust nun für ihr Unternehmen? Wer bezahlt ihnen den Schaden? Haben sie die Kraft und die finanziellen Mittel gegen Google, Amazon oder Microsoft zu klagen?

Was ist Cloud Computing, wie wird Cloud Computing heute verkauft?

Die IT-Landschaft (in diesem Zusammenhang z. B. Rechenzentrum, Storage, Mail- oder Collaboration-Software, Entwicklungsumgebungen, aber auch Spe-

erfolgt über ein Netzwerk, beispielsweise das Internet. Der Zugriff auf die Anwendungen oder die Konfiguration von z. B. Cloud-Storage selbst erfolgt über einen Webbrowser. (Quelle: Wikipedia)

Was versteht man heute unter Datenschutz?

Informationelle Selbstbestimmung ist das Recht und die Fähigkeit des Einzelnen, über die Beschaffung, Verwendung und Verbreitung seiner personenbezogenen Daten durch andere selber Kontrolle auszuüben. Sie bildet die Grundlage eines zeitgemässen Datenschutzes rund um die Welt. Auf dem Spiel steht nicht allein der Datenschutz, sondern das Vertrauen von Millionen von Individuen oder Benutzern,

Kunden und Bürgern in der heutigen Informationsgesellschaft.

Risiken des Cloud Computings

- Grosse Abhängigkeit in Bezug auf den Internetanschluss im eigenen Unternehmen.
- Grosse Abhängigkeit zum Cloud-Provider (Anbieter).
- Disaster-Recovery-Lösungen und Backup-Strategien beim Cloud-Anbieter sind nicht oder nur teilweise vorhanden. Der Cloud-Anbieter könnte nicht in der Lage sein, ihre Daten wiederherzustellen.
- Das Service Level Agreement (SLA) ist nicht klar genug formuliert und enthält Lücken.
- Die vereinbarten Dienstleistungen werden nicht mit der gewünschten Qualität ausgeführt (Performance, Funktionserweiterungen, Support, Release-Wechsel, Benutzeradministration usw.).
- Die IT- und Informationssicherheit wird nicht gewährleistet.
- Der Datenschutz kann nicht eingehalten werden.
- Der Benutzerzugriff: Benutzer ausserhalb der Firma oder nicht autorisierte Benutzer erhalten Zugang zu ihren sensiblen Daten.

- Der Speicherort ihrer Daten kann ohne ihr Wissen verlagert werden. Wie sieht die Gerichtsbarkeit im Land der Daten aus?
- Wie werden ihre Daten gespeichert? Wählen sie ein günstiges Cloud-Modell aus, werden ihre Daten in einer Umgebung mit den Daten anderer Kunden gespeichert?
- Eigentum der Daten. Wem gehören die Daten wirklich?
- Wie können sie Kontrolle über die Vorgänge in der Wolke haben? Wie können sie die Compliance durchsetzen?
- Zugriffsrechte für den Datenzugriff können nicht optimal vergeben werden.
- Know-how-Verlust.
- Bis heute gibt es noch keine Standards für das Cloud Computing.

Ist es nicht so, dass sie Strom aus der Dose beziehen und ihnen nun weisgemacht wird, sie können die Programme und Daten auch wie Strom aus der Dose beziehen? Aber sind die Programme mit ihren Daten und ihrem Know-how nicht mehr wert als «nur» Strom aus der Dose? Wie sieht die rechtliche Sichtweise aus? Bei der rechtlichen Betrachtung sollte grundsätzlich zwischen der Beziehung Endkunde (Sie) und Cloud-Anbieter und Cloud-Anbieter und den rechtlichen Beziehungen innerhalb der Wolke unterschieden werden.

Interessant ist, dass ein aktueller Leitfaden von RSA, EMC und VMware zur Schlussfolgerung kommt, dass Clouds das Sicherheitsniveau herkömmlicher IT-Infrastrukturen in Zukunft bei Weitem übertreffen könnten. Ist das nicht einfach Werbung im eigenen Interesse? RSA, der grosse US-Anbieter von Sicherheitslösungen, EMC, der grosse US-Anbieter von Festplatten, VMware, der grosse US-Anbieter von Virtualisierungs-Software. Sind nicht diese grossen US-Player die Hauptprofiteure des neuen Hype «Cloud»?

Fazit

Wird Cloud Computing ein Standard? Wer seine Daten, seine Innovation, sein Know-how schützen möchte, wird sich dies zweimal überlegen. Sind die Kostenersparnisse so gross, dass sie sich eine Datenpanne erlauben können?

Denn Cloud Computing ist auch eine Frage des «Vertrauens». Beim Cloud Computing, das zur Kostenoptimierung ausgelegt ist, sind Sicherheitsaspekte, die Berücksichtigung von Landesgrenzen und eine sehr hohe Vertrauenswürdigkeit nicht integral vorgesehen. Oder wurden wir alle vom neuen Cloud Computing oder Green-IT-Virus befallen? ■

