ARTIKEL Datensicherheit

Sichere Wolke

Internationale Standards zur IT-Sicherheit schützen Daten in der Cloud. Anbieter sollten zertifiziert sein und transparente Verträge anbieten.

VON OTMAR RHEINHOLD

Zurecht sorgen sich Firmen und Privatanwender beim Cloud Computing um die Sicherheit ihrer Daten. Was passiert eigentlich mit meinen Daten, wenn sie auf einem „fremden" Rechner liegen? Wer garantiert, dass niemand den Datenverkehr anzapft? Was ist, wenn das Rechenzentrum abbrennt?
Und noch ein Aspekt wird oft vernachlässigt. Er betrifft den physischen Verbleib der Daten. Gerade bei günstigen, leicht zugänglichen Public Cloud-Angeboten ist oft völlig unklar, wo die Server physisch stehen. Die Gefahr ist gross, dass sie sich in Ländern befinden, die es mit dem Datenschutz nicht sehr ernst nehmen. Am besten fahren Kunden mit Anbietern, die einen Standort in der Schweiz oder der EU garantieren – die Zone mit den nach Ansicht vieler Experten besten Datenschutz- und -sicherheitsvorschriften. Zudem sind andere Standorte, etwa für Finanzdaten, oft gar nicht legal.

Auf Zertifikate achten

Wenn sich viele Anwender gemeinsame Ressourcen teilen, kann es bei nicht standardgemässer Handhabung durch den Anbieter zum Beispiel zu unerlaubten Zugriffen auf fremde Datenbankinhalte kommen. Dann nutzt auch die sicherste Datenverschlüsselung für die Verbindung in die Cloud, etwa über ein Virtual Private Network (VPN), nichts mehr. Deshalb sollten Anbieter grundsätzlich Testate über ihre Zuverlässigkeit nachweisen können. Goldstandard ist hier die Zertifizierung nach der

internationalen Sicherheitsnorm ISO 27001. Sie beruht zu grossen Teilen auf den Richtlinien zum IT-Grundschutz, den das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt hat. Die Richtlinien der BSI finden auch in der Schweiz breite Anwendung, viele Cloud-Anbieter sind nach ihnen zertifiziert. Für das Management von IT-Services können sich Unternehmen nach der internationalen ISO 20000 zertifizieren lassen, ein weiterer Hinweis auf Vertrauenswürdigkeit.

Transparente Verträge

Von diesen Standards abgesehen gilt für die Vertragsgestaltung: Ohne transparente Vereinbarungen kein Geschäft. Das bezieht sich nicht nur auf die Abrechnungsmodalitäten. Es muss klar sein, welche Massnahmen der Dienstleister zur Datensicherheit und zum Datenschutz im Rahmen der Standards trifft – von der physischen Zugangskontrolle bis zur Passwortverwaltung. Auch, was im Falle einer Vertragsauflösung passiert, muss geregelt sein. Anwendern – privaten wie geschäftlichen – muss es problemlos möglich sein, mit Daten und Anwendungen umzuziehen. Dafür muss der Dienstleister anerkannte Standards der Portabilität einhalten und es müssen klare Schnittstellenvereinbarungen getroffen werden. Für den Fall, dass Server physisch ausfallen, muss ein Notfallplan bestehen, der für die weitgehend unterbrechungsfreie Kontinuität der Dienstleistung sorgt.
Angst vor der Cloud muss deshalb niemand haben. Wichtig ist nur, dass die Geschäftsbeziehungen auf diesem Gebiet denselben Sicherheitsmassnahmen unterliegen wie andere Outsourcing-Dienstleistungen auch. Für erfahrene Geschäftsleute und kluge Privatnutzer selbstverständlich. Denn auch wenn die Welt vernetzt ist – sicher sollte die Sache schon sein. ■

GASTBEITRAG Sicher in der Cloud

Den Kopf in der Cloud – die Füsse auf der Erde

Alles spricht von der Cloud – viele Firmen profitieren vom immensen Potenzial der Cloud-Technologie. Die Risiken lassen sich mit den richtigen Massnahmen bewältigen.

Die sichere Nutzung der Cloud-Technologie setzt ein effektives Risikomanagement voraus – was viele Unternehmen im Vertrauen auf die Privatheit ihrer Daten beim Betrieb einer eigenen Infrastruktur oft unterlassen. Sie müssen nun oft zum ersten Mal ihre Datenstrukturen katalogisieren: Wo sind die Informationen gespeichert, wer hat darauf Zugriff und wie geschäftskritisch sind die Daten? Danach erfolgt eine Abwägung mit dem geschäftlichen Nutzen.

Mehr Sicherheit erlangen

Die „Cloud" an und für sich weckt bei vielen Menschen nur wenig Vertrauen. „In der Cloud" heisst für viele „im Nebel". Die damit verbundenen Ängste sind oft mit dem empfundenen Kontrollverlust über die ICT-Infrastruktur erklärbar. Die effektiven Kontrollmöglichkeiten sind aber meist grösser als angenommen, der Support professionell und die hohe Flexibilität und Anpassbarkeit beseitigen meist die Bedenken.
Heute lässt sich die ICT-Infrastruktur eines kleineren und mittleren Unternehmens kaum mehr kostengünstig und gleichzeitig hoch sicher betreiben. Die Anforderungen an die hier meist unterdimensionierte ICT-Abteilung sind schlicht zu gross.

