IT-Ressourcen über das Internet

Das Speichern von Daten über das Internet in einer Cloud sowie das Nutzen von Software aus der Cloud gewinnt immer mehr an Bedeutung. IT-Sicherheit ist dabei ein entscheidender Faktor.

Bei *Cloud-Computing* werden Daten nicht auf dem eigenen Computer abgelegt, sondern über das Internet an einem Speicherort, der sich auf dem Server eines Providers befindet, einer „Cloud“ (Wolke). Neben Speicherkapazitäten können auch Software und Rechenleistung aus der Cloud bezogen werden. Betriebe, die Cloud-Computing nutzen, müssen weniger in Hardware und Software-Lizenzen investieren. Mitarbeiter eines Unternehmens können ihr bevorzugtes Gerät *(„Bring Your Own Device“ – BYOD)* benutzen. Sie können auch unterwegs mit mobilen Geräten wie Smartphones und Tablets auf Firmendaten zugreifen, die in der Cloud gespeichert sind. Ein Vorteil der Cloud ist, dass Dienste nur bezahlt werden müssen, wenn sie tatsächlich genutzt werden.

Hinter Cloud-Computing stecken Hardware, Software, Netzwerke, Sicherheit und Administration. Man kann sich die Cloud wie ein Stromnetz vorstellen. Damit Strom aus der Steckdose kommt, benötigt man Infrastruktur wie Wasserkraftwerke, Transformatoren, Stromleitungen, Verteilerstationen, Sicherungen und internationale Abkommen. Es gibt öffentliche, private, Hybrid und Community-Clouds.

- *Öffentliche Clouds* können in der Regel nur über das Internet genutzt werden und werden etwa von *Amazon, Microsoft* oder *Google* zur Verfügung gestellt, um ihre Dienste anzubieten.
- *Private Clouds* stehen Firmen oder Organisationen zur Verfügung, um den internen Bedarf an Diensten zur Verfügung zu stellen. Sie können direkt gemanagt werden oder auch von Drittanbietern bereitgestellt werden.
- *Community-Clouds* stellen Dienste für eine gleichgesinnte Gemeinschaft zur Verfügung. Gleicher Bedarf an Sicherheit, Anwendungen, rechtliche Rahmenbedingungen sind hier Voraussetzung.
- *Hybrid Clouds* sind eine Mischung verschiedener Cloud-Formen. Große Firmen stellen etwa die interne IT-Infrastruktur genauso zur Verfügung wie Kundenzugänge zu den Angeboten. Das ist eine Möglichkeit, bei Bedarfsspitzen auf jeweils andere oder geeignetere Dienste zuzugreifen.

„Cloud-Computing“: Daten werden nicht mehr auf dem eigenen Computer abgelegt, sondern über das Internet auf dem Server eines Providers.

Vier Dienste gibt es derzeit bei Cloud-Computing:

- *Infrastructure as a Service (IaaS)* ist dem Endnutzer am nächsten. Hier werden die Dienste bereitgestellt – Rechnerleistung und Speicher.
- *Software as a Service (SaaS)* erlaubt Anwendern, Software-Anwendungen zu nutzen, die in der Cloud auf Servern der Anbieter laufen, ohne diese auf ihrem Computer zu installieren. Die Anwender müssen sich weder um Updates noch um Sicherheit sorgen. Wenn sie ein Programm benötigen, loggen sie sich ein und arbeiten damit, solange es nötig ist.
- *Platform as a Service (PaaS):* Hier laufen grundlegende Dinge wie Betriebssysteme oder Datenbanken. Hier wird auch bestimmt, wie viele Ressourcen die Anwendungen benötigen. Das ist für Entwickler interessant, die gemeinsam Programme über das Internet entwickeln und anbieten können.
- *Network as a Service (NaaS):* Hier stellen Service Provider Netzwerkkapazitäten (Bandbreiten) zur Verfügung, wenn diese benötigt werden. Es können auch *VPNs (Virtual Private Networks)* und *Inter-Cloud-Services* für Sicherheitszwecke genutzt werden. Dabei werden Daten auf mehrere Standorte kopiert, um schnell und sicher verfügbar zu sein.

Datensicherheit. Experten empfehlen, die Daten in die Cloud über eine verschlüsselte Verbindung zu übertragen. Bei besonders sensiblen Informationen sollte man überlegen, sie in der Cloud zu speichern. Passwörter müssen sicher sein und sollten regelmäßig geändert werden. Seriöse Anbieter von Cloud-Computing sichern die Daten meist mehrfach ab. Cloud-Computing funktioniert nur, wenn das Internet funktioniert. Deshalb sollte man Daten auch durch regelmäßige Backups sichern. Betriebe sollten sich über den Anbieter von Cloud-Computing und dessen Dienstleistungen informieren. Gibt es innerhalb eines Unternehmens keinen IT-Sicherheitsverantwortlichen, sollte man externe Beratungs- und Informationsangebote nutzen. Für die öffentliche Verwaltung sind vor allem Datenschutzfragen elementar. Während im Rahmen einer *Private Cloud* die Anforderungen des Datenschutzgesetzes grundsätzlich erfüllbar erscheinen, stellt sich die Problematik insbesondere bei einer Nutzung von *Public Cloud-Services* durch die öffentliche Verwaltung. Zentral ist die Frage, wie die Integrität und Vertraulichkeit der Daten gewährleistet werden kann.

Für Sicherheitsbehörden werden Schnittstellen definiert, um die Kriminalitätsbekämpfung zu erleichtern. Abkommen, Policys, aber auch Gesetze regeln diesen Zugang. Das Problem ist nach wie vor die Internationalität: Die Server der Provider, die Cloud-Computing anbieten, können überall auf der Welt stehen. Universitäten wie das University College Dublin investieren in Forschungsprojekte, um Kriminalitätsbekämpfung zu unterstützen und zu erleichtern. Es wird bereits an der Weiterentwicklung von Cloud-Computing gearbeitet.

Bernhard Otupal

FOTO: I-STOCK/DELL