goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Sicherheit in der Cloud

Das Thema Cloud Computing ist zu einem ständigen Begleiter geworden. Viele Firmen sind sich bereits am Überlegen, ob Sie ihre Daten auslagern möchten. Dieser INFONEWS geht näher auf die Sicherheitsaspekte der Cloud ein und beantwortet dabei folgende Fragen:

- Welche Arten von Cloud-Diensten gibt es?
- Welche Gefährdungen existieren in der Cloud?
- Wie kann den Risiken begegnet werden?

Der Begriff „Cloud" (frei übersetzt: Rechnen in der Wolke) ist zu einem richtigen Hype geworden. Praktisch jeder spricht darüber, alle Zeitschriften berichten darüber. Dieser INFONEWS zeigt einige Facetten der Cloud und geht speziell auf das Thema der IT-Sicherheit ein, die es zu beachten gibt.

Inhaltsverzeichnis

1 ANWENDUNG 2
2 ARTEN VON CLOUDS 2
3 ANFORDERUNGEN AN DIE CLOUD 3
4 SNIA STANDARD 4
4.1 CDMI – ein neuer Standard für die Cloud 4
5 SICHERHEIT IN DER CLOUD 5
6 GEFAHREN IN DER CLOUD 6
7 DATENSCHUTZ 6
8 FAZIT 7
9 QUELLEN 7

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Anwendung

Die Cloud wird für verschiede Arten genutzt:

- Auslagerung von Rechenkapazität bzw. Datenspeicher (IaaS),
  Unter Infrastructure-as-a-Service (IaaS) versteht man ein Geschäftsmodell, das entgegen dem klassischen Kaufen von Rechnerinfrastruktur vorsieht, diese on demand zu mieten. Die bekannteste Anwendung von IaaS ist Amazon EC2.

- fertigen Programmpaketen (SaaS),
  Unter Software-as-a-Service (SaaS) versteht man ein Geschäftsmodell, Software nicht länger als Lizenz an einen Benutzer zu verkaufen, sondern lediglich die Benutzung selbiger als Service zur Verfügung zu stellen. Besonders vorangetrieben wurde diese Entwicklung durch Webservices, die in der Regel pro Aufruf abgerechnet werden. Als Beispiele für Software as a Service sind Google Docs und Apple iWork.com zu nennen.

- Programmierumgebungen (PaaS) und
  Unter Platform-as-a-Service (PaaS) versteht man den Ansatz eine integrierte Laufzeit- (und evtl. auch Entwicklungs-) -umgebung als einen Dienst zur Verfügung zu stellen, für den der Nutzer on demand zahlen muss. Ein bekanntes Beispiel dafür ist die Google App Engine.

- der kompletten Auslagerung (XaaS)
  Everything as a Service, kurz XaaS bezeichnet einen Ansatz, „alles" als Service zur Verfügung zu stellen und zu konsumieren. Damit ist es der konsequente letzte Schritt, nachdem es bereits Software, Laufzeitumgebungen, Hardware und menschliche Arbeit "as a Service" gibt.

Die Abrechnung erfolgt nutzungsabhängig, das heisst, es werden nur die tatsächlich genutzten Dienste bezahlt. Ein weiterer zentraler Punkt des Konzeptes ist, dass die Bereitstellung basierend auf der Kombination aus virtualisierten Rechenzentren und modernen Webtechnologien wie Webservices vollautomatisch erfolgen kann und somit keinerlei Mensch-Maschine-Interaktion mehr erforderlich ist.

2 Arten von Clouds

[Quelle: wikipedia] Der Begriff „Cloud Computing" stammt aus dem IT-Management und wird dem Wirtschafts-Professor Ramnath K. Chellappa zugeordnet. Klassischerweise wird zwischen verschiedenen Arten von Clouds unterscheiden, die je nach Anwendungsfall ihre Berechtigung haben:

- Private Cloud: Bei „Private Clouds" steht im Vordergrund, dass sich sowohl Anbieter als auch Nutzer im selben Unternehmen befinden, wodurch beispielsweise sämtliche Probleme aus dem Bereich Datensicherheit mehr oder minder hinfällig werden. Man unterscheidet dabei folgende Evolutionsstufen:
  - Exploratory Cloud: Hier steht das Ausprobieren von Cloudfunktionalität innerhalb eines Unternehmens im Vordergrund. Dabei geht es insbesondere darum, Potential und Nachteile für konkrete Anwendungen herauszufinden.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

