TEC WORKSHOP

Link: https://www.tecchannel.de/a/flexibilitaet-aus-der-wolke,2044493

IAM-Services aus der Cloud haben Potenzial

Flexibilität aus der Wolke

Datum: 09.09.2013
Autor(en): Werner Kurzlechner

Die Identitäts- und Zugriffsverwaltung wird immer anspruchsvoller, je mehr Services aus der Cloud genutzt werden. Aus der Wolke kommen auch IAM-Lösungen, die nach Analystenmeinung großes Potenzial haben, aber auch noch reifen müssen.

Stöbert man mit den Suchbegriffen „Cloud" und „Identity & Access Management" (IAM) im Internet, findet man Überschriften wie Heilsversprechen. Eine „Segnung" sei Cloud Computing fürs IAM. Richtig daran ist, dass es in der Wolke reichlich attraktive Services auch fürs IAM gibt. Aus IT-Sicht macht das die Lage aber nicht zwingend übersichtlicher. Es droht, zusätzliche Komplexität in die Systemlandschaft gespült zu werden, wenn die User selbst für einen IAM-Wildwuchs sorgen. Vor diesem Hintergrund kommen die Analysten von Ovum in einer aktuellen Studie zu einem weniger euphorischen Urteil. Ja, Cloud Computing transformiere IAM, sagt Ovum-Analyst Andrew Kellett. Aber das bringe auch Aufgaben mit sich, die erst einmal gemeistert werden müssen.

Irgendwann in der Zukunft findet IAM womöglich gänzlich in der Cloud statt. „In absehbarer Zeit werden die Firmen aber eine Mischung aus On-Premise-, gehosteten und cloud-basierten Systemen und Dienstleistungen nutzen", so Kellett. Der zunehmende Einsatz von Cloud Services sorge aktuell für steigenden Bedarf nach besseren und interaktiven Möglichkeiten für Single Sign-Ons (SSO) und Federated Identity Management (FIM).

1. Gefährliche Schatten-IT

Wie auch in anderen Feldern zu beobachten skizziert Ovum die Wolke als doppelten Faktor: Zum einen kommen aus der Cloud neue IAM-Angebote, was etablierte Anbieter unter Druck setzt und Anwendern attraktive Alternativen bietet. Zum anderen schafft die zunehmende Nutzung der Cloud allgemein Probleme, die ein funktionierendes IAM notwendiger und schwieriger gestalten. 80 Prozent der Unternehmen weltweit versorgen sich laut Kellett momentan schon zu einem gewissen Grad mit Services aus der Wolke. Das geschehe zum Teil strategisch; zum Teil aber auch auf Ad-Hoc-Basis durch die Mitarbeiter – also ohne Rückkoppelung an die IT-Abteilung. So entstehe die berüchtigte Schatten-IT mit ihren negativen Folgen hinsichtlich Infrastruktur, Kontrolle und Sicherheit.

Für Unternehmen erscheine es da als einzig sicherer und gangbarer Weg, nur über ein einziges Identitätsmanagement-System den Login in die Business-Systeme zu erlauben – und zwar Cloud-Dienstleistungen inklusive. Auf IAM-Anbieterseite wiederum arbeite man an einem möglichst sicheren Übergang zwischen On-Premise-Systemen und Cloud-Services. Zum Teil würden die Angebote auch so rekonfiguriert, dass die IAM-Lösungen direkt aus der Cloud geliefert werden können. „Die Frage ist allerdings, ob die damit verbundenen Versprechen eingehalten werden können", so Ovum-Analyst Kellett. Die Antwort darauf müsse zwiespältig ausfallen, weil zum Teil ausgefeilte Cloud-Strategien vorhanden sein, zum Teil aber auch nicht. Insgesamt bedürfe es noch deutlich größerer Reife, die Anforderungen an Cloud-IAM müssten geklärt werden.

Dennoch lässt Ovum am Potenzial keinen Zweifel. „Die Cloud bleibt eine Chance für den IAM-Sektor", sagt Kellett. Gepunktet werden könne durch größere Flexibilität, mehr Benutzerfreundlichkeit und Kosteneffizienz.

2. BYOD verkompliziert IAM

Wie IAM im Cloud-Zeitalter auf Basis von Benutzerrollen und -rechten konkret aussehen kann, hat vor einiger Zeit Wolfgang Hirsch für die Computerwoche erläutert. „Auf dieser Grundlage legt ein IAM-System fest, steuert und kontrolliert, welche Anwender auf welche Informationen und Applikationen zugreifen dürfen", so der Autor. „Zugang erhalten diese erst dann, wenn sie sich erfolgreich identifiziert haben, zum Beispiel anhand einer Chipkarte, eines Passworts oder eines biometrischen Verfahrens – und zwar für alle Daten und Dienste, die an das IAM-System angeschlossen sind."

Verkompliziert wird IAM im Cloud-Zeitalter aber auch dadurch, dass wegen Bring-Your-Own-Device und des Mobility-Trends nicht nur die stationären Rechner, sondern eine ganze Schar von Geräten und Gerätetypen gesteuert werden müssen. Andreas Cser und Eve Maher, Analysten bei Forrester Research, gehen davon aus, dass der Fokus der Firmen deshalb vorerst auf der Konsolidierung der Directories liegt. Die Experten empfehlen die laufende Überprüfung der Zugriffsrechte, die Zusammenarbeit der IAM-Teams mit den Compliance- und HR-Verantwortlichen sowie ein Augenmerk auf das Zusammenspiel von IAM-Systemen und genutzten Cloud Apps.

In der Cloud haben neben jungen Spezialisten auch Software-Riesen wie Microsoft die Bedeutung von IAM erkannt. Auf der Cloud-Plattform Windows Azure sorgt der Service Active Directory für eine einfache Identitäts- und Zugriffsverwaltung. Benutzer und Cloud-Anwendungen werden in einem Verzeichnis verbunden, um eine nahtlose Anmeldung bereitzustellen. Diese kann mithilfe einer mehrstufigen Authentifizierung geschützt werden. Mit der mehrstufigen Authentifizierung wird der nicht autorisierte Zugriff auf lokale Anwendungen und Cloud-Anwendungen verhindert, indem eine zusätzliche Authentifizierungsebene geschaffen wird. Die Anzahl von Helpdesk-Anfragen und zurückgesetzten Kennwörtern kann laut Microsoft reduziert werden, indem den Benutzern lediglich ein Satz von Anmeldeinformationen für alle Anwendungen und eine Start-Webseite bereitgestellt werden.