Netzwerk Elektronischer Geschäftsverkehr

Fachhochschule Gelsenkirchen

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheitstipp: Cloud-Dienste sicher nutzen

Im Jahr 2011 könnte es das Top-Thema aller IT-Anwender werden. Laut einer Statistik des BITKOM [1] vom Oktober 2010 zufolge, werde hier der Umsatz in Deutschland jährlich um mehr als 45 % ansteigen. Die Rede ist vom so genannten *Cloud Computing.* Hierbei handelt es sich um die Nutzung von externen Hard- und Softwareressourcen in Online-Netzwerken, der *virtuelle Wolke*. Sind die eigenen Daten des Nutzers innerhalb der virtuellen Wolke ausgelagert, so können berechtigte Teilnehmer von jedem beliebigen Standpunkt aus via Internet auf diese zugreifen und sie in Echtzeit weiterverarbeiten.

Diese Technologie bietet zwar viele Vorteile, sollte jedoch nicht bedenkenlos angewendet werden. Denn das Risikospektrum des Cloud Computing reicht vom Verlust privater Urlaubsfotos bis hin zu immensen Finanz- und Imageschäden für das eigene Unternehmen. Wie Sie die Vorteile des Cloud Computing nutzen können und dabei trotzdem stets auf der sicheren Seite stehen, erfahren Sie in diesem IT-Sicherheitstipp.

Geben Sie keine sensiblen Daten von sich preis

Die Nutzer von Cloud-Diensten haben meist wenig Einfluss darauf, wie ihre hoch geladene Daten durch den Anbieter weiterverarbeitet werden. Bei großen Anbietern ist es üblich, dass die Dateien über den ganzen Globus verstreut auf verschiedenen Servern in verschiedenen Ländern lagern und entsprechend bei Bedarf abgerufen werden. Im Nachhinein ist es für die Anwender nicht nachvollziehbar, wo und wie diese dort gespeichert werden. Genau hier liegt ein nicht zu unterschätzendes Sicherheitsrisiko: Da keine internationalen Datensicherungsbestimmungen existieren, gelten – je nach Serverstandort – unterschiedliche Richtlinien.

Auch wenn Sie beispielsweise einen europäischen Cloud-Dienst verwenden, gelten nicht automatisch auch europäische Sicherheitsbestimmungen für alle Rechenzentren des Anbieters, wenn diese außerhalb des europäischen Raumes liegen. Niedrige Sicherheitsbestimmungen in manchen Ländern begünstigen Hackerangriffe auf Server und somit auch auf Ihre Daten. Unterliegen bestimmte Dateiinhalte den Zensurbestimmungen einer jeweiligen Regierung, kann es auch zu einem Zugriff auf Ihre Daten seitens staatlicher Stellen kommen.

Kurzum: Speichern Sie **keine sensiblen Daten** in der Wolke ab, die beispielsweise Informationen über **Ihre Bankgeschäfte** oder **Ihren Gesundheitszustand** preisgeben.

Prüfen Sie die Sicherheitsbedingungen und -vorkehrungen der Anbieter

Sofern Sie einen US-amerikanischen Cloud-Dienst favorisieren, sollten Sie zunächst sicherstellen, dass dieser Anbieter dem ***Safe-Harbor*-Abkommen zugestimmt** hat. Dadurch akzeptiert der Anbieter freiwillig geltende Sicherheitsbestimmungen der Europäischen Union, sodass Ihre internationale Datenhaltung ausreichend abgesichert ist.

Auf den Servern der Cloud-Dienstleister sind meist Millionen verschiedener Daten gespeichert. Die Datenmassen machen die Rechenzentren der Betreiber zur beliebten Zielscheibe von Hackerangriffen und Schadprogrammen wie Viren, Würmern und Trojanern. Jedes Rechenzentrum verfügt heutzutage über Sicherheitsvorkehrungen, die Ihrer privaten oder geschäftlichen Firewall wahrscheinlich überlegen sind. Ein Restrisiko bleibt jedoch immer, denn kein Netzwerk ist zu 100 Prozent sicher. Minimieren Sie das Risiko und erkundigen Sie sich im Vorfeld über die Sicherheitsbestimmungen der einzelnen Anbieter. **Generell gilt: Die Datenübertragung Ihrer Daten in die Cloud sollte nur verschlüsselt, etwa mittels der Technologie SSL, erfolgen.**

