COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/vertrauen-ist-gut-die-cloud-auch,2491583

Sicherheit in der Datenwolke

Vertrauen ist gut – die Cloud auch?

Datum: 18.07.2011
Autor(en): Johannes Klostermeier

Cloud Computing ist in aller Munde. Doch das Thema Sicherheit hält noch viele Unternehmen davon ab, ihre Daten auszulagern. Das zeigen auch aktuelle Studien. Zu Recht?

Die Ergebnisse der **Studien**[1] zum Thema Cloud ähneln sich. In einer weltweiten Untersuchung hat die Softwarefirma **Unit 4 Agresso**[2] 700 mittlere und große Kundenunternehmen aus zwölf Ländern über ihre Pläne mit Cloud Computing befragt. Dabei ging es um die Ausgliederung der wichtigsten Back-Office-Funktionen in die IT-Wolke.

Übereinstimmung herrschte unter denjenigen befragten Unternehmen, die sich häufig Veränderungen ausgesetzt sehen, besonders in folgenden vier Punkten: 1. Die Einführungsrate der Cloud ist 2011 konstant gegenüber dem Vorjahr; 2. Der öffentliche Bereich wird Cloud-Technologien im gleichen Ausmaß einführen wie der Wirtschaftssektor; 3. Buchhaltung und Finanzwesen werden im Vergleich zu anderen Geschäftsanwendungen wie CRM oder Personalwesen am ehesten in die Wolke überführt, und 4. Auch Unternehmensanwendungen werden innerhalb der nächsten zehn Jahre in die Cloud übergeben werden.

Dunkle Wolken: IT-Chefs fürchten Kontrollverlust, Internetabhängigkeit und Anpassungsschwierigkeiten.
Foto:

32 Prozent der Befragten gaben an, in diesem Jahr mehr für Cloud Computing ausgeben zu wollen. Die gleiche Anzahl geht von gleichbleibenden Budgets im Vergleich zum Vorjahr aus. Nur vier Prozent erwarten geringere Ausgaben, während 31 Prozent gar nicht in Cloud Computing investieren wollen. Fast die Hälfte der Befragten (334 Firmen) erklärte, derzeit keine Unternehmensanwendung Cloud-basiert zu nutzen. Dagegen befindet sich bei einem Drittel (222) bereits ein bis 25 Prozent des Back-Office in der Wolke. Gerade einmal sechs der Unternehmen unterschiedlicher Größe, Industrie und Land konstatierten, dass ihr gesamtes Back-Office Cloud-basiert läuft.

Als Nachteile des Cloud Computing wurden hauptsächlich Kontrollverlust (51 Prozent), Internetabhängigkeit (54 Prozent) und Anpassungsschwierigkeiten (38 Prozent) genannt. Als Vorteile stellten die Unternehmen die leichtere Pflege und Wartung (62 Prozent), das Automatisieren von Updates (42 Prozent) und die Skalierbarkeit (44 Prozent) heraus.

Sicherheitsbedenken[3] stehen oft an erster Stelle, wenn es um Public Cloud Services geht. „Die Ergebnisse der Untersuchung haben gezeigt, dass die Zurückhaltung insbesondere bei mittelständischen Unternehmen auf Unsicherheiten hinsichtlich der Informationssicherheit, des Datenschutzes oder Compliance“ zurückzuführen sei, lautet das Fazit von **Pricewaterhouse Coopers**[4] in der **Studie**[5] „Cloud Computing im Mittelstand“.

„Bedenken bei Governance und Compliance bestimmen den Weg in die Cloud“, melden die Markforscher von **IDC**[6], die gerade ihre **Studie**[7] „Transformation der Unternehmens-IT auf dem Weg in die Cloud, Deutschland 2011“ vorgestellt haben. Fragen der Governance (bei 34 Prozent der Unternehmen) und Compliance (24 Prozent) sowie Zweifel an der Performance und Verfügbarkeit (24 Prozent) sind die hauptsächlichen und meist genannten Hürden für eine weitere Verbreitung von Public Cloud Services, so IDC.