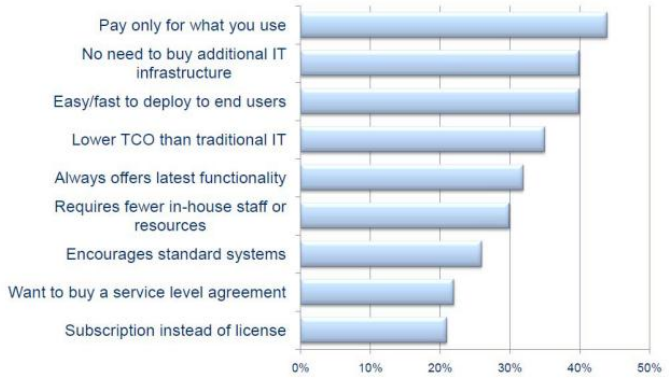
Telefon 052 320 91 20
Fax 052 320 91 21

- „Departmental Cloud“: Hierbei handelt es sich um eine Cloud, die sich innerhalb eines Unternehmens auch lediglich innerhalb einer Abteilung befindet. Dies bedeutet insbesondere, dass Anbieter und Nutzer innerhalb der gleichen Abteilung zu finden sind. Diese Cloudart dient nicht mehr nur Testzwecken.
- Enterprise Cloud: Im Gegensatz zur „Departmental Cloud“ stammen hier Anbieter und Nutzer aus unterschiedlichen Unternehmensabteilungen.

- Public Cloud: Eine „Public Cloud“ ist eine „Cloud“, die öffentlich ist, d. h. von beliebigen Personen und Unternehmen genutzt werden kann und nicht mehr auf interne Anwendungen einer einzelnen Institution/eines Unternehmens beschränkt ist. Hierbei greifen dann auch vor allem Probleme, die mit Datensicherheit zu tun haben und jeder Akteur muss sich selbst überlegen, wie viele und welche Daten er ausserhalb seiner unmittelbaren Kontrolle halten möchte. Auch hier gibt es Unterformen:
  - Exclusive Cloud: „Exclusive Clouds“ setzen voraus, dass sich sowohl Anbieter als auch Nutzer kennen. Sie handeln feste Konditionen aus und schliessen einen Vertrag darüber ab. Es gibt keine Unbekannten.
  - Open Cloud: Bei „Open Clouds“ kennen sich Anbieter und Nutzer vorher nicht. Dies hat zur Folge, dass der Anbieter sein Angebot ohne direkten Input vom Kunden entwickeln und in Form von SLAs festschreiben muss. Auf Grund der Vielzahl an potentiellen Nutzern müssen auch der gesamte Geschäftsabschluss sowie die Nutzung von Instanzen anbieterseitig vollautomatisch ablaufen.
- Hybrid Cloud: Ein Unternehmen betreibt eine eigene „Private Cloud“ und nutzt zusätzlich als Failoverstrategie oder für Belastungsspitzen eine „Public Cloud“.

3 Anforderungen an die Cloud

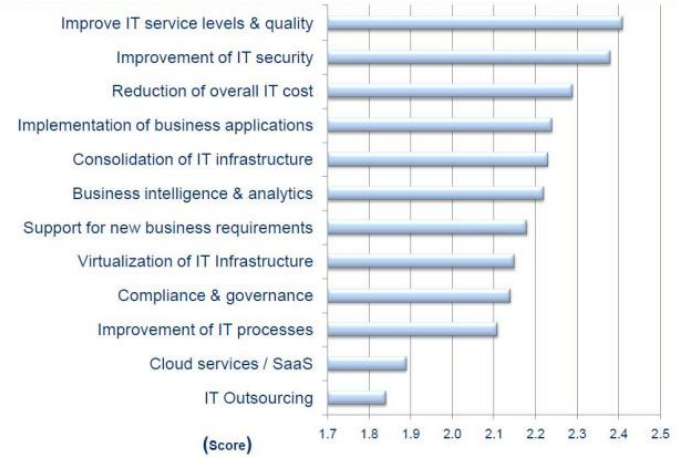
Die IDC führt jährlich eine Umfrage zu den Anforderungen an die Cloud durch. Die Ergebnisse der letzten Auswertung im Mai 2010 liegen nun vor. Der wichtigste Punkt seit dem Start der Studie ist, nur das bezahlen, was auch genutzt wird. Weiter kommen Ersparnisse der eigenen Infrastruktur und dem eigenen (IT-) Personal dazu.



