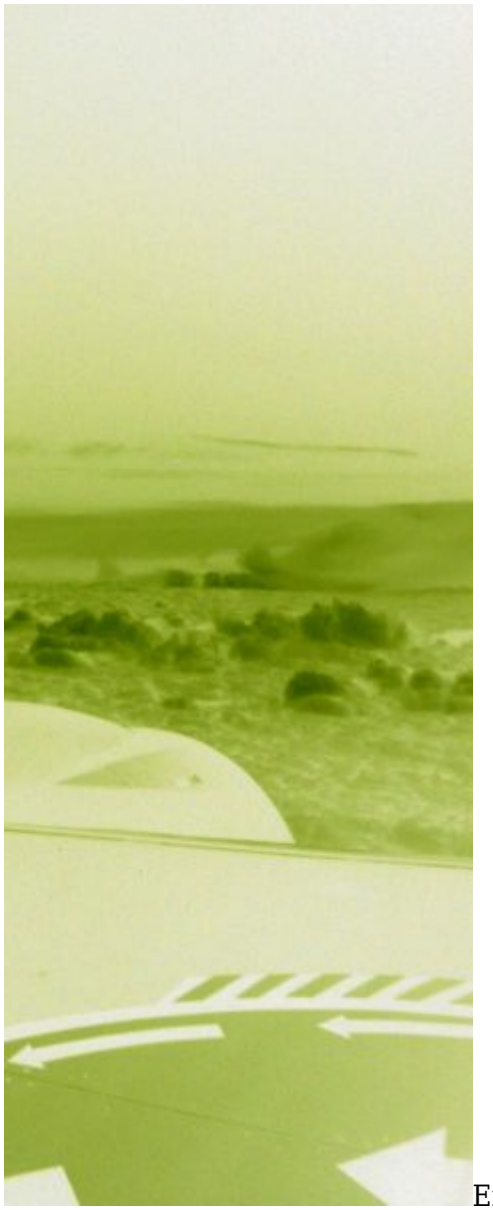

Ein zentrales Sicherheitsproblem bei der Nutzung von Cloud-Services liegt darin, dass Administratoren des Service-Providers Zugang zu unternehmenskritischen Applikationen, Prozessen, Services, Systemen oder Daten erhalten. Laut Sicherheitsexperte Cyber-Ark ist es deshalb unerlässlich, vor einer Entscheidung für die Cloud genau zu überprüfen, welche Lösungen der Service-Provider in diesem Bereich einsetzt und wie er Zugriffsmöglichkeiten regelt beziehungsweise überwacht.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinem Ende September 2010 veröffentlichten Eckpunktepapier zum Thema Informationssicherheit beim Cloud Computing das ID- und Rechtemanagement als Basisanforderung für Cloud-Anbieter definiert und unter anderem betont: „Das Rechtemanagement muss gewährleisten, dass jede Rolle nur die Daten (auch Metadaten) sehen darf, die zur Erfüllung der Aufgabe notwendig sind. Das gilt auch für Administratoren.“(1)

Worauf sollte der an einer Cloud-Lösung Interessierte folglich genau achten? Die acht konkreten Tipps von Cyber-Ark im Überblick:

1. Management privilegierter Benutzerkonten: Der Service-Provider muss ein Privileged-Identity-Management-System für die Verwaltung privilegierter Accounts im gesamten IT-Betrieb implementiert haben, damit der Nutzer der Cloud die Gewähr hat, dass Policies, Prozesse und Practices seine Anforderungen an die Datensicherheit erfüllen. Dabei sollten Standards wie ISO

27001 oder 27002 eingehalten werden.

2. Policy-Konformität: Die Policies und Prozesse des Privileged Identity Management auf Providerseite müssen den unternehmenseigenen entsprechen. Im Idealfall sind sie alle ISO-basiert.