Die Sicherheit ist ein wirklich wichtiger Aspekt

Stefan Schröder, Entwicklungschef bei **Datev**[8], einer Genossenschaft, die schon seit langem Rechenzentren für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte betreibt, hält die Sicherheitsbedenken der Verantwortlichen nicht für übertrieben: „Das ist ein wirklich wichtiger Aspekt“, sagt er. Sein Unternehmen setzt deswegen auf Sicherheitsverfahren, die es auch schon lange vor der Cloud gegeben hat: Eine Kombination aus Wissen und Besitz, die den Zugriff auf Anwendungen und Daten sichern hilft. Der Nutzer muss sich dabei nicht nur über seine User-ID und ein Passwort identifizieren, sondern zusätzlich auch noch über andere Verfahren wie eine spezielle Smartcard.

Die Grundfrage der **Sicherheit**[9] in einem Rechenzentrum, das für mehr als einen Kunden arbeitet, ist stets die Frage: Wie sorgt der Dienstleister dafür, dass die Daten wirklich so separiert sind, dass auch jeder nur auf seine eigenen Daten zugreifen kann und auf gar keinen Fall auf die der anderen? Neben notwendigen technischen Verfahren, geht es dabei auch um menschliche Schwächen. Mit Schulungen und organisatorischen Vorgaben wie etwa dem Vieraugen-Prinzip wollen die Cloud-Anbieter dafür sorgen, dass niemand mit den Daten Unzulässiges treibt. Eine Erkenntnis der Vergangenheit lautet: Wo die Daten nicht sicher waren, sind die Angriffe meistens von den eigenen Mitarbeitern erfolgt, also von innen heraus.

Die Private Cloud ist derzeit beliebter, sagt Lynn Thorenz, Director Research & Consulting bei IDC.

„Unsere Ergebnisse zeigen, dass sich die Unternehmen momentan mit der Migration zur Private Cloud wohler fühlen“, sagt Lynn Thorenz, Director Research & Consulting bei IDC. Die Marktforscher von IDC sagen voraus, dass in Zukunft ein Mix aus unterschiedlichen Sourcing-Modellen, aus herkömmlich lokalem IT-Betrieb, sowie einer Kombination aus virtualisierten Private Clouds und Public Clouds die IT-Landschaft bestimmen werde, das der Markt aktuell aber die Private Cloud **bevorzugen**[10] würde.

Aber auch die Private Cloud muss noch um Anerkennung kämpfen: „Fehlendes **Wissen**[11] im Unternehmen“ (bei 32 Prozent der Befragten), „Unternehmens-IT ist noch nicht bereit“ (27 Prozent) und „Mangelnde Sicherheit des Rechenzentrums“ (26 Prozent) heißen hier die drei der am häufigsten genannten Problemfelder. Neben dem fehlenden **Know-how**[12] scheinen in vielen Unternehmen aber auch einige Kernvoraussetzungen für den Aufbau der Private Cloud noch nicht erfüllt zu sein. Dies betrifft die Standardisierung und Konsolidierung der IT und das Thema Virtualisierung als wichtige Vorstufe. Außerdem hätten die Unternehmen noch nicht die richtigen Tools zum Management der Private Cloud im Einsatz.

Kann ich mich darauf verlassen, dass der andere mit den Daten sorgfältig umgeht?

Auch bei der Private Cloud spielt das Thema IT-Sicherheit eine große Rolle, so IDC, jedoch stehen hier weniger Fragen der Governance und Compliance im Vordergrund, sondern die Rechenzentrumssicherheit. Immerhin 26 Prozent der Befragten haben Bedenken bezüglich der (eigenen) Sicherheit im Rechenzentrum. Nach Ansicht von **Matthias Kraus**[13], Research Analyst bei IDC, sprechen im Grunde genau diese hemmenden Faktoren bei der Private Cloud **für** eine Nutzung von Public Cloud Services.

Letztlich geht es aber bei der Überlegung, wie vertraulich die Daten der Cloud sind, natürlich vor allem um das Vertrauen in den jeweiligen Partner. Kann man sich darauf verlassen, dass er mit den Daten sorgfältig umgeht? Dabei läuft es letztlich auf die Frage hinaus, wem man überhaupt im Umgang mit wichtigen Daten vertraut. Wobei man sich klar sein muss, dass es bei der Sicherheitsfrage oft auch um die zwingend notwendige Erfüllung rechtlicher Verpflichtungen geht, die sich aus den verschiedenen Gesetzen zum Gesellschaftsrecht, Haftungsrecht, Datenschutz und Bankenrecht oder aus Basel II und dem Sarbanes-Oxley Act ergeben. Das **Bundesamt für Sicherheit in der Informationstechnik**[14] hat gerade in einem „**Eckpunktepapier**[15] Cloud Computing“ die Mindestanforderungen zur Informationssicherheit bei Cloud Computing Diensten formuliert. Hierzu zählen auch Themen wie Vertragsgestaltung, Datenschutz und Mandantenfähigkeit.

