FAQ

Peter Schüler

Sichere Cloud-Speicherdienste

Antworten auf die häufigsten Fragen

Risiken

Mit welchen Risiken muss man beim Einsatz eines Cloud-Speichers rechnen?

Relevante Gefahren rühren von technischen Defekten, von Datendiebstahl und Netzwerkausfällen durch externe Angreifer sowie von der möglichen Datenherausgabe durch Provider-Personal.

Auf technische Defekte dürfte ein gewerblicher Dienstleister besser vorbereitet sein als die meisten seiner Kunden, bei denen die Pflege der IT-Landschaft nur eine von vielen Aufgaben darstellt.

Die meisten gewerblichen IT-Dienstleister treiben mehr Aufwand bei der Abwehr von Eindringlingen als viele ihrer Kunden. Andererseits ziehen sie aber auch besonders viele Angriffe auf sich.

Davon unberührt bleibt die Gefahr, dass man bei einer Netzwerk-Störung nicht auf den Cloud-Speicher zugreifen kann. DOS-Attacken, welche die Internetverbindung eines Servers lahmlegen, bedrohen wohl direkt nur große und prominente Internet-Nutzer. Darunter leiden muss man aber gegebenenfalls auch als kleiner Kunde eines attackierten Providers. Bei manchen Arten von Informationen ist das freilich verschmerzbar – Handbücher, Kataloginhalte und Literaturlisten sind Beispiele für Daten, die sich in die Cloud auslagern lassen, ohne dass im Fall einer vorübergehenden Netzwerk-Unterbrechung gleich Probleme entstehen.

Außerdem sollte man sich vor Augen halten, dass die Admins beim Dienst-Anbieter auf alle gespeicherten Daten zugreifen und diese an Dritte herausgeben können – sei es aus kriminellen Motiven oder unter dem Druck eines behördlichen Ermittlers.

Vertragsanforderungen

Wie kann man den Umgang mit den Daten im Cloud-Speicher reglementieren?

Als Unternehmenskunde sollte man mit dem Anbieter eines Cloud-Speichers einen schriftlichen Vertrag abschließen, der einerseits die technischen Details regelt und andererseits festlegt, welches nationale Recht und welcher Gerichtsstand zum Tragen kommt und was nach Ablauf des Vertrags mit den gespeicherten Daten geschieht.

Für personenbezogene Daten verlangt das Bundesdatenschutzgesetz (BDSG) zudem eine schriftliche Vereinbarung zur Auftragsdatenverarbeitung, die ein seriöser Anbieter vor dem Vertragsabschluss schon von sich aus als Entwurf vorlegen wird. Sie muss vor allem den Auftraggeber schützen, denn dieser ist durchgehend Herr des Verfahrens und für alle Konsequenzen etwaiger Fehler verantwortlich. Paragraf 11 des BDSG stellt zusammen, was in einer solchen Vereinbarung alles zu regeln ist. Hinweise für die Kooperation mit ausländischen IT-Dienstleistern nach dem BGH-Urteil zum Safe-Harbor-Abkommen gibt der Beitrag „Hafen-Blockade“ in c’t 25/15, Seite 128.

Selbstschutz

Kann man sich vor unberechtigten Datenzugriffen durch Admins schützen?

Ja, wenn man einen Speicherdienst mit Ende-zu-Ende-Verschlüsselung verwendet. Dabei werden die Daten schon verschlüsselt, bevor sie den Rechner des Absenders verlassen, und erst dann wieder entschlüsselt, wenn sie der Anwender auf seinen Rechner heruntergeladen hat. In der Zeit dazwischen kann man die unberechtigte Weitergabe der verschlüsselten Daten zwar immer noch nicht verhindern, aber in diesem Fall kann niemand etwas damit anfangen. Entscheidend ist das Prinzip Zero Knowledge: Keiner der beteiligten Dienstleister darf Informationen erhalten, die er zum Entschlüsseln der kodierten Daten verwenden könnte.

Selbst dann muss man aber darauf vertrauen, dass die Client-Software, mit der man die Daten lokal verschlüsselt, ebenso wie jede andere Anwendung auf dem Rechner frei von Keyloggern und anderer Malware ist. Diese könnten nämlich jedes Geheimnis schon vor der Speicherung im Internet ausplaudern.

Nachrüstung

Sind „normale“ Cloud-Speicher wie Dropbox oder OneDrive für sichere Datenspeicherung unbrauchbar?

Nein. Praktisch in jedem Fall kann man seine Dateien selbst verschlüsseln, bevor man sie einem Cloud-Speicherdienst übergibt, und sie nach dem Download selbst wieder entschlüsseln. Dafür gibt es Zusatzdienste wie in c’t 19/15, Seite 106 vorgestellt.

Sicherheit und Teamwork

In vielen Fällen dient Cloud-Speicher als Teamwork-Hilfe, indem er Dokumente der Teammitglieder verschlüsselt im Web spiegelt. Kann man solche Dateien für andere Nutzer freigeben, ohne dabei das Passwort für die Entschlüsselung preiszugeben?

Ja. Einige Speicherdienste enthalten dafür passende Funktionen, die quasi auf Knopfdruck die nötigen Zugangsdaten asymmetrisch verschlüsseln und dann zum Empfänger übertragen, sodass sie sich nur mit dessen privatem Schlüssel dekodieren und für den Dateizugriff nutzen lassen. Die Grundlagen der Technik dazu erläutert der Beitrag auf Seite 174 in diesem Heft.

Krypto-Sicherheit

Welche Anforderungen muss ein Passwort erfüllen, um ausreichend sichere Verschlüsselung zu gewährleisten?

Für den Schutz von Dokumenten mit dem AES-Verfahren empfehlen Experten 64 Bit lange Schlüssel. Als Anwender braucht man sich damit jedoch nicht zu belasten – Softwaredienste generieren diese langen Schlüssel bei Bedarf aus einem vom Nutzer vorgegebenen Passwort. Dieses sollte eine Länge von mindestens acht Zeichen haben und Groß- und Kleinbuchstaben, Ziffern und möglichst auch Sonderzeichen enthalten. Auf keinen Fall sollte man ein sinnvolles Wort aus der Alltagssprache als Passwort wählen. Das lässt sich zwar leichter merken, doch solche Kandidaten werden von Angreifern als erste probiert. Besser fährt man mit Zeichenkombinationen etwa aus den Anfangsbuchstaben eines Satzes, den man sich leicht merken kann, zum Beispiel „G8d,sPzv“ („Gib 8 darauf, sichere Passwörter zu verwenden“).

Versehentlich gelöschte Dateien

Lassen sich irrtümlich in der Cloud überschriebene Dokumente aus dem Backup des Dienst-Anbieters wiederherstellen?

Normalerweise nicht. Diese Option scheidet aus, weil die meisten Speicher-Anbieter gar nicht mit Backups arbeiten. Stattdessen nutzen sie für den Fall eines Hardware-Defekts redundante, auf mehrere Orte verteilte Speichersysteme. Allerdings kann man mit den meisten marktüblichen Speicherdiensten Dateien versionieren – dann überschreibt der Server eine veränderte Datei nicht mit der neuen Fassung, sondern speichert die jeweils jüngste Version zusammen mit einer einstellbaren Zahl vorheriger Fassungen. (hps@ct.de)