manage IT, 01.08.2013, verbr. Auflage: k.A.

Cloud Computing

»Der sicherste Cloud-Hafen«

Das Thema Cloud Computing ist mehr als präsent, und dennoch bleiben viele Fragen zur richtigen Anwendung offen – gerade in Bezug auf die Datensicherheit.

Bild: Shutterstock.com/olhyy

Der deutsche Cloud-Markt wächst dynamisch. Doch während Privatanwender im täglichen Gebrauch mittlerweile völlig selbstverständlich verschiedenste Anbieter als virtuellen Datenspeicher verwenden, haben viele Unternehmen – insbesondere der deutsche Mittelstand – bei der Nutzung der »Wolke« häufig noch ihre Bedenken.

Ist diese Art des Datentransfers und -speicherns auch sicher? Welche rechtlichen Grundlagen gilt es zu beachten? Und was passiert, wenn bei einem ausländischen Anbieter der Serverpark zerstört wird?

Datensicherheit und Datenschutz. Zwei Aspekte, die im allgemeinen Bewusstsein privater Nutzer häufig zu kurz kommen, sind Datensicherheit und Datenschutz. Gerade diese beiden Bereiche jedoch spielen für Unternehmen, die auf strenge Vertraulichkeit angewiesen sind, eine entscheidende Rolle. Obgleich die Vorteile der Cloud, wie Globalität, Mobilität, Flexibilität und eventuelle Kostensenkung, nicht von der Hand zu weisen sind, muss sich ein Unternehmen vorab auch mit dem möglichen Ernstfall »Datenverlust« und den daraus resultierenden Konsequenzen auseinandersetzen.

Zunächst einmal gilt es, auf Unternehmensseite den Unterschied zwischen dem Schutz und der Sicherheit von Daten sowie zwischen Cloud- und Hostingangeboten zu erkennen. Datenschutz impliziert die Verschwiegenheit aller Beteiligten im Hinblick auf personenbezogene Daten von Mitarbeitern, Kunden oder Lieferanten. Seine Gewährleistung erfordert Datensicherheit im technologischen Sinne, sprich den Schutz gegenüber Viren und Trojanern sowie die Absicherung der Hardware und des Rechenzentrums selbst. Das bedeutet, es muss eine entsprechende Sicherheitskontrolle gewährleistet sein, die alle wichtigen Parameter berücksichtigt und vor allem die Daten jedes einzelnen Nutzers klar voneinander trennt.

Der Unterschied zwischen Cloud Computing und Hosting ist hingegen nicht sehr groß, denn in beiden Diensten werden Kapazitäten wie Rechenleistung, Speicherplatz, Datenbanken oder Software durch einen Anbieter an den Nutzer »vermietet«. So kann der Kunde seine eigene IT-Infrastruktur virtuell erweitern, ohne dabei selbst entsprechenden Raum oder Technologie bereitstellen zu müssen. Allerdings können die Services im Hosting-Bereich sehr viel individueller und vertraglich abgesicherter auf den einzelnen Kunden zugeschnitten werden. Die Cloud ist in der Regel weitaus standardisierter, dafür aber auch kostengünstiger und flexibler nutzbar.

Die Verantwortung bleibt beim Dateninhaber. Ganz gleich, ob Cloud Computing oder Hosting, datenschutztechnisch haben Anwender sich hierzu-

lande strikt an das Bundesdatenschutzgesetz (BDSG) zu halten. Davon ausgenommen sind lediglich solche Daten, die keinerlei Personenbezug aufweisen, wie zum Beispiel Produktlisten. Sobald in den zu speichernden Unterlagen jedoch Kundendaten, Namen oder Gehaltsabrechnungen auftauchen, fallen die Daten unter das BDSG und im Falle von externer Datenspeicherung über einen Provider unter den § 11. Danach ist Cloud Computing der klassischen Auftragsdatenverarbeitung zuzuordnen, was bedeutet, dass Verantwortung und Verfügungsgewalt beim Nutzer verbleiben. Dieser ist verpflichtet, den Anbieter vorab genau zu überprüfen und sich vor allem während der Datenverarbeitung regelmäßig selbst von der Sicherheit zu überzeugen. Um diese Einhaltung zu überwachen, sollten die Ergebnisse regelmäßig schriftlich durch den Anbieter dokumentiert werden, denn ein fahrlässiger Verstoß gegen das BDSG kann eine Geldbuße von bis zu 50.000 Euro nach sich ziehen.

