

→ VON ULRIKE PETER

Die Frage, ob die Cloud nur eine weitere IT-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 nicht nur Nerven, sondern auch viel Geld investieren. Die schnelle Verfügbarkeit, eine Abrechnung nach tatsächlicher Nutzung und der daraus resultierende Kostenvorteil sowie Flexibilität sind in Zeiten von Optimierungsstrategien und Einsparndruck stichhaltige Argumente. Während manche Unternehmen ihre Geschäftsprozesse bereits mehr und mehr in die Cloud verlagern, blicken andere noch rat- und wolkenlos in die Zukunft.

Michael Eisenmann, IT-Security-Consultant beim Global-Sourcing-Spezialist NIIT Technologies, nennt die Hauptursachen für die Unsicherheit der skeptischen Unternehmen: «Über IT in der Wolke wird viel diskutiert, aber meist wenig gesagt – es herrscht immer noch ein Informationsdefizit. Zu viele Ansätze, die unterschiedliche Interpretation und der breite Aktionsspielraum in einem noch grösstenteils unerprobten Umfeld führen schlichtweg zu Verwirrung auf Anwenderseite.»

Die Dienstleister sind daher gefordert, ihre Angebote transparent zu gestalten und klar im Markt zu positionieren. Auf Anwenderseite 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, Funktion, Branche etc. recht stark. Besonders schwierig gestaltet sich die Auslagerung in die Public Cloud. «Die grösste Chance auf Erfolg haben deshalb in Zukunft standardisierte und strukturierte Services, die sinnvoll in die Unternehmensstrategie eingebunden und kontrolliert werden können, um klare Leistungs- sowie Kostenvorteile zu erzielen», meint Eisenmann.

**EINE FRAGE DER SICHERHEIT**

Eines der stärksten Kontra-Argumente, die Kritiker hinsichtlich Cloud Computing ins Feld führen, ist der Sicherheitsaspekt. Der negative Beigeschmack, Daten aus der Hand zu geben und damit gefühlt die Kontrolle zu verlieren,

bremsst viele Unternehmen aus. Gerade, wenn sie gesetzlichen Anforderungen wie dem Schutz personenbezogener Daten oder bei der Archivierung unterliegen, ist das Misstrauen oft gross. Diese Einstellung ist nicht einmal unberechtigt, denn es gibt einige Cloud-Anbieter, die diese Richtlinien nicht erfüllen können oder sich bewusst nicht daran halten.

Daher steht an erster Stelle, die eigenen Sicherheitsanforderungen zu definieren und einen potenziellen 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 (siehe rechts) hilft bei der Definition der eigenen Anforderungen und der damit einhergehenden Sondierung des richtigen Anbieters. Sind alle Fragen beantwortet und die individuellen Anforderungen erfüllt,



«Um das Vertrauen der Kunden zu gewinnen, sind weltweite Standards nötig»

Michael Eisenmann, NIIT Technologies

wird das Risiko kalkulierbar. Gerade weil der Sicherheitsaspekt so stark im Fokus der Anwender steht, legen auch viele Anbieter bereits bei der Entwicklung ihrer Strategien ein besonderes Augenmerk darauf. Oft ist das Sicherheitsniveau der Public Cloud sogar höher als bei herkömmlichen, selbst gestrickten Inhouse-Lösungen.

**MASSTÄBE UND STANDARDS SETZEN**

Die Sicherheitsstrategien und deren Umsetzung basieren heute grösstenteils noch auf individuellen Kriterien und Vereinbarungen. Für Eisenmann kein zufriedenstellender Zustand: «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.»

Ziel muss also sein, die Standardisierung sowie das SLA-Management weiter voranzutreiben. Dann kann sich das vermeintliche Risiko in Luft auflösen und zur Chance werden. ←

Ulrike Peter schreibt als Fachautorin unter anderem für NIIT Technologies → [www.niit-tech.de](http://www.niit-tech.de)

**Cloud Security Check**

Die folgenden Fragen sollen dabei helfen, die Security-Vorkehrungen eines potenziellen Providers zu durchleuchten.

- Wie transparent ist der angebotene 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 bei Transport und 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 dieser sichergestellt?
- Welche Sicherheitsmassnahmen werden gegen Angriffe eingesetzt (z. B. DDOS, Guest Hopping, Malware etc.)?
- Werden Industriestandards bzgl. der Sicherheitstechniken sowie -lösungen von führenden Herstellern eingesetzt?
- Welche Leistungen bezieht der Cloud-Anbieter von Dritten? Wie werden die Sicherheitsrichtlinien in diesem Fall umgesetzt?
- Wie umfassend sind die SLAs definiert und erfüllen diese die individuellen Anforderungen?
- In welchen Fällen und in welchem Umfang haftet der Cloud-Anbieter?
- Wie werden gesetzliche Anforderungen realisiert (z. B. Archivierung von geschäftlichen Dokumenten etc.)?
- Was passiert mit den Daten nach Ablauf des Geschäftsverhältnisses? In welcher Form werden gespeicherte Daten an den Eigentümer übergeben und auf Anbieterseite gelöscht?