Eine deutsche Cloud ist vielen IT-Verantwortlichen lieber - weil vermeintlich sicherer.
Foto: zentilia - Fotolia.com

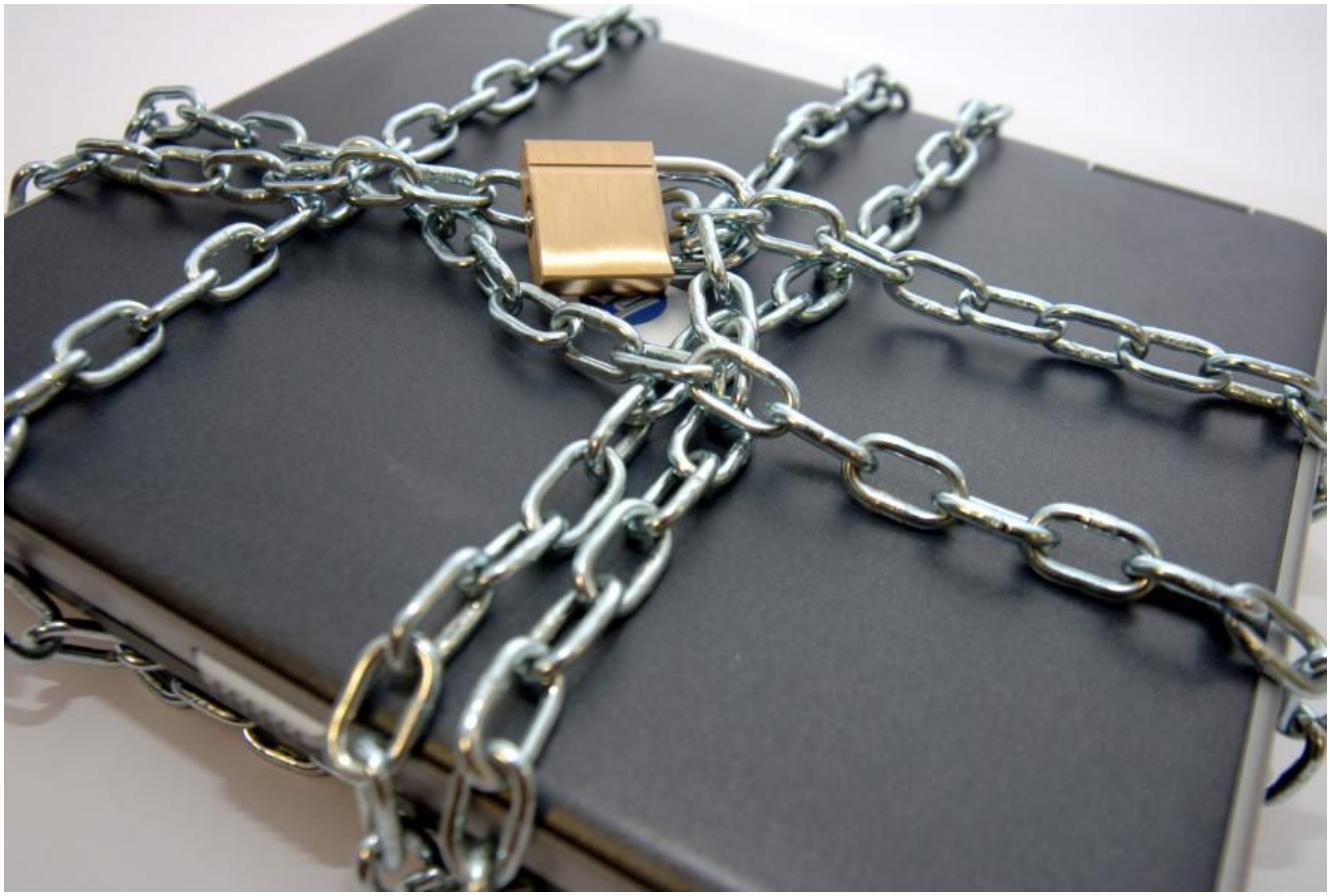
Für manchem deutschen Unternehmensverantwortlichen könnte eine deutsche Cloud, bei der die Daten auch tatsächlich in Deutschland bleiben, ein Mehr an Vertrauen schaffen. Bei vielen der großen allgemeinen Cloud-Anbieter, die weltweit agieren sind, können sich die Verantwortlichen nicht immer genau sicher sein, wo die Daten gerade liegen oder wohin sie gespiegelt werden. Denn das ist ja gerade das Prinzip der Cloud: Die Daten wandern zwischen den Servern hin und her.

