

# IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Compliance

## RECHENZENTRUMS-SICHERHEIT

Public Cloud Security – Blauer Himmel oder Wolkenbruch?

### Die Zukunft der Rechenzentren liegt in den Wolken

**Heiter bis wolkig – so lautet die Stimmung vieler Unternehmen und Hersteller in Bezug auf Cloud-Computing-Konzepte. Während bei den einen Euphorie ob der Einsparpotenziale und schnellen Verfügbarkeit herrscht, dominiert die anderen hauptsächlich die Frage nach der (Un-)Sicherheit. Das ist nicht verwunderlich, denn die IT in der Wolke ist viel diskutiert und es scheiden sich die Geister, wenn es um Vor- und Nachteile geht. Der Global-Sourcing-Spezialist NIIT Technologies zeigt auf, wie sich der größtmögliche Nutzen bei gleichzeitiger Vermeidung von Risiken erzielen lässt.**

Die Frage, ob Cloud-IT eine Luftblase ist, die in Kürze zu platzen droht, stellt sich wohl nicht mehr. Dafür gibt es mittlerweile zu viele Konzepte, Interessenten und Anbieter – davon einige Branchenriesen –, die sich intensiv mit der Thematik auseinandersetzen und eine Menge Geld investieren. Die schnelle Verfügbarkeit, die Abrech-

nung nach tatsächlicher Nutzung und daraus resultierende Kostenvorteile sowie die Flexibilität sind in Zeiten von Optimierungs- und Einsparstrategien stichhaltige Argumente. Während einige mehr und mehr ihre Geschäftsprozesse in die Cloud verlagern, schauen die anderen jedoch noch ratlos in die Zukunft.



„Zu viele Ansätze, die unterschiedliche Interpretation und der breite Aktionsspielraum in einem noch größtenteils unerprobten Umfeld führen beim Cloud Computing schlichtweg zu Verwirrung auf Anwenderseite“, Michael Eisenmann, IT-Security-Consultant bei NIIT Technologies

Michael Eisenmann, IT-Security-Consultant bei NIIT Technologies nennt zwei der Hauptursachen für die Unsicherheit der skeptischen Unternehmen: „Viele Anbieter tummeln sich mittlerweile in diesem Markt und Anwender stehen vor der Aufgabe, den Überblick zu behalten und Vertrauen zu fas-

sen. Über IT in der Wolke wird viel diskutiert, aber meist wenig gesagt – hieraus ergibt sich ein Informationsdefizit. Zu viele Ansätze, die unterschiedliche Interpretation und der breite Aktionsspielraum in einem noch größtenteils unerprobten Umfeld führen schlichtweg zu Verwirrung auf Anwenderseite.“

Daher sind Dienstleister gefordert, ihre Angebote transparent zu gestalten und klar im Markt zu positionieren. Für Anwender steht ganz oben auf der Agenda, zu analysieren, wo die Potenziale und wo die Risiken liegen, die es auszuräumen gilt, um Cloud-gerechte Bedingungen zu schaffen. Diese differieren je nach ausgelagertem Geschäftsbereich, der Funktion, Branche etc. stark. „Besonders schwierig gestaltet sich die Auslagerung in die Public Cloud. Die größte Chance auf Erfolg haben in Zukunft standardisierte und strukturierte Services, die sinnvoll in die Unternehmensstrategie eingebunden und kontrolliert werden können, um klare Leistungs- sowie Kostenvorteile zu erzielen“, sagt Michael Eisenmann.

#### Eine Frage der Sicherheit

Eines der stärksten Contra-Argumente, die Kritiker hinsichtlich Cloud Computing ins Feld führen, ist der Sicherheitsaspekt. Der negative Beigeschmack, Daten aus der

Anzeige

## Rittal – Das System.

Erleben Sie „Rittal – Das System.“ live  
CeBIT Hannover  
1. bis 5. März 2011  
Halle 11, Stand E06

SCHALTSCHRÄNKE      STROMVERTEILUNG      KLIMATISIERUNG

FRIEDHELM LOH GROUP

Hand zu geben und damit gefühlt die Kontrolle zu verlieren, bremst viele Unternehmen aus. Gerade, wenn sie gesetzlichen Anforderungen wie dem Schutz personenbezogener Daten (Bundesdatenschutzgesetz) und rechtlichen Vorgaben wie Archivierung etc. unterliegen, ist das Misstrauen groß. Und diese Einstellung ist nicht unberechtigt, denn es gibt einige Cloud-Anbieter, die diese Richtlinien nicht erfüllen können oder sich bewusst nicht daran halten.

