IAM aus der Cloud – aber sicher

Unter der Prämisse betriebswirtschaftlicher Effizienz, Flexibilität und Skalierbarkeit nutzen Unternehmen zunehmend cloudbasierte Dienste. Dabei müssen sie sich auch im Bereich Identity und Access Management (IAM) neuen Herausforderungen stellen.

Digitale Identitäten überschreiten die Grenzen von Unternehmen. Mitarbeiter, Kunden und Partner sollen dennoch sicheren und einfachen Zugriff auf lokale wie auch cloudbasierte (SaaS) Anwendungen haben. Identity und Access Management «as-a-Service» (auch IAMaaS genannt) bietet dazu vielversprechende Lösungsansätze.

Wie funktioniert das?

Um IAMaaS zu zu verwenden, melden sich Nutzer an einem Portal einmalig an und erhalten Zugriff auf alle für sie autorisierten cloudbasierten und lokalen Anwendungen. Für die Authentisierung werden die in die Föderation integrierten lokalen und externen Identity Provider (IDP) miteinbezogen, wie etwa das lokale Active Directory. Abhängig vom erforderlichen Schutzbedarf ist eine Multi-Faktor-Authentifizierung (MFA) erforderlich.

Vereinfacht ausgedrückt werden Identitäten und Zugriffe für eine Vielzahl von lokalen wie auch cloudbasierten Anwendungen konsolidiert in einem zentralen Identity Store verwaltet. Dabei spielen Unternehmensgrenzen keine Rolle mehr, wenn sich mehrere Unternehmen zu einer Föderation zusammenschliessen. Die Nutzer der Anwendungen greifen mittels Single Sign-on (SSO) auf die Anwendungen zu. IAMaaS bietet Unternehmen in vielerlei Hinsicht markanten Mehrwert (siehe Kasten). Doch trotz der vielen Vorteile und der allgemeinen Notwendigkeit eines strukturierten Identity- und Access-Managements tun sich Entscheider oft schwer, eine solche Lösung zu implementieren.

Reflexartige Abwehrhaltung gegen die Cloud

Denn sie sind gegenüber einem Outsourcing in die Cloud oder einem sicherheitsbezogenen Leistungsbezug aus der Cloud skeptisch eingestellt und beziehen ihre Stellung oftmals mit reflexartiger Abwehrhaltung. Insbesondere KMUs verzichten meist aus Kosten-, Komplexitäts- oder Know-how-Gründen darauf, die innere Sicherheit auf einen zeitgemässen und den bekannten sowie unbekannten Risiken entsprechend akzeptablen Stand zu bringen.

Während viele Unternehmen heute noch mit ineffizienten Prozessen, Strukturen, internen Interessenkonflikten und dazu noch stark konservativen Denkweisen zu kämpfen haben, sind Cloud-Dienstleister daran, Innovationen in puncto Sicherheit weiter auszubauen. In so manchen Vergleichsfällen beantwortet sich die Frage «Wo sind meine Daten sicherer aufgehoben?» wohl von selbst. Technologisch und auch hinsichtlich der Motivation sind heute viele Cloud-Dienstleister auf der Überholspur, einige von ihnen sind schon längst weiter, was «State of the Art», «Effectivenes & Efficiency» und «Security & Compliance» betrifft.