Allerdings sollten IT-Leiter und CIOs auch bedenken, ob ihre bisher praktizierte Datenspeicherung wirklich so sicher wie gedacht ist. Oder wie es IDC formuliert: „Die dezentrale und redundante Datenhaltung kann Anwenderunternehmen zudem ein großes Plus an Datenausfallsicherheit bieten, die sich kaum ein Unternehmen mit einem eigenen Rechenzentrum selbst leisten kann. Fällt das eigene Rechenzentrum aus und die IT-Systeme stehen still, hilft auch die Kenntnis des Datenstandorts wenig.“ Das Thema „Sicherheit“ kann so betrachtet also auch zu einem Antriebsfaktor für Cloud Services werden. Denn für die Anbieter von Cloud Services gehört die Gewährleistung der Sicherheit der Daten natürlich zum Kerngeschäft.

Auch das **Fraunhofer Institut SIT**[16] stellt in seiner Studie „Vergleich der Sicherheit traditioneller IT-Systeme und Public Cloud Computing Systeme“ fest: „Im traditionellen Modell muss der Konsument das Sicherheitskonzept selbst vollständig im Unternehmen implementieren. In diesem Fall ist er für die stetige Aktualität seiner Anwendungen verantwortlich. Dies umfasst Konfiguration, Betrieb, Wartung, Änderungsmanagement und Sicherheitstests der Anwendungen und spiegelt sich zudem in höheren Kosten wieder. Im Software-as-a-Service-Fall bezieht der Konsument eine Anwendung als Service, die immer aktuell mit dem neusten Sicherheitsstandard verfügbar ist.“

Die Cloud ist oft sicherer als das eigene Rechenzentrum

Darauf weisen natürlich auch die Cloud-Anbieter gerne hin. So hat das IT-Sicherheitsunternehmen **Check Point Software**[17] mit den Marktforschern von Ponemon herausgefunden: In Deutschland kam es im vergangenen Jahr bei rund 83 Prozent der Unternehmen zu Datenverlusten. Dabei sind in erster Linie Kundeninformationen (52 Prozent), aber auch Mitarbeiterdaten (28 Prozent) und Geschäftspläne (20 Prozent) betroffen.



Hauptursache für Datenverluste: Hardware geht verloren oder wird gestohlen.
Foto: LEWIS

Jedoch waren die Hauptursache für den Datenverlust mitnichten Hackerangriffe, sondern der Diebstahl oder der Verlust von Hardware. „In 31 Prozent der Fälle geht der Datenverlust auf verlorene oder gestohlene Hardware zurück, dabei ließe sich gerade diese Lücke so einfach schließen“, wirbt Jürgen Schüssler, Geschäftsführer von **Wice**[18], für seine webbasierten CRM-Systeme. Und weiter: „Eine webbasierte Lösung könnte dies zu hundert Prozent verhindern, denn die Daten sind sicher auf dem zentralen Rechner in einem Hochleistungsrechenzentrum gelagert.“

Links im Artikel:

[1] **https://www.computerwoche.de/netzwerke/2489273/**
[2] **http://unit%204%20agresso/**
[3] **https://www.computerwoche.de/netzwerke/mobile-wireless/2485371/**
[4] **http://www.pwc.de/de/**
[5] **http://www.pwc.de/de/mittelstand/cloud-computing-im-mittelstand.jhtml**
[6] **http://www.idc.de/**
[7] **http://www.idc.de/press/presse_mc_cloud2011.jsp**
[8] **http://www.datev.de/**
[9] **https://www.computerwoche.de/management/it-services/2357492/**
[10] **https://www.computerwoche.de/management/it-strategie/2367187/**
[11] **https://www.computerwoche.de/management/it-services/1879547/**
[12] **https://www.computerwoche.de/subnet/telekom/cloud-computing/2484316/**
[13] **http://www.idc.de/research/cv_kraus.jsp**
[14] **http://www.bsi.de/**

[15] **https://www.bsi.bund.de/cloud**
[16] **http://www.sit.fraunhofer.de/**
[17] **http://www.checkpoint.com/**
[18] **http://www.wice.de/**
