

# Schutzmaßnahmen zur Informationssicherheit in Cloud-Anwendungen

Dr. Gerhard Klett

31.03.2010

Cloud Computing stellt Unternehmen und Institutionen gemeinsame Datenspeicher, Applikationen und Hardware über das Internet auf Abruf zur Verfügung. Ermöglicht wird diese Form der IT-Infrastruktur durch eine Kombination aus Virtualisierung und Outsourcing.

Cloud Computing unterscheidet sich durch die Entkopplung der Daten und Applikationen von Speicherplatz und Servern sowie deren Lokation signifikant von herkömmlicher IT-Infrastruktur. Die traditionellen physikalischen Grenzen wie bauliche Gegebenheiten oder Netzwerkübergänge, die mit zum Schutz von Informationen in einem Unternehmen dienen, sind in der Cloud nicht mehr vorhanden.

Clouds sind sehr flexible Gebilde, die ihre Ausdehnung und ihren Standort, beispielsweise durch die Vertragsgestaltung des Cloud-Anbieters mit seinen Subkontraktoren, ständig verändern können. Die Analyse und die Bewertung der Risiken für den Informationsschutz gewinnen dadurch an Komplexität. Die Anforderungen an den Informationsschutz, das heißt die Integrität, Vertraulichkeit, und die Verfügbarkeit der Informationen in einem festgelegten Umfang zu gewährleisten, steigt beim Übergang zum Cloud Computing stark an.

Dabei ändern sich die Standards, Verfahrensweisen, Methodiken zur Einhaltung von Informationssicherheit nicht grundlegend; sie müssen aber an die Gegebenheiten des Cloud Computing adaptiert werden. In besonderem Maß muss der Informationsschutz durch einen erhöhten Abstraktionsgrad der outgesourcten Virtualität mit Zugang zur Cloud als Service im Internet Rechnung tragen.

Zum Beispiel kann in der Cloud eine sehr konkrete Regel in der Security Policy des Unternehmens, dass bestimmte Dienste und Ports auf einem Unix Server mit dem Betriebssystem Redhat Linux zu sperren sind, in der Cloud nicht eingehalten und überprüft werden, da man als Unternehmen bei der Verwendung von Diensten in einer Cloud in der Regel weder die Hardware noch das Betriebssystem oder den Standort des Servers kennt.

Als weiterer Aspekt kommt hinzu, dass der Begriff der Benutzeridentität beim Cloud Computing zu erweitern ist. In der Cloud kommen neben den obligaten Mensch-Maschinen Kommunikationen zahlreiche Maschinen-Maschinen Transaktionen hinzu.

Wichtig für Informationssicherheit ist ebenfalls, in einem Unternehmen vor dem Übergang in das Cloud Computing Vorgehensweisen und Prozesse zu etablieren, wie der in Frage kommende Cloud-Anbieter hinsichtlich der Etablierung einer Vertrauensbasis evaluiert und im Betrieb überwacht werden kann. Die dafür in Frage kommenden Prozesse und Maßnahmen mit ihren Schlüsselindikatoren sind für die weitere Vertragsgestaltung mit dem Cloud Anbieter in Form von Service Level Agreements von großer Relevanz.

Wichtige Maßnahmen zur Etablierung einer Vertrauensbasis sind beispielsweise:

- Klare, festgelegte Regelwerke und Vorgehensweisen zum Schutz sensibler Daten
- Nachweis der Einhaltung von Informationssicherheits- und Compliance Standards wie, z.B. ISO 27001, ISO 27005, Sarbanes Oxley Act, etc. durch den Cloud Anbieter und seiner Subkontraktoren. Der Nachweis wird in der Regel durch erfolgreiche Zertifizierung oder durch die Vorlage eines Prüfberichtes wie zum Beispiel bei Sarbanes Oxley ein SAS70 Report für den Betrachtungszeitraum erbracht.
- Transparenz der Informationsverarbeitung in der Cloud, Anwendung des 4-Augen- Prinzips (segregation of duty) bei wichtigen, festgelegten, administrativen Vorgängen; dabei sollten 2 Augen aus dem eigenen Unternehmen kommen.
- Kenntnis der Vorgehensweise des Cloud Anbieters beim Einrichten virtueller Maschinen
- Separierung sensibler Unternehmensdaten und Anwendung von Verschlüsselung wenn immer möglich.

Im eigenen Unternehmen ist der Zugang zur Cloud kritisch zu betrachten, da er mit hohen Risiken behaftet sein kann. Man betrachte beispielsweise einen Finanzdienstleister, der einen Teil seiner Infrastruktur in einer Cloud betreibt und deren Zugänge über unzureichend abgesicherte Browser einen Diebstahl von Benutzeridentitäten über das Internet mit Hilfe von so genannter Schadsoftware („Malware“), darunter fallen Computerviren, -würmer und Trojaner, ermöglichen.

Als Schutzmaßnahmen beim Zugang zu sensiblen Applikationen und Daten in einer Cloud ist als erstes auf eine starke Authentifizierung des Benutzers zu achten. Eine Authentifizierung über eine Benutzeridentifikation und ein Passwort ist in der Regel nicht ausreichend. Von einer starken Authentifizierung spricht man, wenn man zwei schwer kompromittierbare Verfahren wie regelmäßig wechselnde Passwörter mit vorgeschriebenen Bildungsregeln und einen personifizierten Gegenstand

(z.B. Chipkarte) oder ein evaluiertes, biometrisches Merkmal zur Authentifizierung verwendet. Zugriffe über mobile Geräte wie Smartphones sollten die absolute Ausnahme in Notfällen bleiben, da diese Geräte milieuwechselnd sind und von ihrer Ausstattung her ein hohes Sicherheitsrisiko darstellen. Es muß technisch unterbunden werden, administrative Tätigkeiten über ein Smartphone in der Cloud auszuführen.

Aktuelle Patches und Updates für Client-Betriebssystem und Browser sind zeitnah von der zentralen Administration im Unternehmen einzuspielen. Regelmäßige Audits und Risikomanagement mit Fokus auf die Zugänge des Unternehmens zur Cloud unterstützen die Einhaltung der Unternehmensrichtlinien und sichern die korrekte Funktionsfähigkeit der installierten Schutzmaßnahmen.

Zusammenfassend lässt sich sagen das Cloud Computing mit allen seinen wirtschaftlichen Vorteilen ein Paradigmenwechsel bei der Gestaltung der IT-Infrastruktur darstellt, der wesentliche Implikationen auf die Ausgestaltung des Informationsschutzes eines Unternehmens hat. Eine auf Cloud Computing abgestimmte Security Policy mit genau festgelegten vertraglichen Vereinbarungen mit dem Cloud-Anbieter über Ausgestaltung und Überprüfung von Sicherheitsmaßnahmen sowie Konsequenzen bei deren Nichteinhaltung treten dabei zusammen mit einem adäquaten Zugriffsschutz in den Vordergrund.