SECIANUS-GESCHÄFTSFÜHRER JÖRG KARNER, SACHVERSTÄNDIGER FÜR INFORMATIONSSICHERHEIT UND DATENSCHUTZ, IM GESPRÄCH MIT ROBERT TORUNSKY

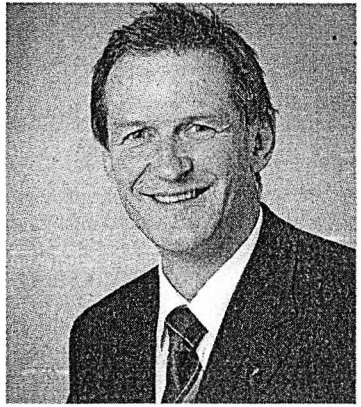
Datenschutz bei „Cloud Computing" entscheidend

Herr Karner, die Cloud Computing-Anbieter sehen die weltweite Erreichbarkeit der Unternehmensdaten als großen Vorteil. Welche Bedenken bestehen bezüglich des Datenschutzes in der „Wolke"?

Jörg Karner: „Die internationale Erreichbarkeit kann zu Problemen führen, wenn dabei personenbezogene Daten verarbeitet oder auf solche zugegriffen werden soll. Dies kann für in Deutschland ansässige Firmen unter Umständen zum Konflikt mit dem Bundesdatenschutzgesetz (BDSG) führen. Im BSDG gibt es keinen Konzernprivileg – somit müssen ihm auch Konzernteile aus dem Ausland Folge leisten. Dies wird dann problematisch, wenn sich diese Konzernteile nicht in der Europäischen Union befinden. Ein weltweiter Zugriff bedeutet auch, dass Zugriffsmöglichkeiten von Dritten von überall aus möglich sind. Hier ist unbedingt mit dem Cloud Computing-Anbieter zu klären, wie eine Kontrolle und eine Realisierung von Beschränkungen umgesetzt werden können. Da Daten beim Anbieter gespeichert werden, besteht zudem die Frage nach ausreichendem Schutz der Daten vor unberechtigten Zugriff.

Sehen Sie Risiken bei der Sicherheit?

Im Vorfeld einer Daten-Auslagerung seitens des Unternehmens ist unbedingt festzuhalten, welche Schutz-Maßnahmen der Anbieter getroffen hat bzw. trifft. Ein Problem „herkömmlicher" IT-Umgebungen ist, dass nur schwer nachvollziehbar und kontrollierbar ist, wie Daten das Unternehmen verlassen. Mit einer Cloud-Lösung wird dies noch schwieriger, da die Daten ja bereits das Unternehmen verlassen haben. Es muss nun zusätzlich sichergestellt werden, wie Daten nicht unbefugt die Cloud verlassen können. Wer ist für diese Maßnahmen zuständig? Gibt es eine solche Lösung überhaupt in der Cloud und was kostet diese? Bei einer lokalen Installation könnte man notfalls den „Stecker ziehen", wenn man merkt, dass Daten unberechtigt abgezogen werden. Eine solche „Not-Aus"-Funktion ist in der Cloud nur schwer realisierbar. Da ein Cloud-Anbieter mehrere Kunden hat, ist eine sichere und funktionierende Mandantentrennung im Betrieb und auch bei Updates zwingende Voraussetzung.



„Der Kunde bleibt auch bei einer Daten-Auslagerung in die Cloud für die Daten verantwortlich."
JÖRG KARNER

Auf was müssen Nutzer von Cloud Computing-Diensten im Störungsfall achten?

Entscheidend ist, ob und in welchem Umfang der Kunde im Störungsfall informiert wird. Dies ist für den Fall wichtig, wenn besonders personenbezogene Daten verloren gehen oder in unbefugte Hände gelangen sollten. Auch durch die Auslagerung der Daten in die Cloud kann sich der Kunde nicht seiner Verantwortung entziehen – er bleibt aufgrund des §11 (1) Bundesdatenschutzgesetz verantwortlich! *Interview: Robert Torunsky*