Daher steht es an erster Stelle, die eigenen Sicherheitsanforderungen zu definieren und einen Dienstleister dahingehend auf Herz und Nieren zu prüfen sowie vertraglich zu regeln, dass der Betrieb der Public Cloud die Security- und Compliance-Bestimmungen erfüllt. Eine Checkliste hilft bei der Definition der eigenen Anforderungen und der damit einhergehenden Sondierung des richtigen Anbieters:

- Wie transparent ist der Cloud-Service? Wie, wo und in welcher Form erfolgt die Datenverarbeitung und -speicherung?
- Wie erfolgt der Schutz der Vertraulichkeit der Daten bei der Übertragung der Daten zwischen Anbieter und Kunde sowie beim Transport und bei der Ablage innerhalb der Cloud?
- In welcher Form erfolgt der logische Zugriffsschutz? Wie gestaltet sich das Berechtigungskonzept?
- Auf welche Weise wird der physische Zugangsschutz zu den gespeicherten Daten und den Systemen des Cloud-Anbieters realisiert?

- Wie hoch ist die Verfügbarkeit des Services und wie wird dies sichergestellt?
- Welche Sicherheitsmaßnahmen werden gegen Angriffe eingesetzt (zum Beispiel DDOS, Guest Hopping, Malware...)?
- Werden Industriestandards bzgl. der Sicherheitstechniken sowie -lösungen von führenden Herstellern eingesetzt?
- Welche Leistungen bezieht der Cloud-Anbieter von Dritten? Wie werden die Sicherheitsrichtlinien hier umgesetzt?
- Wie umfassend sind die SLAs definiert – erfüllen diese die individuellen Anforderungen?
- In welchen Fällen und in welchem Umfang haftet der Cloud-Anbieter?
- Wie werden gesetzliche Anforderungen realisiert (zum Beispiel Archivierung von geschäftlichen Dokumenten,...)?
- Was passiert mit Daten nach Ablauf des Geschäftsverhältnisses? In welcher Form werden gespeicherte Daten an den Eigentümer übergeben und auf Anbieterseite gelöscht?

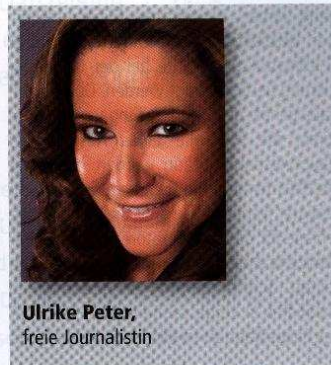
Sind diese Fragen beantwortet und die individuellen Anforderungen erfüllt, sind die Risiken kalkulierbar und die Sicherheit befindet sich auf einem hohen Niveau – oft sogar stärker, als es bei herkömmlichen und oft selbst gestrickten Inhouse-Lösungen der Fall ist. Denn gerade weil der Sicherheitsaspekt so stark im Fokus steht, ergibt sich hieraus eine erhöhte Security, da die Anbieter verstärkt darauf achten und bereits bei der Entwicklung ihrer Strategien ein besonderes Augenmerk hierauf legen. Der Dienst aus der Public Cloud muss also

nicht zwangsläufig ein erhöhtes Risiko darstellen – ganz im Gegenteil.

### Neue Maßstäbe und Standards setzen

Die Sicherheitskriterien und deren Umsetzung basieren heute größtenteils noch auf individuellen Kriterien und Vereinbarungen. „Um das Vertrauen der Nutzer nachhaltig zu stärken und Cloud-basierende Lösungen transparenter zu gestalten, wären weltweite Standards sinnvoll. Erst dann kann dieses Modell aus den Kinderschuhen herauswachsen und echte Veränderungen erwirken“, sagt Michael Eisenmann.

Zielsetzung ist es also, die Standardisierung sowie das SLA-Management weiter voranzutreiben. Dann kann das vermeintliche Risiko sich in Luft auflösen und zur Chance werden.



Ulrike Peter,  
freie Journalistin

## Schneller – besser – überall.

IT-INFRASTRUKTUR
SOFTWARE & SERVICE

www.rittal.de