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Als höchste Priorität für das Jahr 2010 wird mit Cloud Lösungen die Erhöhung der IT-Sicherheit angestrebt. Weiter sollen die Kosten reduziert und neue Anforderungen des Business erfüllt werden.



4 SNIA Standard

Das grosse Problem an der Cloud ist, dass jeder Anbieter etwas anderes darunter versteht. Gemäss Markforschungsunternehmen soll sich der Markt bis 2014 mit 6.2 Milliarden US-Dollar durchsetzen. Dafür muss die praktische Nutzung aber einhundert Prozent reibungslos funktionieren.

Um solche Standards zu entwickeln, hat die Storage Networking Industry Association (SNIA) eine Technical Work Group (TWG) ins Leben gerufen. Darüber hinaus will der Verband dazu beitragen, die Bemühungen der Storage-Hersteller im Interesse der Endkunden zu kanalisieren und generell für Klarheit beim Thema Cloud Storage sorgen. Offene Fragen gibt es beispielsweise bei der Kostentransparenz und in Bezug auf Security, Übertragbarkeit und Bezahlbarkeit von Cloud-Diensten.

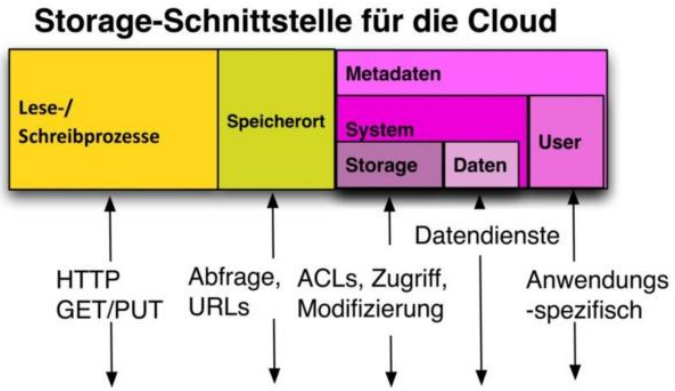
4.1 CDMI – ein neuer Standard für die Cloud

Die SNIA hat zum Thema Cloud Storage zwei Gruppen gebildet: Die noch junge SNIA Cloud Storage Initiative (CSI) wurde im Oktober 2009 gegründet, um die Entwicklung des Marktes voranzutreiben und Aufklärungsarbeit für Hersteller, Entwickler und Endkunden zu leisten. Eine SNIA Cloud Storage Technical Work Group (TWG) mit mehr als 140 Gründungsmitgliedern besteht bereits seit April 2009. Sie formulierte den Cloud Data Management Interface (CDMI) Standard, dessen öffentliche Evaluierung im September 2009 mit der Vorstellung auf der SNIA Storage Developer Conference startete.

CDMI erleichtert die Implementierung von Cloud Storage auf allen Ebenen. Davon profitieren Cloud-Storage-Kunden, Dienstleister, Entwickler sowie Anbieter von Cloud Software, Hardware und Infrastruktur. Im Detail definiert CDMI die Schnittstelle beziehungsweise die Funktionalitäten, über die Anwendungen innerhalb der Cloud interagieren: CDMI regelt, wie Daten in der Cloud erstellt, gesucht, aktualisiert oder gelöscht werden. Mit seiner Hilfe können Clients die Möglichkeiten von Cloud-Storage prüfen. Und sie können über diese Schnittstelle Datencontainer und die darin enthaltenen Daten managen. Zusätzlich lassen sich den Containern und Datenelementen per CDMI-Schnittstelle Metadaten zuweisen.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



Administrations- und Management-Applikationen nutzen CDMI für das Management von Containern, Accounts, Zugriffsberechtigungen und Monitoring-/Abrechnungsdaten. CDMI funktioniert auch, wenn der Storage-Zugriff über Protokolle wie SAN, NAS, FTP, WebDAV oder http/REST abläuft. Die Schnittstelle legt die Fähigkeiten sämtlicher Storage- und Datendienste offen, so dass die Möglichkeiten für die Clients transparent sind.

Weitere Informationen zum Standard sind unter http://cdmi.sniacloud.com/ zu finden.