Die Autoren
Marc Burkhard, CEO, ITSENSE

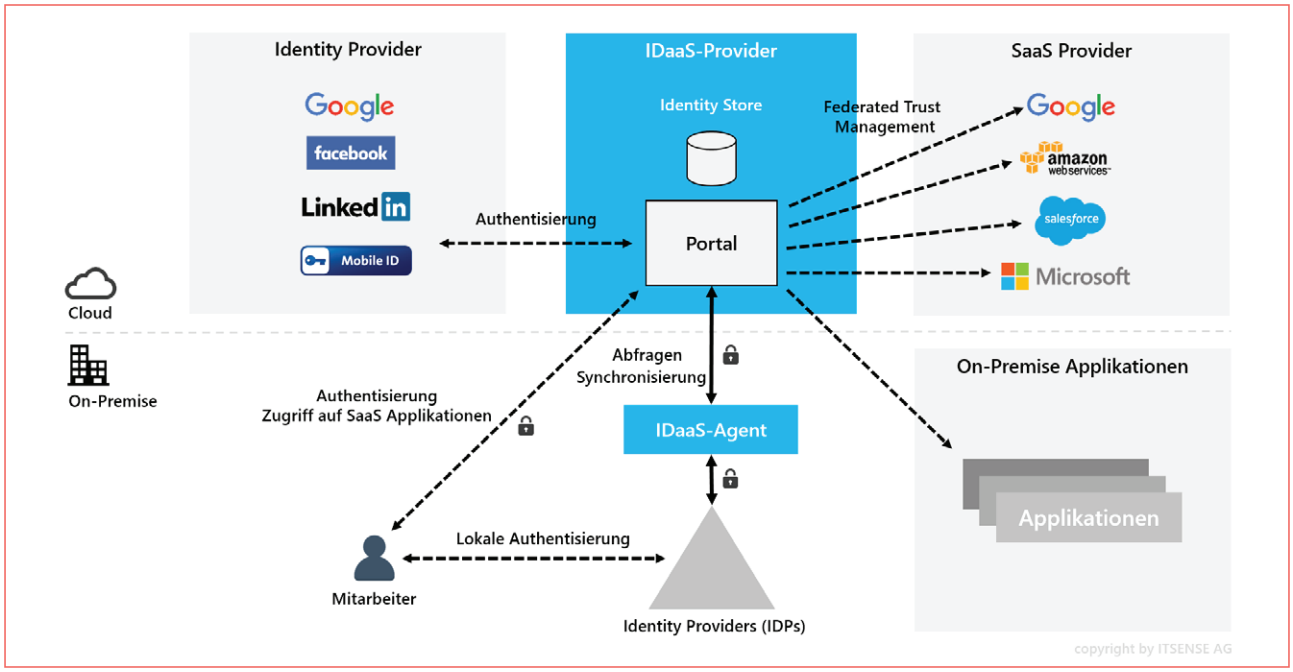
Orkan Yoksulabakan, Senior Security Expert, ITSENSE

Über ITSENSE
Die ITSENSE AG ist Expertin im Bereich IAM und bietet eine vollständig in der Schweiz entwickelte IAM-Lösung mit IDaaS Fähigkeiten an. Mehr Infos: coreone.ch

Man muss sogar damit rechnen, dass Cloud-Dienstleister durchaus den gleichen, wenn nicht sogar höheren Standard für Informationssicherheit und Datenschutz bieten, als dies in vielen Unternehmen der Fall ist. Es ist ergänzend zu erwähnen, dass europäische Bestimmungen zum Schutz personenbezogener Daten ungleich stärker sind als etwa jene in den USA. Dort wurde bis heute kein geeignetes Datenschutzgesetz verabschiedet. EU-Recht und schweizerisches Recht sind in den USA indes nicht relevant. Es empfiehlt sich daher grundsätzlich, einen in Europa ansässigen Federation-Provider zu wählen. In der Schweiz, Deutschland und Österreich besteht die Auskunfts-, Informations-, Löschungs- sowie Richtigstellungspflicht für personenbezogene Daten.

Abgesehen von den anfänglichen Schwächen, die sich Cloud-Dienstleister im Bereich der Sicherheit leisteten, haben diese bereits weit früher erkannt, dass die Sicherheit und die nachweisliche sowie nachhaltige Konformität wichtig für den Erfolg ihrer Dienste sind. Mittlerweile – und zum Glück für die Konsumenten – ziehen immer mehr Cloud-Dienstleister mit den markantesten und wichtigsten Sicherheitssiegeln wie die Sicherheitsnormen der Payment Card Industry (PCI), ISO/IEC, Finma oder ISAE zwecks Vertrauensgewinnung durch «Best Practices» in der Sicherheit nach. Das müssen diese Anbieter auch, denn nur so können sie gewährleisten, dass sie als seriöse und zuverlässige Partner wahrgenommen werden.

