COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/5-fragen-an-den-provider,2535634

Worauf es bei der Cloud Security ankommt

5 Fragen an den Provider

Datum: 09.04.2013
Autor(en): Werner Kurzlechner

Cloud Computing eröffnet auch neue Wege bei der Sicherheit. Anwender sollten allerdings mit dem Provider vorab vor allem fünf Security-Fragen klären.

Foto: ollyy, Shutterstock.com

Cloud Security ist mittlerweile ein Phänomen mit zwei Gesichtern – und das ist in diesem Fall eine gute Nachricht. Denn das eine altbekannte Antlitz jagte vielen Anwendern lange Furcht ein, so zerfurcht und löchrig sah es aus. Seine Botschaft: Beim Cloud Computing werden naturgemäß Daten aus dem eigenen Beritt gegeben – und das hat eine ganze Reihe von Anfälligkeiten und Sicherheitsrisiken zur Folge. Analystenhäuser wie Gartner geben mittlerweile aber auch dem zweiten Gesicht Konturen und Profil. Und dieses blickt aus Anwendersicht äußerst freundlich drein.

Denn die Wolke birgt im Hinblick auf die IT-Sicherheit nicht nur neue Gefahren, sondern auch neue Chancen. So sagt Gartner voraus, dass sich die Cloud in den kommenden Jahren zu einem bevorzugten Liefermodell für Sicherheitslösungen entwickeln werde. „Die Beliebtheit und der wachsende Einsatz von cloud-basierten Security-Services wird – wenngleich in unterschiedlichem Ausmaß – die Gestalt künftiger Security-Märkte beeinflussen“, sagt Gartner-Analyst Ruggero Contu. Die Ablösung traditioneller physischer Hardware-Plattformen durch Virtualisierung führt demnach auch dazu, dass im Bereich der Netzwerksicherheit immer mehr virtuelle Applikationen zum Einsatz kommen.

Kompatibilität, Performance und Zugänglichkeit klären

Es schadet sicherlich nicht, wenn Anwender auch diese Entwicklung bei ihren Gedankenspielen um Cloud-Sicherheit im Hinterkopf haben und dieses Potenzial der Wolke berücksichtigen. Konkret dürften die meisten Unternehmen aber derzeit noch weniger strategische Aspekte im Blick haben. Zunächst zählt die Gewissheit, dass der Provider der Wahl auch die Security-Fragen so adressiert, dass man als Anwender keine Bedenken haben muss. Hilfreich ist dabei sicherlich ein Katalog der wichtigsten Fragen, die man einem möglichen Provider vor der Vertragsunterzeichnung zur Cloud-Sicherheit stellen sollte.

Wer im Internet nach den fünf wichtigsten Fragen dazu sucht, wird eine Menge an Material finden. Was letztlich nützt, hängt offenbar ganz von der individuellen Lage ab. Fragen nach der Kompatibilität des Providers mit den eigenen Systemen oder nach Performance und Zugänglichkeit müssen kleineren und mittleren Firmen womöglich ins Gedächtnis gerufen werden, anderen Unternehmen erscheint derlei als Selbstverständlichkeit. Insofern lohnt der Versuch, die wirklich entscheidenden Fragen herauszufiltern, die man dem Cloud-Provider zum Thema Sicherheit stellen sollte:

1. Was genau passiert mit den Daten? Eine allgemeine Verständnisfrage, die nichtsdestotrotz von entscheidender Bedeutung ist. Man sollte sich vom Provider so exakt wie möglich erläutern lassen, wie Datentransfer und -lagerung ablaufen und wo genau die Daten deponiert werden, um im Bilde zu sein und die Sachlage beurteilen zu können. Aber auch, um selbst flankierende Maßnahmen zur Datensicherheit einleiten zu können. Analysten weisen in jüngster Zeit immer wieder darauf hin, dass viele Unternehmen blind darauf vertrauen, dass ihr Provider schon für adäquate Security sorgen wird. Es empfiehlt sich indes, selbst immer aktiv am Ball zu bleiben.

Notfallpläne des Providers prüfen

2. Was geschieht bei einem Ausfall? Selbstverständlich lautet der Anspruch beim Cloud Computing, dass alle Services immer verfügbar sind. Aber die Erfahrung lehrt, dass es dafür wie so oft im Leben keine Garantie gibt. Ausfälle kommen vor – nicht oft, aber ein Restrisiko besteht. Dieses gilt es, umfassend abzuklopfen. So sollte man sich nach der Robustheit der Cloud-Umgebung erkundigen. Das beinhaltet zum Beispiel die Frage, ob das Rechenzentrum womöglich in einem Gebiet liegt, in dem Naturkatastrophen drohen. Eine genaue technische Prüfung ist ratsam. Man sollte sich ebenso über die Notfallpläne erkundigen, womöglich sogar durch einen Ortsbesuch mit Audit.

„Nur weil der Anbieter über einen Notfallplan verfügt, bedeutet das nicht, dass dieser auch funktioniert“, warnt indes Cloud-Experte René Büst auf seinem Portal Clouduser.de. Es könne sinnvoll sein, sich die Ergebnisse der letzten Tests zeigen zu lassen und diese Option vertraglich zu verankern. Büst weist auch auf die Möglichkeiten hin, bei den Service Level Agreements (SLAs) – in der Regel gegen Aufpreis – ein höheres Anspruchsniveau zu verhandeln und eventuell eine Vorzugsbehandlung für den Fall der Fälle auszuhandeln.

3. Wie aktiv werden Sicherheitsfragen angegangen? Man sollte herausfinden, ob es beim Provider wirklich ein aktives Team gibt, das sich um Security kümmert. Hier reicht es nicht aus, sich über formale Qualifikationen zu unterrichten. Besser sucht man das Gespräch mit den Experten des Providers und gewinnt so einen Eindruck von vorhandenen Erfahrungen und Kenntnissen.

4. Gibt es einen Prozess für Vorfälle? Sicherzustellen ist, dass der Provider proaktiv nach Schwächen und Sicherheitslücken auf seiner Plattform sucht. Bestehen sollte man auf aktivem Monitoring sowie auf Support und Information, sobald Probleme auftreten. Einzufordern sind in diesem Zusammenhang monatliche Berichte, regelmäßiger Informationsfluss oder sogar Meetings, um Probleme und Handlungsbedarf zu erörtern.

5. Wie ist es um die Due Diligence bestellt? „Neben den technischen Prüfungen ist es ebenfalls interessant zu wissen, wie der Anbieter zum Beispiel auf der finanziellen Seite aufgestellt ist, um seine eigenen Rechnungen zu bezahlen“, lautet ein weiterer Tipp von Cloud-Experte Büst. Denn was nütze eine sehr robuste Infrastruktur, wenn der Anbieter auf Grund einer Insolvenz plötzlich nicht mehr erreichbar ist?