5 Sicherheit in der Cloud

Das Fraunhofer-Institut für Sichere Informationstechnologie SIT ist der Frage nachgegangen, wie sich IT-Sicherheit und der Trend zum Cloud-Computing vereinbaren lassen. Dazu hat sie drei Projektgruppen mit mehr als 30 Personen eingerichtet. Eine der drei Projektgruppen, die Projektgruppe Sichere Services und Qualitätstests, die sich unter anderem mit Cloud-Computing und Service-orientierten Architekturen (SOA) beschäftigt, veröffentlichte Mitte 2009 eine Studie über die Sicherheit von Cloud-Computing-Systemen. „Fast jeder grosse Anbieter von Cloud-Services hatte in der Vergangenheit einen grösseren Vorfall im Bereich Verfügbarkeit oder Sicherheit“, berichtet Dr. Werner Streitberger Projektleiter dieser Studie.

Bei der Untersuchung des SIT zeigte sich auch, dass trotz solcher Risiken kleine und mittlere Unternehmen ihre Sicherheit durch den Einsatz von Cloud-Services erhöhen können, da beim Anbieter das Wissen rund um die IT-Sicherheit in der Regel vorhanden ist.

Grosse Unternehmen hingegen sollten die Sicherheitsfunktionen eines Cloud-Anbieters individuell prüfen und im Einzelfall entscheiden, ob die angebotenen Sicherheitsmechanismen für den konkreten Bedarf des Unternehmens ausreichend sind. Wegen der wenig standardisierten Vorgehensweise beim Einsatz von Sicherheitstechnologien in Cloud-Computing-Systemen ist dies nicht garantiert. Massstab sind auch hier die allgemeinen Schutzziele der IT-Sicherheit, also Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit, Verfügbarkeit und Schutz der Privatsphäre.

Eine weitere Schwachstelle sind die Service-Level-Agreements (SLAs), also die Vereinbarungen über die Rechte und Pflichten zwischen den Cloud- Benutzern und Cloud-Anbietern: Die bisher üblichen Vereinbarungen geben nur minimale Garantien der Dienstgüte des Cloud Service. Vor allem Sicherheitsgarantien sind nur rudimentär vorhanden und die dafür nötigen Funktionen durch den Cloud-Anbieter nur unzureichend dokumentiert. Eventuell sollte ein Proof-of-Concept, eine Machbarkeitsstudie, vor dem eigentlichen Einsatz realisiert werden«, rät Fraunhofer-Forscher Streitberger.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

6 Gefahren in der Cloud

Gemäss der bereits erwähnten, aktuellen Studie der IDC ist die Erhöhung der IT-Sicherheit eines der grössten Ziele, um die Cloud zu nutzen. Aber genau dieser Punkt ist auch das grösste Hindernis, die eigene Infrastruktur in fremde Hände zu geben. Daher gilt es auch die Sicherheitsrisiken frühzeitig in die Planung einzubeziehen. Davon betroffen sind vor allem die Integrität und die Vertraulichkeit der Daten.
Je nach Anbieter der Cloud-Lösung werden die Administratoren-Rechte komplett dem Kunden übergeben. Andere ermöglichen ihren eigenen IT-Angestellten kompletten Zugriff auf die Kundendaten. Auch im ersten Fall muss sich der Anbieter um die Verteilung der Daten (Redundanz) bzw. um die Sicherung dieser kümmern. Dazu benötigt er in der Regel ebenfalls Zugriff auf die Daten. Auf jeden Fall besteht die Gefahr, dass die Kontrolle über den Zugriff auf die eigenen Daten abgegeben wird. Somit ist nicht mehr klar, wer genau auf diese Daten zugreifen kann.

Generell kann natürlich davon ausgegangen werden, dass die Administratoren vertrauenswürdig sind. Doch welcher IT-Angestellte musste schon je seine Identität beweisen, zum Beispiel mit der Identitätskarte oder seine Vergangenheit offenlegen, zum Beispiel mittels Strafregisterauszug. Vermutlich die wenigsten. Verschiedene aktuelle Fälle zeigen, dass es immer wieder geschieht, dass sich jemand eine andere Identität aufbaut und so unbemerkt einen Datendiebstahl durchführen kann.

Eine vertragliche Lösung könnte eine Abhilfe sein (durch Definieren einer einzelnen oder mehrerer Personen), doch dies widerspricht der Idee von Cloud Computing. Somit bleibt nur eine Verschlüsselung der Daten, um den Zugriff auf die eigenen Daten sicherzustellen. Bei einem Online Datenspeicher stellt dies in der Regel kein Problem dar, ja wird sogar von einigen Anbietern direkt in die zu nutzende Software integriert. Anders sieht es jedoch aus, wenn eine Applikation in der Cloud genutzt wird. Diese Applikation muss verständlicherweise auf die Daten zugreifen können und erwartet diese in unverschlüsselter Form.