Gelänge es also tatsächlich, das Sicherheitsniveau von vertrauenswürdigen und nach bekannten Sicherheitsstandards zertifizierten Cloud-Dienstleistern mit dem eines typischen Schweizer KMUs zu vergleichen, so müssen sich in der Realität nicht die Unternehmen vor der Nutzung von Cloud-Diensten schützen, sondern vielfach vor sich selbst.



Sicherheit ist nicht alles

Sind die pauschal formulierten, sicherheitsbezogenen Vorurteile einmal aus dem Weg geräumt, so erkennt man, dass cloudbasierte Dienste weitere markante Vorteile bieten können, die über den Sicherheitsgedanken hinausgehen. Ein CEO hat in der Regel nicht die Sicherheit im Fokus, sondern sein Geschäft, dessen Erfolg sein Kernziel bleibt. Auch dann, wenn das Wort «Sicherheit» ein unverzichtbarer Teilaspekt zur Nachhaltigkeit und Vermeidung von möglichen Reputationen darstellt. Für die Industrie war Sicherheit noch nie gewinnbringend, doch sie ist stets verlustreduzierend. Daher bleibt sie weiterhin ein notwendiges Übel, denn sie ist monetär nicht spürbar, zumindest nicht für den CEO, dessen Kerngeschäft nicht die Sicherheit ist.

Aus Sicht des CEO ist die Sache ganz einfach: Die IT muss funktionieren und mit Funktionieren ist primär eine möglichst hohe Verfügbarkeit gemeint. So können Gewinne erzielt werden. Wie das erreicht wird, liegt im Verantwortungsbereich des CIO. Dieser wünscht sich eine schlanke IT-Organisation, die sich flexibel an die Anforderungen und Bedrohungen anpasst.

IAMaaS hat Zukunft

Mit dem Einsatz von IAMaaS erhalten Unternehmen die Möglichkeit, ihre Ressourcen zu bündeln und einem grösseren Benutzerkreis sicher zur Verfügung zu stellen. Dabei müssen für die Servicebereitstellung keine hohen Investitionen getätigt werden, und vorhandene On-Premise-IAM-Lösungen können integriert werden.

Die zunehmende Bedeutung von Cloud-Services und die Verbreitung von Authentisierungsdiensten sowie der zunehmende Bedarf an Informationssicherheit und Datenschutz unterstreichen die Bedeutung und Notwendigkeit eines strukturierten Identity- und Access-Managements.

Gemäss Gartner wird die Nutzung von auf IAMaaS basierenden Lösungen bis Ende 2017 einen Anteil von rund 20 Prozent erreichen.

MEHRWERT DURCH IAM-AS-A-SERVICE

- Die Installation, Konfiguration und der Betrieb des Federation-Providers werden von einem vertrauenswürdigen Cloud-Dienstleister angeboten und die Kosten für einen On-Premise-Aufbau reduziert.
- Zentrale Etablierung und Verwaltung der Vertrauensbeziehungen (Federated Trust Management) zum Cloud- und lokalen Identity-Provider.
- Die Provisionierung und De-Provisionierung von Identitäten kann durch vorhandene lokale IAM-Lösungen initiiert und unterstützt werden.
- Mittels Just-in-Time-Provisioning werden Benutzerkonten erst dann angelegt, wenn ein Nutzer auf die Anwendung zugreift. Das spart Kosten bei userbasierten Nutzungsgebühren.
- Der Zugriff auf Anwendungen kann global überwacht und gesteuert werden.
- Die zentrale Protokollierung stellt die Nachvollziehbarkeit sicher und bietet ein einfaches Auditing.
- Es kann mittels Virtual Directories eine globale Sicht auf die lokalen und cloudbasierten Identity Stores angeboten werden.
- Einmalige Integration der Multi-Faktor-Authentifizierung (MFA) im Portal anstatt in den jeweiligen Anwendungen.
- Der gewählte Federation-Provider stellt die hohe Verfügbarkeit des Dienstes sicher.
- Das System ist auch vor internen Administratoren ausreichend geschützt.