



Alles im Netz und im Griff

Mythen und Modalitäten der »Cloud«

»Cloud Computing« ist in den Unternehmen angekommen. Konzerne und Mittelständler erkennen die Vorteile einer flexiblen, beliebig skalierbaren IT, die von professionellen Anbietern betrieben, geschützt und gewartet wird, ohne die eigenen Ressourcen zu binden.

Diverse Angebote im Markt ▶ Unter »Cloud Computing« versteht man die Bereitstellung gemeinsam nutzbarer, flexibel skalierbarer IT-Leistungen (»Cloud Services«), die als nicht exklusive Angebote in der »Public Cloud« bereitgestellt werden. Dadurch stehen alle global verfügbaren Rechenkapazitäten unterschiedslos allen globalen Nutzern zur Verfügung. Die Speicherung und die Verarbeitung der Daten erfolgt für jeden Nutzer in Mandantentrennung. Kunden haben jedoch keine Kontrolle und keinen Einfluss darauf, wo ihre Daten im weltweit vernetzten IT-System gespeichert und verarbeitet werden.

Das Gegenmodell heißt »Private Cloud«. Hier wird ein dedizierter Bereich des globalen »Cloud Systems« für einen Kunden reserviert. Insofern bestehen deutlich bessere Kontrollmöglichkeiten über den Ort und die Art und Weise der Datenverarbeitung sowie hinsichtlich eventueller Zugriffsmöglichkeiten Dritter. Oft werden beide Modelle auch in einem hybriden Ansatz verbunden: Rechenintensive Verarbeitungsschritte, die hohe Skalierbarkeit erfordern, ohne be-

sondere Anforderungen an Vertraulichkeit und Kontrolle zu stellen, werden in die »Public Cloud« gegeben, während sensiblere Verarbeitungsschritte in einem kontrollierten, dezidierten Bereich passieren. Häufig werden beide Systeme noch durch konventionelle eigene IT-Systeme ergänzt, die Kunden lokal selbst (»on premise«) betreiben.

»Cloud Services« unterscheiden sich auch durch die Service-tiefe, inwieweit also die Abläufe vollständig unter der Kontrolle des »Cloud Service«-Providers erfolgen oder durch Systeme, die Kunden kontrollieren. Basislösungen bieten lediglich eine Infrastruktur aus virtualisierten Servern, Speichern und Netzwerken an. In solchen Infrastrukturen können die Kunden dann ihre Applikationen, Daten und das Betriebssystem unter ihrer Kontrolle betreiben (»Infrastructure as a Service«). Allerdings müssen die Kunden sich dann um die Integration der »Cloud«-Infrastruktur in ihr Netzwerk sowie um das Berechtigungsmanagement der Administratoren und der Endnutzer, um die eigentliche Betriebssteuerung (Monitoring, Back-ups, Ausfallservice, Virenschutz bzw. Firewall) und um ihre Softwarelizenzen kümmern. Stellt der »Cloud Service«-Provider hingegen eine ganze Plattform zur Verfügung, schließt dies auch die Betriebssysteme und die »Middleware« ein. Die Kunden haben mit der Besorgung und Steuerung der eigentlichen Applikationen, mit den Daten, dem Berechtigungskonzept und der Integration ins eigene Netzwerk zu tun (»Platform as a Service«).

Beim voll integrierten »Cloud Service« kommt die Software gewissermaßen aus der Internet-Steckdose. Der Provider stellt die Infrastruktur, die Plattform und die Softwareapplikation zur Verfügung und er stellt das Hosting sowie die Verarbeitung der Daten (»Software as a Service«) dar. In diesem Fall müssen Kunden nur noch die Netzwerkintegration und das Berechtigungsmanagement organisieren.