Reto Häni,
Chief Security Advisor, Microsoft Schweiz

Ein erfahrener Cloud-Provider hingegen setzt zur Absicherung seiner Rechenzentren definierte Prozesse, geschulte Leute sowie State-of-the-art-Technologien ein und erzielt so eine weitaus höhere Sicherheit bei tieferen Kosten, als dies vielen Unternehmen je möglich wäre.
So manches Management hegt dennoch Befürchtungen, die Daten seien nicht sicher genug gespeichert – Berichte über erfolgreiche Hackerangriffe und offengelegte Daten im Hinterkopf. Zudem wirken sich rechtliche Grundlagen auf Unternehmen und ihre Datendienstleister aus. Um es kurz zu sagen: Gegen behördlichen Zugriff sind auch Cloud-Provider machtlos; sie müssen sich wie ihre Kunden und auch die Behörden, an bestehende Gesetze halten. Die meisten erfolgreichen Hackerangriffe nutzen bekannte Schwachstellen. Cloudlösungen sind hier im Vorteil, da sie immer aktuell sind.
Wer trotzdem ein mulmiges Gefühl hat, kann seine heiklen Daten selbst verschlüsseln und die Schlüssel bei sich unternehmensintern behalten. So sind die Informationen auch gegen mutwilligen oder versehentlichen Abfluss durch Externe oder Mitarbeitende geschützt.

Fazit: Fast eine Vertrauenssache

Die effektive Sicherheit in der Cloud ist weitaus höher als in den meisten Firmennetzwerken. Das sicherste Indiz für eine hohe Cloud-Qualität ist die Zertifizierung des Providers nach dem ISO 27001-Standard – und seine Bereitschaft zur Transparenz. Letztlich sollten die Nutzer im Unternehmen oder zu Hause gar nicht mitbekommen, wo die Daten gespeichert werden, sondern aus einer gepflegten, sicheren Cloud-Infrastruktur mehr Produktivität, optimierte Prozesse und das höchste Mass an Sicherheit geniessen. ■

Die sichere Cloud

- Vertrauen: Auf ISO 27001 Zertifizierung des Providers achten
- Transparenz einfordern: Leistungsausweis, Speicherort der Daten, Sicherheitsaudits, Datenschutz
- Rechtliche Aspekte klären: Vertragsrecht, Datenschutz, Informationssicherheit und Compliance
- Risikomanagement und -Assessment vor dem Gang in die Cloud: Welche Daten sind geschäftskritisch, wer hat Zugriff und wo liegen sie? Welche Applikationen sind geschäftskritisch und können/müssen intern auch ohne Internetverbindung betrieben werden?
- Internetzugriff: Im Zuge der Cloud-Pläne sollte die Verfügbarkeit des Zugangs verbessert und gesichert werden.

Werbebeitrag — Verbandspräsentation

Ist Cloud Computing sicher unsicher?

Cloud Computing – das grosse Schlagwort in der Informatik. Wer in die Cloud einsteigt, sei im Trend. Bei „Software as a Service" (SaaS) übernimmt der Anbieter das Patchmanagement, was insbesondere KMUs von dieser aufwendigen Sicherheitsaufgabe befreit. Wenn es um Marketing geht, werden vor allem die Vorzüge dargestellt, selten aber die kritischen Sicherheitsfragen des Abenteuers „Cloud" gestellt. Die meisten interessierten Firmen zitieren den Datenschutz als ihre wichtigste Sicherheitsfrage. Wo sind die Daten gespeichert? Wer kann Sie wie abrufen? Bei den betriebswirtschaftlichen Fragen müssen die Kosten von Datenpannen, Meldepflichten und Imageschaden beantwortet werden. Die Verschlüsselung der Daten bei ihrem Transport in die Cloud und bei deren Speicherung müssen angesprochen werden. Dabei ist der Verwaltung der Schlüssel eine grosse Bedeutung beizumessen. Um eine gute Lösung mit dem Provider zu erreichen, sind klare interne Richtlinien inklusive Klassifizierung der Daten nötig, denn kritische Daten sind oft nur bedingt geeignet für die Cloud. Unternehmen benötigen aber auch Einblick in den Sicherheitsstatus ihrer Wolke. Dazu gehört Change-Management, Incident-Management wie auch Incident-Reporting. Ebenfalls sollte der Einblick in die spezifischen Log- und Audit-Daten gewährleistet sein. Öffentliche Clouds sind oftmals „Blackboxes", bei denen der Kunde nicht selbst die Einhaltung der Compliance-Vorschriften wie zum Beispiel The Sarbanes-Oxley Act, HIPAA oder das Datenschutzgesetz überprüfen kann. Klare Service Level Agreements bieten hier Abhilfe. An der Berner Tagung 2011 der Information Security Society Switzerland (ISSS) wurde vom Informatikstrategieorgan Bund erklärt, dass auch die Schweizer Behörden bereits geeignete Dienste in die Cloud auslagern.
Fazit: Die Cloud ist tendenziell sicherer als die traditionelle Art des IT-Betriebs, insbesondere bei KMUs ohne eigene IT-Sicherheitsfachleute. Die zahlreichen Vorteile des Cloud Computings bieten es an, selbst einen Versuch zu starten. Es braucht aber klar festgelegte Anforderungen an den Provider, die vom Anwender überprüft werden können, sowie vertraglich geregelte Verantwortungsabgrenzungen. Es ist von grosser Bedeutung, welchen Cloud-Partner man wählt. ■

ISSS-Präsident Dr. Thomas Dübendorfer spricht an der Berner Tagung "Cloud Computing".

„Full-house" an der Berner Tagung der Information Security Society Switzerland (ISSS) zu Cloud Computing.

Weitere Informationen

Der Verein Information Security Society Switzerland (ISSS) vernetzt über 900 Security Professionals in der Schweiz. Mit Tagungen, Security Lunches, Special Interest Groups, Mitwirkung an Vernehmlassungen sowie dank Weiterbildungsrabatten sind deren Mitglieder bestens informiert zu aktuellen Trends der Informationssicherheit. Alles Weitere auf **www.isss.ch**.