Für mittelständische bis große Unternehmen bietet es sich zudem an, die Sicherheit eines Cloud-Services durch einen externen Dienstleister überprüfen zu lassen, um auf Nummer Sicher zu gehen. **Erkundigen Sie sich genauestens über Referenzen und jüngste Presseberichte ausgewählter Anbieter.** Laut einer Studie des *Fraunhofer Instituts für Sichere Informationstechnologie* vom Mai 2009 [2] habe nahezu jeder große Cloud-Dienst in der jüngsten Vergangenheit Probleme

in den Bereichen Verfügbarkeit und Sicherheit gehabt.

Hinterfragen Sie kostenlose Angebote kritisch

Kostenlose Cloud-Services sollten kritisch hinterfragt werden. Was sind die Absichten des Anbieters? Kein Dienstleister bietet seine Leistungen gratis an. Die für Sie scheinbar kostenlose Nutzung der Wolke kann einen bitteren Beigeschmack haben. In manchen Fällen nutzen die Anbieter die hochgeladenen Daten für eine inhaltliche Auswertung, um Sie anschließend mit **personenspezifischer Werbung** zu überfluten. Achten Sie stets auf die **allgemeinen Geschäftsbedingungen**, damit Sie **kein Opfer von Datenmissbrauch werden**. Meist besteht ein Zusammenhang zwischen dem Preis eines Dienstleisters und seinen Sicherheitsvorkehrungen, deshalb gilt die Faustregel: Höhere Kosten bedeuten meist höhere Datensicherheit.

Halten Sie stets aktuelle Sicherungskopien lokal gespeichert vor

Gesetzt den Fall, Sie hätten alle Systemabläufe auf die Benutzung des Cloud-Dienstes A zugeschnitten. Höhere Sicherheitsvorkehrungen, mehr Transparenz und ein besserer Preis machen Anbieter B allerdings zu einem attraktiveren Dienstleister. Bei dem Wechsel wird eine aufwendige Umstrukturierung ihrer Organisation erforderlich.
Ersparen Sie sich den oben beschriebenen Aufwand und **machen Sie sich nicht von Ihrem Cloud-Dienst abhängig.** Achten Sie darauf, auch im Falle von Serverausfällen Ihres Cloud-Dienstes mithilfe von lokal-gespeicherten Sicherungskopien weiterarbeiten zu können.

Wechseln Sie regelmäßig Ihre Passwörter

Um die Sicherheit Ihrer Daten gewährleisten zu können, sollten Sie regelmäßig die Passwörter und Zugriffscodes für Ihre Cloud-Anwendung wechseln. Vergeben Sie nur **starke Passwörter von mindestens zehn Zeichen** (Näheres finden Sie hierzu in unserem bereits erschienenen IT-Sicherheitstipp „*Wie erstelle ich ein sicheres Passwort?“ [3]*). Die Zugriffsrechte Ihrer Cloud-Teilnehmer sollten entsprechend Ihrer nutzungsbedingten Rollenzuweisung unterschiedlich stark gewichtet sein, damit einem Datenmissbrauch oder einem Identitätenschwindel vorgebeugt werden kann. Unternehmen sollten besonders die Teilnehmer der Cloud unter die Lupe nehmen. Sind weitere Unternehmen in die Cloud involviert, sollten diese zunächst einer Sicherheitsprüfung unterzogen werden und nur Zugriff auf die Daten erhalten, die auch wirklich notwendig sind.

Sebastian Spooren vom *Institut für Internet-Sicherheit* - if(is) [4] rät: „**Achten Sie bei der Auswahl eines geeigneten und vertrauenswürdigen Cloud-Dienstes möglichst auf transparente Service-Vereinbarungen. Es gibt zahlreiche seriöse Testberichte, die Sie bei der Entscheidung**

zurate ziehen können.“

Autoren:

Malte G. Schmidt, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

B. Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Weiterführende Informationen:

http://www.ec-net.de

https://www.it-sicherheit.de

http://www.bsi.bund.de

Quellen:

[1] http://www.bitkom.org

[2] http://www.fraunhofer.de

[3] http://ratgeber.it-sicherheit.de

[4] http://www.internet-sicherheit.de

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU

NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 29 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: http://www.kmu-sicherheit.de