Merkmale von »Cloud Services« ▶ Die Angebote zeichnen sich durch eine Reihe gleicher Grundmerkmale aus, die sie von den konventionellen IT-Systemen im eigenen Rechenzentrum unterscheiden:

- ▶ Die Elastizität und die Skalierbarkeit der Rechenkapazitäten nach oben und unten, jeweils mit oder ohne Mindestabnahmemengen.
- ▶ Die Möglichkeit zur Selbstprovisionierung. Kunden bestellen in einem eigenen Kontrollzentrum, was sie benötigen.
- ▶ Die Vergütung erfolgt oft verbrauchsabhängig, also je nach Inanspruchnahme.
- ▶ Die verbrauchsabhängige Vergütung setzt voraus, dass die System-Performance und der Verbrauch in Echtzeit nachvollziehbar sind.
- ▶ »Cloud«-Plattformen haben einen hohen Industrialisierungsgrad und einen hohen Standardisierungsgrad, so dass individuelle Programmierungen nur bedingt möglich sind.



Dr. Matthias Orthwein

Von A nach B mit  !

 **Wir sind Experten in Sachen Kurven.**

Unsere Ladungssicherungsmittel halten, was sie versprechen – auch bei Ausfügen in anspruchsvolles Gelände.

Egal ob Seile, Ketten, Hebebänder, Rundschlingen, Zurrmittel oder Hebezeuge – auf www.dolezych.de finden Sie neben Qualität auch immer einen erfahrenen Ansprechpartner.

Heben oder Transportieren – seit über 75 Jahren wird's sicher mit  wie Dolezych.

Dolezych
einfach sicher

-
- ▶ Die Integration von »Cloud Services« in die eigene IT-Infrastruktur kann trotz des standardisierten Industrieansatzes aufwendig sein.
 - ▶ Vorteilhaft ist die hohe Agilität der Systeme hinsichtlich des »Roll-outs« neuer Produkte und Features, die der »Cloud Service«-Provider allen Nutzern flächendeckend zugleich zur Verfügung stellt.
 - ▶ Die Datenspeicherung erfolgt nach Vorgaben des Kunden auf regional oder weltweit verteilten Serverstrukturen. Dabei stehen meist global verteilte Lösungen sowie in Europa lozierte Serverkapazitäten zur Wahl. In Einzelfällen sind auch rein deutsche »Clouds« möglich.
 - ▶ Die Speicherung und die Verarbeitung erfolgen auf geteilten Infrastrukturen. Die Daten werden logisch getrennt ohne die Hardware physisch zu separieren.
 - ▶ Die Verfügbarkeit des Gesamtsystems entscheidet stets auch über die Verfügbarkeit der Anwendungen für die Kunden.

Risiken von »Cloud Services« ▶ Bevor sich Unternehmen entscheiden, ihre Daten oder Applikationen in einer »Cloud« abzulegen, ist das damit verbundene Risiko zu bewerten. Dies geschieht im Rahmen einer Klassifizierung. Dabei wird geklärt, ob Daten und Applikationen überhaupt für den Einsatz in der »Cloud« in Frage kommen. Konkret wird zunächst der Schutzbedarf anhand der in Unternehmen üblichen Sicherheitseinstufungen ermittelt (»geheim« = Schutzklasse 3: meist nicht für die »Cloud«; Schutzklasse 2: nur verschlüsselt in die »Cloud«; Schutzklasse 1: ohne Einschränkungen in die »Cloud«). Außerdem sind die erheblich gestiegenen Anforderun-

gen der neuen europäischen DSGVO zu berücksichtigen. Personenbezogene Daten dürfen nur noch in sichere Drittstaaten oder besonders geschützt in unsichere Drittstaaten (z.B. USA) exportiert werden oder sie sind vor der Übertragung in eine »Cloud« vollständig und irreversibel zu anonymisieren. Im Rahmen der Verfügbarkeitsprüfung ist zu klären, wie wichtig ein unterbrechungsfreier Zugriff auf Daten und Applikationen ist und welcher Schaden Unternehmen gegebenenfalls durch einen eventuellen, wenn auch nur vorübergehenden Ausfall drohen. Des Weiteren ist das Risiko eines möglichen Zugriffs durch Dritte (Behörden, Hacker, Datenadministratoren) sowohl unter dem Gesichtspunkt des Datenschutzes als auch unter dem Gesichtspunkt des Schutzes der Geheimnisse von Unternehmen zu beachten. Schließlich sind die Sicherheitsmaßnahmen des »Cloud Service«-Providers zu bewerten, und zwar insbesondere im Hinblick auf die Verschlüsselung der Daten und anerkannte Zertifikate.

