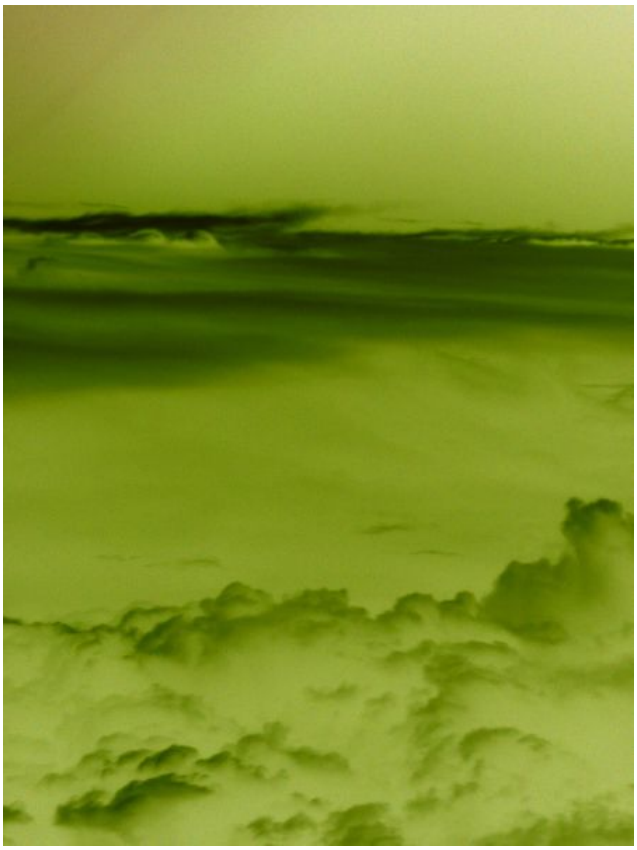
Risiko-Minimierung durch Analyse

VON MEL BECKMAN



Der Dialog geht dann so weiter:

„Ist es sicher?“ wiederholt Olivier.

„Was soll sicher sein?“ antwortet Hoffman.

„Ist es sicher?“

„Ich weiß nicht, was Sie meinen.“

„Ist es sicher?“

„Sagen Sie mir, worauf sich die Frage bezieht.“

„Ist es sicher?“

„Ja, es ist sicher. Sehr sicher. Sie können sich gar nicht

vorstellen, wie sicher.“

„Ist es sicher?“

„Nein, es ist nicht sicher. Es ist sehr gefährlich. Seien

Sie vorsichtig.“

Schließlich sticht Olivier mit einem Dentalwerkzeug Hoffman in die Mundhöhle, dieser schreit vor

Schmerz. Wie man sich vorstellen kann, gehen die Dinge für unseren unglücklichen Helden von da an bergab.

Viele Cloud Nutzer – die-selben Schwierig-keiten

Das Problem der von Hoffman dargestellten Person ist ganz einfach, dass er nicht weiß, wie er Olivier´s Frage beantworten könnte. Viele, die heute Cloud in ihrer IT einsetzen, sehen sich denselben Schwierigkeiten gegenüber, wenn sie eine ähnliche Frage beantworten sollen: Ist die Cloud sicher? Manche sagen, „Sie ist sehr sicher. So sicher, dass ich es kaum glauben kann." Andere warnen, „Nein, sie ist nicht sicher. Sie ist sehr gefährlich. Seien Sie vorsichtig."

Die richtige Antwort hängt von drei Faktoren ab:

- Wie heikel sind Ihre Daten oder die Anwendung?
- Wer macht Sie für die Sicherheit der Cloud-Anwendung in Ihrem Unternehmen verantwortlich?
- Inwieweit können Sie die Sicherheitsmaßnahmen überhaupt selbst einstellen?

Sobald Sie diese drei Fragen mit Bezug auf ein Datenelement bzw. einen Bestandteil einer Anwendung beantwortet haben, können Sie auch beurteilen, wie sicher deren Handhabung in einer Cloud- Umgebung ist.

Wie heikel?

Der erste Test für die Zulassung zur Cloud ist die Einschätzung, wie heikel die jeweiligen Daten bzw. eine Anwendung sein mag. Also: Sollte eine Sicherheitslücke die Daten/Anwendung kompromittieren, wie hoch wäre der Schaden? Hier kann man natürlich argumentieren, dass einfach alles in einer Unternehmensumgebung schützenswert ist – in Wirklichkeit sind aber manche Dinge gar nicht so wichtig.

