Nutzen vs. Risiken

Sicherheit in der Cloud

Der Begriff «Cloud Computing» (frei übersetzt: Rechnen in der Wolke) ist zu einem richtigen Hype geworden. Praktisch jeder spricht darüber, alle Zeitschriften berichten darüber. Dieser Artikel geht nicht auf die Cloud ein, sondern soll einige Facetten der IT-Sicherheit zeigen, die es zu beachten gibt.

Autor: Andreas Wisler

Gemäss einer aktuellen Studie der IDC ist die Erhöhung der IT-Sicherheit eines der grössten Ziele, um die Cloud zu nutzen. Aber genau dieser Punkt ist auch das grösste Hindernis, die eigene Infrastruktur in fremde Hände zu geben. Die Cloud wird für verschiede Arten genutzt: Auslagerung von Rechenkapazität respektive Datenspeicher (Infrastructure-as-a-Service, kurz IaaS), fertigen Programmpaketen (Software-as-a-Service, kurz SaaS) und Programmierumgebungen (Platform-as-a-Service, kurz PaaS). Der Vorteil darin liegt in der einfach skalierbaren Lösung. Jedoch gilt es auch die Sicherheitsrisiken frühzeitig in die Planung einzubeziehen. Davon betroffen sind vor allem die Integrität und die Vertraulichkeit der Daten.

Der menschliche Faktor

Je nach Anbieter der Cloud-Lösung werden die Administratoren-Rechte komplett dem Kunden übergeben. Andere ermöglichen ihren eigenen IT-Angestellten kompletten Zugriff auf die Kundendaten. Auch im ersten Fall muss sich der Anbieter um die Verteilung der Daten (Redundanz) respektive um deren Sicherung kümmern. Dazu benötigt er in der Regel ebenfalls Zugriff auf die Daten. Auf jeden Fall besteht die Gefahr, dass die Kontrolle über den Zugriff auf die eigenen Daten abgegeben wird. Somit ist nicht mehr klar, wer genau auf diese Daten zugreifen kann.

Generell kann natürlich davon ausgegangen werden, dass die Administratoren vertrauenswürdig sind. Doch welcher IT-Angestellte musste schon je seine Identität beweisen, zum Beispiel mit der Identitätskarte, oder seine Vergangenheit offenlegen, zum Beispiel mittels Strafregisterauszug? Vermutlich die wenigsten. Verschiedene aktuelle Fälle zeigen, dass es immer wieder geschieht, dass sich jemand eine andere Identität aufbaut und so unbemerkt einen Datendiebstahl durchführen kann.

Eine vertragliche Lösung könnte eine Abhilfe sein (durch Definieren einer einzelnen oder mehrerer Personen), doch dies widerspricht der Idee von Cloud Computing. Somit bleibt nur eine Verschlüsselung der Daten, um den Zugriff auf die eigenen Daten sicherzustellen. Bei einem Online-Datenspeicher stellt dies in der Regel kein Problem dar, ja wird sogar von einigen Anbietern direkt in die zu nutzende Software integriert. Anders sieht es jedoch aus, wenn eine Applikation in der Cloud genutzt wird. Diese Applikation muss verständlicherweise auf die Daten zugreifen können und erwartet diese in unverschlüsselter Form.

Für einen Cloud-Anbieter macht die Lösung nur dann einen Sinn, wenn er die vorhandenen Ressourcen auf mehrere Kunden aufteilen kann. Dies stellt den nächsten «Knackpunkt» dar. Der Anbieter muss garantieren, dass die Daten sicher voneinander getrennt sind. In virtualisierten Umgebungen stellt dies, je nach Software, kein Problem dar. Die Virtualisierung von Kundendaten gehört hingegen nicht dazu (bzw. es sind erst sehr wenige zertifizierte Lösungen auf dem

Zum Autor

Andreas Wisler, Tel.: 052 320 91 20, Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. System Hardening rundet das Profil ab. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) heruntergeladen werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.

Markt, die dies beherrschen und dadurch sehr teuer sind). Dies gilt auch für Datenbanken. Der Anbieter muss den Spagat zwischen sicherer Datenseparierung und den Kosteneinsparungen machen. Es empfiehlt sich, genau abzuklären, wie der Anbieter mit dieser Problematik umgeht und welche Lösungen er umgesetzt hat.

Beachtet werden müssen auch länderspezifische Gesetze und rechtliche Anforderungen. So verbietet es das Schweizerische Datenschutzgesetz, Daten ins Ausland zu transferieren, wenn keine Gesetzgebung zum Schutz dieser Daten besteht (DSB, Art 6, Abs 1). Die EU erfüllt diese Anforderung, Amerika gehört hingegen nicht dazu. Viele Cloud-Anbieter haben darauf reagiert und bieten ihre Cloud-Umgebungen in der EU an. Sollte jedoch ein Rechenzentrum ausfallen, werden die Daten an einen anderen Standort transferiert (oder sind bereits redundant dort abgelegt). So kann es schnell geschehen, dass die Datenschutzbestimmungen verletzt werden. Dieser Umstand sollte ebenfalls schriftlich festgehalten werden.

Notfallplan erarbeiten

Oft wird unterschätzt, dass durch die Auslagerung eines Dienstes mehr Single Points of Failure entstehen, als gelöst werden. Zwischen dem eigenen Netzwerk und dem Anbieter entsteht ein grösseres Netzwerk mit weiteren Komponenten. Damit erhöht sich auch die Gefahr von Ausfällen. Klar kann dies wiederum durch Redundanzen gelöst werden (beispielsweise durch eine redundante Internet-Anbindung zum Anbieter), doch auch dies widerspricht dem Cloud-Gedanken, da die Netzwerkpfade auf Seiten des Anbieters unbekannt sind. Oft sind auch verschiedene Provider zwischen dem eigenen Netzwerk und der Cloud. Daher sollte als dritter zu regelnder Punkt auch ein Nachweis über die Ausfallsicherheit des gesamten Netzwerkpfades definiert sein. Zusätzlich lohnt es sich, bereits im Vorfeld einen entsprechenden Notfallplan zu erarbeiten.

Bevor die Wahl auf einen Anbieter fällt, sollten folgende Elemente beachtet werden:

- Verfügbarkeit der Cloud-Security-Lösung
- Zertifizierung des Cloud-Anbieters (SAS 70 Type II, ISO 27001)
- Transparenz bezüglich der Lokation der Daten
- Unabhängigkeit gegenüber dem Anbieter
- Umsetzung von Standards (ISO 20000, ITIL)

Die Cloud stellt alle beteiligten Parteien vor neue Herausforderungen, für welche es nur teilweise befriedigende Lösungen gibt. Daher sollten alle erwähnten Problemfelder für den eigenen Einsatzzweck gründlich überprüft und schriftlich festgehalten werden. Eine zusätzliche Risiko-Analyse hilft, die möglichen Schwachpunkte zu erkennen und im Vorfeld geeignete Massnahmen umzusetzen. ◆