



Quellen zum Thema

- ▶ Wagner/Groß, BB-ONLINE, BBL2011-36-I.
- ▶ Nägele/Jacobs, Zeitschrift für Urheber- und Medienrecht 2010, S. 281-291.
- ▶ Splittgerber/Rockstroh, Betriebs-Berater 2011, S. 2179-2185.

Cloud Computing

von Dr. Axel-Michael Wagner und Peter Weger^{*)}

Cloud Computing bezeichnet das Zurverfügungstellen von IT-Ressourcen über das Internet. Es erlaubt den Zugriff auf Daten und Services, die auf extern gelagerter und über Datenleitungen angebundener Hardware gespeichert bzw. angeboten werden. Wirtschaftlich gesehen ist die Inanspruchnahme z.B. von „Software as a Service (SaaS)-Lösungen“, die dem Cloud Computing zugerechnet werden, nichts anderes als „Global Sourcing“ im Bereich der Informationstechnologie. So wie beispielsweise die Bänder von Zulieferern für mehrere Abnehmer gleichzeitig produzieren können, bieten Anbieter von Cloud-Dienstleistungen beliebige IT-Services global verteilt für beliebig viele Kunden unabhängig voneinander an. Ihr Angebot basiert auf derselben Hardware und nutzt dieselbe öffentliche Dateninfrastruktur (Internet) wie die Unternehmen selbst. Die daraus resultierenden Standortvorteile und Synergieeffekte schlagen sich regelmäßig direkt in niedrigeren und verbrauchsabhängigen IT-Kosten für den jeweiligen Auftraggeber nieder. Wirtschaftlich betrachtet handelt es sich also um eine klassische „Win-Win-Situation“. Dieser stehen allerdings auch rechtliche Risiken, wie eine mögliche Verletzung des Datenschutzes, entgegenstehende Urheberrechte, „Datenexportverbote“ und Einsichtsmöglichkeiten Dritter, gegenüber. Die Verfügbarkeit der extern gespeicherten und verarbeiteten Daten muss zudem jederzeit gewährleistet sein. Im Vorfeld einer Einführung von Cloud-Lösungen ist daher eine Reihe von Risikopotenzialen sorgfältig zu evaluieren. Insofern wird Cloud Computing auch zum Gegenstand der Compliance-Verantwortung eines Unternehmens, die in unterschiedlicher Weise und Intensität von Vorstand und Aufsichtsrat wahrzunehmen ist.

Entscheidet sich der Vorstand eines Unternehmens für die vollständige (oder teilweise) Auslagerung seiner IT in die Cloud, so stellt sich für den Aufsichtsrat die Frage, ob und inwieweit er in diese Entscheidung (sowie die Berücksichtigung der potenziellen Folgen) einzu-beziehen ist. Sind die Unternehmensdaten bedeutend und sensibel, ist die Einbeziehung des Aufsichtsrats ein Muss. Dagegen ist beispielsweise die Umstellung auf papierlose Rechnungsstellung unter Einbezug externer Dienstleister noch eher als operative Maßnahme des Vorstands und daher unkritisch für den Aufsichtsrat anzusehen. Die komplette Verlagerung „missionskritischer“ IT-Funktionen und Daten aber würde gewichtige Fragen nach der Datensicherheit und -verfügbarkeit mit Bedeutung für das Unternehmen als Ganzes aufwerfen. Daher muss der Aufsichtsrat hier grundsätzlich einbezogen werden. Denn wie bei jeder Überwachungstätigkeit des Aufsichtsrats

drohen in einem solchen Fall, der die grundlegenden Strukturen des Unternehmens betrifft und potenziell gefährdet, immer auch Haftungsrisiken. Je weniger sich der Aufsichtsrat der Angelegenheit im Vorhinein angenommen hat, desto früher können sich diese ihm gegenüber manifestieren.

Unmittelbar die Aufgabenstellung des Aufsichtsrats betrifft der hochsensible Austausch von vertraulichen Dokumenten über Unternehmensgrenzen hinweg, der im Rahmen der Gremien- bzw. Organ-kommunikation entsteht. Hier ist es insbesondere die oberste Pflicht des Aufsichtsrats, zu jeder Zeit die Wahrung der Verschwiegenheit zum Schutz der Gesellschaft vor Schaden sicherzustellen. Daher erweitern Lösungsanbieter mit einer „Secure Cloud“-Lösung das Spektrum der Möglichkeiten, um Geschriebenes auf effizientem Wege sicher zu übertragen. Es gilt für den Aufsichtsrat abzuwägen, inwieweit der sicheren Kommunikation und dem regelkonformen Umgang mit vertraulichen, schriftlichen Angaben über Geschäftsgeheimnisse im Rahmen einer Cloud-Lösung stattgegeben werden darf. Viele Aufsichtsräte hegen aber heute noch ein latentes Misstrauen im Hinblick auf die Gewährleistung des unbedingten Schutzes der Inhalte vor unbefugtem Zugriff. Stehen doch bei Verletzung der Verschwiegenheitspflicht die Abberufung einzelner Aufsichtsratsmitglieder oder bei Vorsatz sogar eine Strafverfolgung nach § 404 AktG im Raum. Insofern muss der Aufsichtsrat im Rahmen der pflichtgemäßen Evaluierung geeigneter Lösungen auch hier auf technische Voraussetzungen, wie den Standort der Server und Speichermedien, die durchgängige Datenverschlüsselung und die Zugriffsfunktionalitäten der Lösung, unbedingtes Augenmerk legen.

Wirtschaftlich gesehen sind Services aus der Cloud „en vogue“, weil sie große Sparpotenziale bergen. Ob sich diese Ersparnis für das jeweilige Unternehmen rechnet, hängt entscheidend davon ab, ob das auslagernde Unternehmen vorher ausreichende rechtliche und fachliche Prüfungen in Bezug auf die avisierte Cloud-Lösung betrieben hat. Wenn es um die Einführung von Cloud-Lösungen in kritischen Bereichen geht, sollte der Aufsichtsrat dem Vorstand raten, eine dem unternehmensspezifischen Risiko angemessene Evaluierung und Ausgestaltung vorzunehmen und diese dann auch überwachen; zudem sollte das gesamte Planungs-, Prüfungs- und Einführungsverfahren schriftlich und nachvollziehbar niedergelegt und periodisch auf veränderte Soll-Anforderungen überprüft werden.

^{*)} Dr. Axel-Michael Wagner,
Partner und Rechtsanwalt,
Peters Schönberger & Partner
GbR, München;
Peter Weger, CEO, Brainloop
AG, München.