Computerworld 12/17. Juli 2015
→ **www.computerworld.ch**

FOKUS: STORAGE

Sicher in die Cloud – aber wie?

Viele CIOs zögern, Daten in die Cloud auszulagern. Am meisten beschäftigt sie die Frage nach der Sicherheit ihrer Informationen. Wie profitieren CIOs dennoch von den Vorteilen der Cloud und kommen gleichzeitig ihrer Verantwortung nach?

→ **VON PIUS GRÜTER**

Kosteneinsparungen und Effizienzsteigerungen – die meistgenannten Vorteile der virtuellen Infrastruktur – sind schlagende Argumente für die Verlagerung der IT in die Cloud. Bei einer genaueren Betrachtung fällt es IT-Verantwortlichen jedoch schwer, die von ihnen geforderte Informationssicherheit zu verantworten. Schliesslich müssen sie sicherstellen, dass die Informationen vertraulich, integer und authentisch bleiben und jederzeit verfügbar sind.

Das Angebot vieler Cloud-Anbieter ist verlockend, aber intransparent. Weder der Datenstandort noch die eingebundenen Partnerunternehmen sind bekannt und beeinflussbar. Der Mangel an weitverbreiteten internationalen Standards macht es schwer, Anbieter zu beurteilen und zu vergleichen. Eine unüberwindbare Hürde? Nicht unbedingt – aber eine genaue Prüfung der rechtlichen Rahmenbedingungen, der physischen Infrastruktur und der involvierten Unternehmen ist dringend zu empfehlen.

«Ohne spezifische Zertifizierung des Anbieters ist eine Auslagerung von Datensammlungen in die USA nicht erlaubt»

Pius Grüter

Pius Grüter ist CIO bei green.ch
→ **www.green.ch**

EINHALTUNG DES DATENSCHUTZES

Personenbezogene Datensammlungen unterliegen dem Schweizer Datenschutzgesetz (DSG). Diese Daten dürfen nur zu dem Zweck bearbeitet werden, der bei ihrer Beschaffung angegeben wurde. Für das Gesetz gilt die Auslagerung solcher Daten an einen Cloud-Anbieter als eine Datenbearbeitung durch Dritte. Dies ist zwar grundsätzlich erlaubt, allerdings nur unter der Voraussetzung, dass die Daten dort nicht anders bearbeitet werden, als es das auslagernde Unternehmen selber tun würde. Die Verantwortung dafür und für die Sicherheit der Daten liegt beim auslagernden Unternehmen – und ebenso die Einhaltung der Gesetze durch involvierte Partner des Cloud-Anbieters.

Die Nutzung ausländischer Datenstandorte erlaubt das DSG nur, wenn die lokalen Gesetze ein DSG-konformes Schutzniveau bieten. Welche Länder den gewünschten Schutzgrad erreichen, kann beim Eidgenössischen Datenschutzbeauftragten in Erfahrung gebracht werden. Ohne eine zusätzliche Zertifizierung des Anbieters ist etwa eine Auslagerung von Datensammlungen in die USA aufgrund lokaler Gesetze wie dem Patriot Act nicht erlaubt.

Aber auch im Inland ist eine genaue Prüfung der rechtlichen Rahmenbedingungen erforderlich. Abhängig von der Branche kommen weitere Pflichten (z. B. Finma, ISAE 3402) hinzu. In den letzten Jahren hat sich die ISO-Norm 27001 etabliert. Sie verpflichtet zertifizierte Unternehmen, Ziele, Prozesse und Mittel zur Sicherung von Informationen zu definieren und Schutzmassnahmen umzusetzen.

Mehr Infos zur rechtlichen Situation bei einer Cloud-Auslagerung finden Sie in der Computerworld 10/2015 (Swiss CIO) ab Seite 32.

INFRASTRUKTUR ZENTRAL

Der Begriff Cloud Computing sollte nicht darüber hinwegtäuschen, dass die IT nach wie vor einen festen physischen Standort in einem oder mehreren Rechenzentren hat. Aber wo? Während diese Frage für Privatnutzer nebensächlich sein mag, ist sie für Firmen zentral. Ein optimal gesicherter Primärstandort des Cloud-Anbieters liegt in einer risikoarmen, aber gut erschlossenen Zone und ist durch geeignete physische Sicherheitsmassnahmen vor unbefugten Zugriffen geschützt. Die gleichen Kriterien gelten selbstverständlich auch für den Backup-Standort. Dieser sollte zur Wahrung der Business-Continuity in ausreichender Distanz zum Primärrechenzentrum liegen.