Für einen Cloud-Anbieter macht die Lösung nur dann einen Sinn, wenn er die vorhandenen Ressourcen auf mehrere Kunden aufteilen kann. Dies stellt den nächsten „Knackpunkt“ dar. Der Anbieter muss garantieren, dass die Daten sicher voneinander getrennt sind. In virtualisierten Umgebungen stellt dies, je nach Software, kein Problem dar. Die Virtualisierung von Kundendaten gehört hingegen nicht dazu (bzw. es sind erst sehr wenige zertifizierte Lösungen auf dem Markt, die dies beherrschen und dadurch sehr teuer sind). Dies gilt auch für Datenbanken. Der Anbieter muss den Spagat zwischen sicherer Datenseparierung und den Kosteneinsparungen machen. Es empfiehlt sich genau abzuklären, wie der Anbieter mit dieser Problematik umgeht und welche Lösungen er umgesetzt hat.

7 Datenschutz

Beachtet werden müssen auch länderspezifische Gesetze und rechtliche Anforderungen zu beachten. So verbietet es das Schweizerische Datenschutzgesetz, Daten ins Ausland zu transferieren, wenn keine Gesetzgebung zum Schutz dieser Daten besteht (DSB, Art 6, Abs 1). Die EU erfüllt diese Anforderung, Amerika gehört hingegen nicht dazu. Viele Cloud-Anbieter haben darauf reagiert und

bieten ihre Cloud-Umgebungen in der EU an. Sollte jedoch ein Rechenzentrum ausfallen, werden die Daten an einen anderen Standort transferiert (oder sind bereits redundant dort abgelegt). So kann es schnell geschehen, dass die Datenschutzbestimmungen verletzt werden. Dieser Umstand sollte ebenfalls schriftlich festgehalten werden.

Oft wird unterschätzt, dass durch die Auslagerung eines Dienstes mehr Single Point of Failure entstehen, als gelöst werden. Zwischen dem eigenen Netzwerk und dem Anbieter entsteht ein grösseres Netzwerk mit weiteren Komponenten. Damit erhöht sich auch die Gefahr von Ausfällen. Klar kann dies wiederum durch Redundanzen gelöst werden (z.B. durch eine redundante Internet-Anbindung zum Anbieter), doch auch dies widerspricht dem Cloud-Gedanken, da die Netzwerkpfade auf Seiten des Anbieters unbekannt sind. Oft sind auch verschiedene Provider zwischen dem eigenen Netzwerk und der Cloud. Daher sollte als dritter zu regelnder Punkt auch ein Nachweis über die Ausfallsicherheit des gesamten Netzwerkpfades definiert sein. Zusätzlich lohnt es sich, bereits im Vorfeld einen entsprechenden Notfallplan zu erarbeiten.

8 Fazit

Bevor die Wahl auf einen Anbieter fällt, sollten folgende Elemente beachtet werden:

- Verfügbarkeit der Cloud Security Lösung
- Zertifizierung des Cloud Anbieters (SAS 70 Type II, ISO 27001)
- Transparenz bezüglich der Lokation der Daten
- Unabhängigkeit gegenüber dem Anbieter
- Umsetzung von Standards (ISO 20000, ITIL)

Die Cloud stellt alle beteiligten Parteien vor neue Herausforderungen, für welche es nur teilweise befriedigende Lösungen gibt. Daher sollten alle erwähnten Problemfelder für den eigenen Einsatzzweck gründlich überprüft und schriftlich festgehalten werden. Eine zusätzliche Risiko-Analyse hilft, die möglichen Schwachpunkte zu erkennen und im Vorfeld geeignete Massnahmen umzusetzen.

9 Quellen

http://www.searchstorage.de/themenbereiche/management/daten/articles/255285/

http://cdmi.sniacloud.com/

http://www.idc.com/prodserv/idc_cloud.jsp

http://de.wikipedia.org/wiki/Cloud_Computing

http://www.fraunhofer.de/presse/presseinformationen/2009/09/cloud-computing-sicherheit.jsp

Stephan Müller, Andreas Siegert, http://www.atsec.com

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21