Wird man in der Cloud beklaut?

Häufig lagern Firmen ihre Daten nicht mehr auf der eigenen Festplatte, sondern irgendwo in der großen Welt des Internets - der virtuellen Cloud. Wie es dort mit Datensicherheit und Datenschutz aussieht, ist oft unklar.

Auch die virtuelle Datenwolke - die Cloud - kann manchmal aufreißen

Cloud-Computing macht vieles einfacher: Unternehmensdaten liegen nicht mehr in der Firmenzentrale auf irgendeinem Rechner herum, um den man sich selbst kümmern muss, sondern draußen - in einer virtuellen Wolke (Englisch: "Cloud") irgendwo in den Tiefen des Internets.

Die Firma selbst muss sich dann nur noch darum kümmern, dass die jeweiligen Arbeitsplatzrechner gut funktionieren, die Anti-Viren Software auf dem aktuellen Stand ist, und die Rechner einen schnellen Zugang zum Internet haben - so zumindest die Idealvorstellung.

Viele Menschen nutzen die Cloud auch im Kleinen: Ein Webmail-Account zum Beispiel existiert auch in der virtuellen Wolke: Die E-Mails liegen nicht mehr auf der eigenen Festplatte herum, sondern bleiben bei dem E-Mail-Anbieter. Über das Internet greift man dann darauf zu. Praktisch ist es, weil man das von überall tun kann - unterwegs vom Smartphone, dem Tablet oder aus irgendeinem Internet-Café.

Wo auf der Welt ist meine Wolke?

Im privaten Rahmen ist das oft noch unproblematisch, aber geben Firmen ihre Daten an einen

Cloud-Anbieter weg, stellen sich plötzlich viele Fragen. Zum Beispiel: "Woher weiß ich eigentlich, dass mein Anbieter in der Cloud auch die für meine Firma geltenden Datenschutzgesetze respektiert?" Oder: "Wie kann ich garantieren, dass der Anbieter meine Daten auch effektiv und mit neuester Technik vor unbefugtem Zugriff oder Verlust schützt?"

Viele Nutzer wissen nicht, wo auf der Welt die Server mit ihren Daten stehen

"Wenn es auf Ihrem Territorium ist, wo Ihre Gesetze greifen, dann ist es wahrscheinlich okay. Aber welche Sicherheiten haben Sie, wo Ihre Daten gespeichert werden?" fragt sich zum Beispiel Tim Pierson. Der IT-Sicherheitsfachmann überprüft beruflich Netzwerke großer Unternehmen, indem er versucht, sich von außen einzuhacken. Und er schult die Sicherheitsleute dieser Firmen.

Seiner Meinung nach, müssten Kunden, die Daten in der Cloud speichern, auch das Recht haben, regelmäßige Kontrollen beim Anbieter des Speicherplatzes durchzuführen. Das geht bei vielen Anbietern auch heute schon, nur muss der Kunde das meist selbst finanzieren. "Eigentlich sollte aber der Anbieter der Cloud dafür zahlen", sagt Pierson. Beim ersten Mal sollte ein Prüfer sich die Server anschauen, meint er. Danach könnte die Prüfung aber auch elektronisch ablaufen: "Ich stelle mir ein elektronisches Skript vor - ein Programm, das genau diese Aufgabe übernimmt. Es überprüft die Einhaltung der Verpflichtungen in einer juristisch verwertbaren Form. Jedes Mal, wenn ich es ablaufen lasse, erhalte ich eine Bestätigung, die mir zeigt, dass meine Daten genau hier oder dort liegen."

Wem kann ich vertrauen?

Unternehmen sollten allerdings auch darauf achten, wem sie ihre Daten überhaupt anvertrauen, warnt der IT-Sicherheitsfachmann. "Irgendwo muss ja das Vertrauen beginnen. Als wir klein waren, haben wir auch gelernt jemandem zu vertrauen - auf Grundlage dessen, wem wir selbst vertraut

haben. Wenn Mutti gesagt hat: 'Du kannst Dich auf den Schoß von Tante Sally setzen, aber setz Dich bloß nicht auf den Schoß von Onkel Billy!' Genau so müssen wir dem Cloud-Anbieter vertrauen - und das hat vor allem mit dessen Vorgeschichte zu tun."

Daten lieber virtuell, oder doch besser auf dem eigenen USB-Stick?

Doch selbst bei renommierten Anbietern mit einer soliden Unternehmensgeschichte können Schwachstellen auftreten. Das hat Joshua Tiago von der IT Sicherheitsfirma Cirosec auf der diesjährigen IT-Defense Konferenz in Köln Mitte Februar gezeigt. Er hat eine Sicherheitslücke in einer Cloud-Anwendung von Microsoft offengelegt. "Ich habe einen regulären Account verwendet, wie Microsoft ihn für jeden Kunden bereitstellt. Dann habe ich die Funktionalität für meine Zwecke missbraucht", sagt der Profi-Hacker.

Wenn Schadsoftware in der Cloud entsteht

Konkret ging es um eine Anwendung, die dazu dient, dass Kunden von mehreren Standorten aus gemeinsam Software entwickeln können. Dazu müssen sie aber in der Lage sein, die Software auch zu testen. Also können sie das Programm auf einem Server in der Cloud ablaufen lassen. Und da liegt die Lücke im System: Eigentlich kennt sie jeder Computernutzer von Zu Hause: Starte niemals ein Programm auf Deinem Rechner, wenn Du nicht sicher bist, woher es kommt!

"Microsoft hatte nicht bedacht, dass ein Angreifer die Funktionalität missbrauchen könnte, um darüber Codes einzuschleusen und das System zu übernehmen", erklärt Tiago. So konnte er sich eine Hintertür in den Server einbauen. Über einige Umwege ist es ihm dann gelungen, auf die Daten anderer Nutzergruppen zuzugreifen. In der wirklichen Welt könnten das dann zum Beispiel andere Unternehmen sein, die beim selben Cloud-Anbieter Speicherplatz gemietet haben.

Gerade bei sensiblen Firmendaten rät der professionelle Hacker deshalb zur Zurückhaltung. "Man muss sich überlegen, welche Daten man bereit ist, in diese Cloud-Dienste zu packen", sagt Tiago. "Es ist natürlich ein großer Vertrauensvorschuss, den man diesen Unternehmen entgegenbringt - aber es ist auch eine sehr heikle Geschichte." Also gilt auch für die Cloud: Weniger ist im Zweifelsfall mehr!