Wie presst man eine Wolke in einen Rahmen?

Neue IT-Services erfordern neue Verträge. Der Cloud-Kunde verliert Kontrolle an den Dienstleister. Gegen schädliche Folgen sollte er sich absichern.

Von **Thomas Fischer***

Daten und Dienste können in die Cloud entschwinden und grenzenlos verfügbar sein. Die Verantwortung für das Funktionieren der IT bleibt jedoch bei dem auslagernden Unternehmen vor Ort. Es ist der zwangsläufige Verlust an Einwirkungs- und Kontrollmöglichkeiten in einer Public Cloud, der immer mehr dazu führt, dass der „Evolution in der Technik" auch ein Wandel in der Vertragsgestaltung folgen muss.

Nun mag es so sein, dass „partnerschaftliche Beziehungsgeflechte auf der Basis von Vertrauen in Netzwerken" (so ein Bitkom-Leitfaden) die Grundlage für erfolgreiche Cloud-Computing-Geschäftsmodelle bilden. Aber jeder IT-Verantwortliche wird sich daran messen lassen müssen, ob und wie er dieses Vertrauen rechtlich abgesichert hat. Zu den Punkten, die zu berücksichtigen sind, zählen:

- Spezifizierung und Abgrenzung der zu erbringenden Leistungen;
- angemessene Steuerungs- und Weisungsrechte;
- effiziente Informations- und Prüfungsrechte (durch Dritte);
- Kündigungsrechte und faktische Kündigungsmöglichkeit;
- Gewährleistung der Datensicherung und des Datenschutzes sowie die
- Sicherung der Kontinuität von Leistungserbringung bei Vertragsbeendigung.

Diese Grundanforderungen an jeden Sourcing-Vertrag muss der IT-Verantwortliche auf den Cloud-Vertrag übertragen. Gleichzeitig sollte er dabei die Besonderheiten des Cloud Computing im Blick haben. Sein Vorgehen sollte sich an vier Eckpunkten orientieren: Öffnen, Bestimmen, Begrenzen und Kontrollieren.

Öffnen: Am Anfang an das Ende denken

„Der Provider darf nicht die faktische Macht haben, uns den Datenzugang zu verweigern." Diese Äußerung von Ralf Schneider, CIO der Allianz Gruppe, in der COMPUTERWOCHE (Ausgabe 15/2011, Seite 13) bringt das Problem auf den Punkt. Ist nun die Konsequenz daraus, jede Public Cloud zu meiden? Die Antwort auf diese Frage wird gerade bei mittelständischen Unternehmen davon abhängen, inwieweit der Weg in das Cloud Computing für sie notwendig ist, um den Zugang zu technischen Innovationen zu erhalten.

Wer diesen Weg beschreitet, muss insbesondere den „Lock-in-Mechanismus" verhindern. Sprich: Eine Abhängigkeit von dem jeweiligen Provider sollte unter allen Umständen vermieden werden. Entscheidend hierfür ist das Vorhandensein eines realistischen Exit-Szenarios. Die Grundlagen dafür sind im Vertrag zu legen.

Folgende Regelungen sollte der Kunde berücksichtigen, formulieren und vertraglich vereinbaren:

- Weitgehender Ausschluss von Leistungsverweigerungsrechten des Providers;

Foto: Fotolia.com/kestro; Bitkom

- Verpflichtung zur Datenreplikation beim auslagernden oder einem dritten Unternehmen;
- Bindung des Providers an Marktstandards, die einen Übergang zu einem anderen Provider ermöglichen;
- konkretes Exit-Szenario, das bereits vor Vertragsschluss verhandelt und während der Laufzeit ständig aktualisiert wird;
- Verpflichtung des Providers zur Unterstützung beim Exit und
- Erwerb von zwingend benötigten Lizenzen im Exit-Szenario.

Bestimmen: Individuelle Anforderungen versus Standards

Wesentliches Merkmal des Cloud Computing ist die Standardisierung. Der Möglichkeit für eine Individualisierung sind zwangsläufig Grenzen durch das Geschäftsmodell gesetzt.

Erforderlich ist zudem eine ständige technische Weiterentwicklung der Plattform. Gerade die Änderungen in der Cloud können aber mit den berechtigten Interessen des auslagernden Unternehmens an Planungssicherheit und Investitionsschutz kollidieren.

So notwendig die Rechte des Providers zur eigenen Gestaltung der Cloud auch sind, sie dürfen nicht dazu führen, dass der Anbieter faktisch ein einseitiges Leistungsbestimmungsrecht erhält. Denn damit wäre ihm das auslagernde Unternehmen ja ausgeliefert. Regelungsbedarf besteht auch in Hinblick auf Möglichkeit und Grenzen der Individualisierung sowie auf den Schutz der Individualisierung bei Änderungen in der Cloud.