Wichtig ist darüber hinaus der Standort des Anbieters, an den die Daten ausgelagert werden. Möchte ein deutsches Unternehmen deutsche Daten beispielsweise in einer US-Cloud speichern, dann muss es sicherstellen, dass auch alle deutschen Gesetze eingehalten werden. Einer der Gründe für diese strenge Reglementierung ist der US PATRIOT ACT: Selbst wenn das Rechenzentrum des amerikanischen Anbieters in der EU sitzt, ist dieser dennoch verpflichtet, die Daten auf Anfrage an die US-Regierung weiterzugeben. Das gilt für jedes Datacenter weltweit. Laut BDSG dürfte ein deutsches Unternehmen folglich gar keinen US-Dienstleister nutzen. Es sei denn, es werden ausschließlich verschlüsselte Daten gespeichert, was ohnehin zu empfehlen ist. Eine solche Sicherheit bietet eine End2End-Verschlüsselung der Daten vor der Übertragung, wobei lediglich das Kryptofile in die Cloud geladen wird.

BDSG ist komplex aber sicher. Obwohl es beispielsweise Abkommen mit besonderen Auflagen wie das »Safe Harbor« zwischen der EU und den USA gibt, ist der Unterschied in den rechtlichen Regelungen immens. Um die Kontrollen zu gewährleisten, müssten diese auf amerikanischer Seite auch durchgeführt werden. Dass dies häufig nicht der Fall ist, zeigen die in der Vergangenheit wiederholt aufgetretenen Datenpannen bei bekannten Großkonzernen.

> **»Möchte ein deutsches Unternehmen deutsche Daten** beispielsweise in einer US-Cloud speichern, dann muss es sicherstellen, dass auch alle deutschen Gesetze eingehalten werden.«

Somit wird die Bundesrepublik voraussichtlich auch in naher Zukunft nicht dazu übergehen, das Datenschutzrecht in Deutschland an ausländische Regelungen wie das EU-Recht anzugleichen.

Kritiker geben zudem seit langem zu Bedenken, dass Datenspeicherung im Ausland – speziell in den USA – viel stärker dem Risiko der Betriebsspionage ausgesetzt ist. Trotz seiner häufig kritisierten Komplexität macht das BDSG Deutschland hier eindeutig zum »sichersten Hafen«.

Sorgfalt walten lassen. Welche rechtliche Handhabe der Nutzer letztlich im Ernstfall bei Datenverlust hat, ist schwer abzusehen. Das ist immer davon abhängig, was mit dem Anbieter vertraglich vereinbart wurde. Bei Problemen muss man sich jedoch in jedem Fall auf einen Rechtsstreit nach Landesrecht des Anbieters mit entsprechendem Gerichtsstand einstellen. Das kann sich bei ausländischen Anbietern zum einen über eine längere Zeit hinziehen und ist zum anderen wenig Erfolg versprechend.

Um solche Probleme jedoch gar nicht erst entstehen zu lassen, sollte man bei der Auswahl des Anbieters Sorgfalt walten lassen. Mit entsprechender professioneller Beratung eines seriösen Dienstleisters kann die Nutzung von Cloud Computing oder Hosting einem Unternehmen klare Vorteile verschaffen und wesentlich zu einer Verbesserung der Unternehmensstruktur beitragen.

Auch wenn der Markt derzeit noch recht unübersichtlich ist, und viele Cloud-Services ihrem Angebot leider nicht gerecht werden, kann man die Unsicherheit durch gezielte Aufklärung verringern und das immense Potenzial dieses Dienstes deutlich machen. Ohne Frage sollten Datensicherheit und rechtliche Handhabe in der Cloud noch weiter konkretisiert und abgesichert werden, aber eine staatliche Regulierung im Sinne von Verpflichtungen halte ich nicht für sinnvoll. Dafür ist dieses Thema viel zu komplex und individuell. Eine derartige Regulierung mit festen Vorgaben könnte zahlreiche interessante Produkte zunichte machen und gegebenenfalls neue Technologien verhindern. Stattdessen könnte die Regierung Empfehlungen für die Implementierung von Cloud-Diensten definieren, die unter anderem die Sicherheit behandeln. Zusammen mit einer darauf basierenden Zertifizierung, der sich ein Cloud-Provider unterziehen kann, könnten die Zweifel vieler Mittelständler sicher reduziert werden.

Christoph Maier

Christoph Maier,
Vorstandsvorsitzender der
Thomas-Krenn.AG
aus Freyung