Der Arbeitszeitplan Ihres Putzpersonals könnte beispielsweise sehr gut in Google Apps verwaltet werden. Würde dieser Putzplan versehentlich bekannt, wäre das dann ein großes Schadenspotenzial? Wahrscheinlich nicht. Natürlich kann man sich ein Szenario vorstellen, in dem ein raffi nierter Angreifer für seinen Einbruchsplan die Zeiten der Putzkolonne benötigt, aber wir sprechen ja hier nicht von KEINE Sicherheit: Google Apps unterstützt Passwort und Verschlüsselungstechnologie, die kostenfrei eingesetzt werden kann. Nichts ist risikolos, aber die Putzfrau in der Cloud stellt wohl eher keine wichtige Sicherheitslücke dar.

Was muss geschützt werden?

Bei der Frage danach, ob etwas geschützt werden muss, sollte man sich zunächst die grundlegenden Sicherheitsmaßnahmen des Cloud Providers ansehen. Wer die Cloud einsetzt, sollte dem Cloud Provider vertrauen und dieses Vertrauen durch eine Überprüfung der Sicherheit untermauern. Ein Versprechen wie, „so sicher, wie Sie es sich kaum vorstellen können“, ist wesentlich weniger glaubwürdig, als „wir verwenden 256/ bit AES-Verschlüsselung und Sie generieren und speichern Ihre Schlüssel selbst.“ In Abschnitt drei fi nden Sie einige der üblichen Sicherheitsmaßnahmen. Cloud- Kandidaten, die nur eines geringen Schutzes bedürfen, können mit dem günstigsten Schutz gesichert werden und man braucht auch nicht so viel Zeit in die Evaluierung der Schutzmaßnahmen des Providers zu investieren.

Manche Daten nicht in die Cloud

Am entgegengesetzten Ende der Skala kann man manche Daten ganz mühelos in die Rubrik einordnen, die man auf keinen Fall in der Cloud speichern sollte: das Passwort zu Ihrem Schweizer Bankkonto, der Grundriss Ihres geheimen Regierungs-/Forschungslabors, die Dokumentation Ihrer Zutrittsberechtigung für das Firmengebäude. Überraschenderweise haben Hacker genau diese Informa tionen in Cloud-Storage gefun den, wo sie unbeabsichtigt der allgemeinen Öffentlichkeit zugänglich wurden. Es lohnt sich also, zu prüfen, wie heikel die Daten sind, die sich jetzt in der Cloud befi nden bzw. die Sie künftig in der Cloud speichern wollen. Die Cloud ist noch nicht so zuverlässig wie Hardware, die Ihnen selbst gehört und die Sie selbst kontrollieren.

Es ist empfehlenswert, eine Liste der Daten und Anwendungen zu erstellen, die nicht in die Cloud dürfen. Diese Liste gehört dann in die Dokumentation der Unternehmenssicherheit. Anschließend muss man sicherstellen, dass alle involvierten Mitarbeiter diese Liste regelmäßig auf Aktualität überprüfen. Sie sollten auch alle Mitarbeiter, die eventuell Cloud-basierte Systeme einsetzen wollen, verpfl ichten, in allen Fällen vorher die Genehmigung des Managements einzuholen. Die Fußballmannschaft des Unternehmens auf Facebook zu haben ist eine Sache, die Kundenliste des Unternehmens dort zu speichern, ist eine ganz andere Sache. Und doch haben Mitarbeiter, die die Risiken von Cloud Services nicht richtig einschätzen können, ihren Unternehmen durch unbeabsichtigte Veröffentlichung von Unternehmensgeheimnissen großen Schaden zugefügt.

Unklarheiten, was in die Cloud soll

Zwischen diesen beiden Extremen sind viele unklare Fälle angesiedelt, in deren Zuordnung man die meiste Zeit investieren muss. Wenn Ihr eCommerce System beispielsweise Kreditkarten akzeptiert und Sie das System in die Cloud verlagern wollen – würde das Speichern von Kartendaten dann ein

Problem darstellen? Eine rasche Sichtung der eCommerce Lösungen ergibt viele Cloud-basierte, also scheint das jemand für ok zu halten. Schaut man jedoch genauer hin, so wird klar, dass man die Kreditkartendaten nach Abschluss der Transaktion überhaupt nicht zu speichern braucht, da man mit Tokens arbeiten kann, um die gefährlichen Zahlungsinformationen aus der Cloud-Datenbank zu entfernen.

Während Sie das Angebot an Cloud-Kandidaten nach Sicherheitslücken durchforsten, wird sich mit der Zeit eine Liste an Anwendungen und Daten herauskristallisieren, die für die Cloud zwar infrage kommen, aber doch bei Offenlegung ein zu hohes Risiko darstellen. In solchen Fällen können Sie die Sicherheit durch zusätzliche Schutzmaßnahmen erhöhen. Somit kommen wir zum nächsten Schritt des Cloud-Selektionsprozesses.