Die Regelungen im Vertrag, die hier Klarheit schaffen können, sehen etwa so aus:

- Festlegen von unveränderbaren Leistungsinhalten;
- Vereinbarung eines Rahmens für Leistungsbestimmungsrechte des Providers und des auslagernden Unternehmens;
- Bestimmen der Geräte-, Software- und Prozesshoheit;
- Möglichkeit der Individualisierung in der Cloud regeln – auch durch den Einsatz von Dritten;
- hierbei die notwendigen Haftungsbeschränkungen für das auslagernde Unternehmen berücksichtigen;
- die Leistungen des Providers und weiterer Beteiligter in Einklang bringen, vor allem die Service-Levels über die gesamte Strecke vom Arbeitsplatz bis zum Provider synchronisieren.

Begrenzen: Freiheit kann nicht schrankenlos sein

Zu den Wesensmerkmalen des Cloud Computing gehören die Loslösung von den Fesseln des Ortes, die Orientierung an (weltweiten) Verfügbarkeiten statt an Landesgrenzen, das Denken in globalen Netzwerken sowie die flexible Nutzung der Infrastruktur. Nationale Normen verkörpern hingegen eine andere Sichtweise und zwingen den Beteiligten eine Beachtung der Grenzen auf.

Besonders deutlich wird der Unterschied zwischen technischer und rechtlicher Handlungsmöglichkeit beim Datenschutz. Personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen das Gebiet der europäischen Union verlassen und lediglich auf einem definierten Weg an konkrete Datenverarbeiter weitergegeben werden. Aber das auslagernde Unternehmen bleibt auch bei einer zulässigen Auftragsdatenverarbeitung verpflichtet, den konkreten Ort der Speicherung der Daten zu kennen. Es muss gegebenenfalls die Löschung der Daten kontrollieren können. Eine automatisierte globale Datenverteilung mit einem Verlust der Ortsbezogenheit ist hier nicht möglich.

Übersehen wird häufig das mit drakonischen Strafen versehene Exportrecht. Für die Ausfuhr von bestimmten Technologien ist eine vorherige Genehmigung des Bundesamtes für Wirtschaft und Ausfuhr (Bafa) erforderlich; sogar die Exportkontrolle der USA kann beim Einstellen von Daten in eine globale Cloud betroffen sein. Von der Exportkontrolle erfasst wird „Dual-Use-Technologie", die sowohl zivil als auch militärisch eingesetzt werden kann, also zum Beispiel Verschlüsselungstechnik.

Das mit drakonischen Strafen versehene Exportrecht wird häufig übersehen.

Für Datenschutz wie auch Exportkontrolle gilt, dass ein Download nicht einmal vorausgesetzt wird. Es genügt die Möglichkeit eines Zugriffs.

Unabhängig von gesetzlichen Regelungen kann die Möglichkeit eines Datenzugriffs aus dem Ausland aber für das Unternehmen selbst kritisch sein: In vielen Ländern hat der Staat weitgehende Möglichkeiten, auf Daten zuzugreifen beziehungsweise den Datenverkehr zu überwachen.

Auch hier sollte sich der Kunde möglichst durch Regelungen im Vertrag absichern. Beispielsweise durch die Berücksichtigung folgender Punkte:

- die eigenen Daten nach A-Daten (Beschränkung erforderlich) und B-Daten (keine Beschränkung nötig) unterscheiden;
- Ländergrenzen für A-Daten vereinbaren – mit Gültigkeit für Fernzugriff sowohl von Administratoren als auch von eigenen Mitabeitern; keine Zugriffsmöglichkeit „von überall";
- Alternative: Echtdaten lokal halten und anonymisierte Datenverarbeitung in der Wolke betreiben. Bei Daten, die der Exportkontrolle unterliegen, genügt die Verschlüsselung jedoch nicht;
- unbeschränkte Weisungsrechte über die Datennutzung einräumen lassen;
- Löschprozedere definieren, insbesondere das Einfordern von Löschungsbestätigungen.

Kontrollieren: Zertifizierung ersetzt nicht die eigene Prüfung

Besonders wichtig ist die Kontrolle des Providers. Die erforderliche Risikoabschätzung setzt Kenntnisse über den Dienstleister voraus. Zertifizierungen sind hilfreich, können jedoch die eigene Prüfung nicht ersetzen.

Der Vertrag sollte auch hierzu Regelungen enthalten. Sie können beispielsweise so aussehen:

- Auditrechte definieren, unmittelbaren Zugang auch bei Subunternehmern des Providers zusichern lassen;
- Vorlage und Erneuerung von Zertifikaten regeln;
- Reporting-Pflichten des Providers konkretisieren – nicht nur zur Einhaltung der Service-Levels, sondern auch zu geplanten Systemänderungen;
- Weisungsgebundenheit des Providers gegenüber Dritten, zum Beispiel gegenüber Aufsichtsämtern wie der Bankenaufsicht Bafin, sicherstellen.

Letztlich kann der Vertrag nur eine Absicherung sein. Ebenso bedeutsam wie das Aushandeln sind die sorgfältige Auswahl des Providers und das Vertrags-Controlling während der gesamten Laufzeit. *(qua)*

***Thomas Fischer** ist Partner der Sozietät Waldeck Rechtsanwälte und betreibt den Blog SourcingOut.com.