Regeln von »Cloud«- Serviceverträgen ▶ Haben Unternehmen zugunsten der Nutzung von »Cloud Services« entschieden, sind diese Grundregeln im Vertragsverhältnis mit dem Provider zu beachten:

- ▶ Der Vertrag sollte regeln, dass die Mindeststandards der Informationssicherheit in der gesamten Vertragslaufzeit eingehalten werden.
- ▶ Der vereinbarte »Service Level«, also vor allem die zugesicherte Verfügbarkeit des Systems, vereinbarte Wartungsfenster und die ent-

▶ *Fortsetzung auf Seite 29*

► Fortsetzung von Seite 27

sprechenden Messverfahren müssen den Kundenanforderungen entsprechen. Hier ist neben der Frage, wie der Kunde die Einhaltung der »Service Levels« überprüfen kann, die Motivation des Anbieters zu regeln, sich auch verbindlich an die zugesagten »Service Levels« zu halten. Insofern sind auch Haftungsregeln zu formulieren.

► »Cloud Service«-Provider verlangen viel Flexibilität bezüglich ihrer eigenen Leistungen und deren Änderungen. Kunden müssen sich überlegen, ob sie solche einseitigen Leistungsänderungen akzeptieren wollen und wie rasch gegebenenfalls eine Migration ihrer Daten und Applikationen zu einem anderen Provider möglich ist.

► Preisfallen wie Mindestabnahmemengen und automatische Preisanpassungsklauseln sind in »Cloud«-Serviceverträgen oft Probleme.

► Kunden sollten sich die Kontrolle über den Betrieb der gemieteten Infrastruktur vorbehalten, vor allem im Hinblick darauf, welche Subunternehmer im Rahmen des Services eingesetzt werden können.

► Aus Gründen des Datenschutzes empfiehlt sich, sicherzustellen, dass der Speicherort personenbezogener Daten in der EU liegt, was einen Datenexport in Drittländer wie die USA oder (ab 2019) Großbritannien nur unter besonderen Absicherungen möglich macht.

► Die relativ einfache Verfügbarkeit der »Cloud Service«-Angebote im Internet birgt auch das Risiko, dass in Unternehmen eine Schatten-IT entsteht, indem Fachabteilungen ohne Rücksprache mit dem Leiter der IT damit beginnen, Subsysteme zu betreiben, die sich der Kontrolle der Geschäftsleitung weitgehend entziehen.

► »Cloud Service«-Kunden sollten darauf achten, welche Rechte sich Anbieter an den in der »Cloud« gespeicherten Inhalten vorbehalten, etwa zur Erstellung von Statistiken oder zur Verbesserung ihrer Angebote, und diese Rechte einschränken.

► Um »Compliance«-Anforderungen seiner eigenen Kunden zu erfüllen, ist es wichtig, diese beispielsweise durch Auditrechte in den Verträgen über die Nutzung von »Cloud-Services« abzubilden.

► Last, but not least, empfiehlt sich für Unternehmen, zumal für Mittelständler, ihre eigene Rechtsdurchsetzung nicht durch die Vereinbarung ausländischer Gerichtsstände zu erschweren. Vertragspartner für »Cloud Services« sollten ihren Sitz in Deutschland haben oder eine deutsche Niederlassung als Vertragspartner anbieten.

Fazit ► Der professionelle Einsatz moderner, flexibler und leicht skalierbarer »Cloud Services« bietet nicht nur Konzernen, sondern allen Unternehmen viele zusätzliche Optionen und günstige Kostenstrukturen, die sich in der Regel am tatsächlichen Verbrauch orientieren. Eine effektive Klassifizierung der in die »Cloud« transportierten Daten und Applikationen erlaubt es Unternehmen, ihre damit verbundenen grundsätzlichen Risiken zuverlässig zu erkennen und zu bewerten. Diese lassen sich bei Beachtung einiger wesentlicher vertraglicher Grundregeln zudem zuverlässig steuern und beherrschen. ■

*RA Dr. Matthias Orthwein, Partner
SKW Schwarz Rechtsanwälte Steuerberater
Wirtschaftsprüfer Partnerschaft mbB, München*