Die sogenannten Tier-Levels, die Rechenzentrumsanbieter zur Klassifizierung ihrer Service-Leistungen nutzen, geben Aufschluss über die vorhandenen Redundanzen bei der Strom-, Klimatisierungs- und Netzwerkinfrastruktur. Die höchsten Anforderungen an einen Cloud-Service erfüllen derzeit nach Tier IV zertifizierte Standorte. Sie bieten eine Verfügbarkeit von 99,995 Prozent. Viele Anbieter organisieren auf Anfrage die Prüfung der Infrastruktur vor Ort.

WAHL DER LEISTUNGSERBRINGER

Mit Wachstumsraten von über 40 Prozent pro Jahr ist der Cloud-Markt der derzeit dynamischste ICT-Bereich. Neue Dienstleistungen entstehen fast täglich, ebenso neue Anbieter. Es empfiehlt sich daher, Unternehmen und Dienstleistungsmodelle in Bezug auf Service-Leistungen, Zertifizierungen, Rentabilität und Zukunftssicherheit besonders kritisch zu betrachten. Wichtige Hinweise geben die Kundenreferenzen.

Der Cloud-Anbieter sollte dem Kunden die freie Wahl von Support- und Umsetzungspartner überlassen. Denn welche Zusammensetzung für den Einstieg in die Cloud sinnvoll ist, hängt vom jeweiligen Projekt ab. Damit die Vorteile der Cloud – Kosteneinsparungen und Effizienzgewinn – zum Tragen kommen, ist eine Reduktion auf möglichst wenige spezialisierte Leistungserbringer ratsam. Dies vereinfacht auch die Zuordnung der Verantwortlichkeiten – von der Infrastruktur über die Virtualisierung bis hin zum Support der Anwendung.

Erfolgt die Auslagerung in die Cloud zunächst nur für eine begrenzte Funktion oder einen Prozess, so erweist sich dies bei positivem Verlauf oft lediglich als erster Schritt, dem weitere folgen. Es empfiehlt sich deshalb, bereits zu Beginn abzuklären, welche Zukunftsperspektiven der Cloud-Partner bietet. Welche Schnittstellen stehen beispielsweise zur Verfügung, und was leistet die Managementkonsole? Ist es verhältnismässig einfach, Testumgebungen aufzubauen und Anwendungen in die Cloud oder wieder zurück in die eigene Infrastruktur zu verlagern? Sind beim Cloud-Anbieter mehrere Datenstandorte wählbar, und bietet er auch Lösungen für hybride Clouds? Es lohnt sich, schon bei der Partnerwahl genau hinzuschauen, welche Plattform zum Einsatz kommt und wie der Partner sie weiterentwickelt.

FAZIT: KEIN GRUND ZUM VERZICHT

Auch verantwortungsvolle CIOs müssen auf den Einsatz von Cloud Computing keinesfalls verzichten – wenn sie ihn überlegt angehen und sich aller Implikationen bewusst sind. Vor allem Unternehmen, die im Zusammenhang mit der Benutzung eines Cloud-Services Datensammlungen oder geschäftskritische Anwendungen in die Wolke auslagern wollen, sollten die geplanten Dienstleistungen im Vorfeld genau prüfen. ←

BILD: ISTOCKPHOTO.COM/JIRSAK

Was im Vertrag drinstehen muss

Ein Cloud-Service-Vertrag sollte (gegebenenfalls zusammen mit ergänzenden Vereinbarungen) zusätzlich zu herkömmlichen Aspekten wie Preis und Leistung folgende Punkte klar regeln:

- Wie sieht das Service Level Agreement (SLA) aus?
- Welche Konsequenzen zieht die Nichterfüllung des SLAs nach sich?
- Wie orientiert der Anbieter den Kunden über Wartungsfenster, Updates und Unterbrüche?
- Welche Untervertragspartner beschäftigt der Anbieter?
- Welche Verantwortung fällt dem Kunden zu, welche dem Anbieter?
- Wie orientiert der Anbieter über Verstösse gegen gesetzliche oder vertragliche Bestimmungen in seiner Verantwortung?
- Wie und in welchem Format erhält der Kunde im Kündigungsfall seine Daten zurück?
- Wie erfolgt die Überprüfung der versprochenen Leistungen und Massnahmen?
- Wie sehen das Sicherheitskonzept und die Sicherheitsarchitektur aus?
- Welche Notfalltests führt der Anbieter regelmässig durch?