ipg AG
information process group
Jägerstrasse 2
CH-8406 Winterthur

Tel. +41 52 245 04 74
Fax +41 52 245 04 73
www.ipg-ag.com
info@ipg-ag.com

Fachbericht: Identity Management as a Service (IDaaS)

„IAM-Architektur der Zukunft oder nur Hype?“

Inhalt

ipg AG
information process group
Jägerstrasse 2
CH-8406 Winterthur

Tel. +41 52 245 04 74
Fax +41 52 245 04 73
www.ipg-ag.com
info@ipg-ag.com

1. Einführung: IAM goes Cloud-Computing

Cloud-Computing ist seit einigen Jahren aus dem Kontext der Informationstechnologie nicht mehr wegzudenken. Im Gegenteil: Cloud-Computing stellt einen Ansatz dar, der sich mit der dynamischen Bereitstellung von Plattform, Infrastruktur und Software in verschiedenen Ausprägungen befasst, und an die Bedürfnisse der Nutzer wie Endkunde oder Unternehmen angepasst wird. Cloud-Computing verspricht damit Potenziale für Verbesserung, Optimierung und Kosteneinsparung. Dass Identity & Access Management gerade in diesem Umfeld einen noch wichtigeren Stellenwert hat, wird mit dem Thema IDaaS (Identity Management as a Service) nur allzu deutlich. Die Details dazu legen wir im folgenden Bericht näher dar.

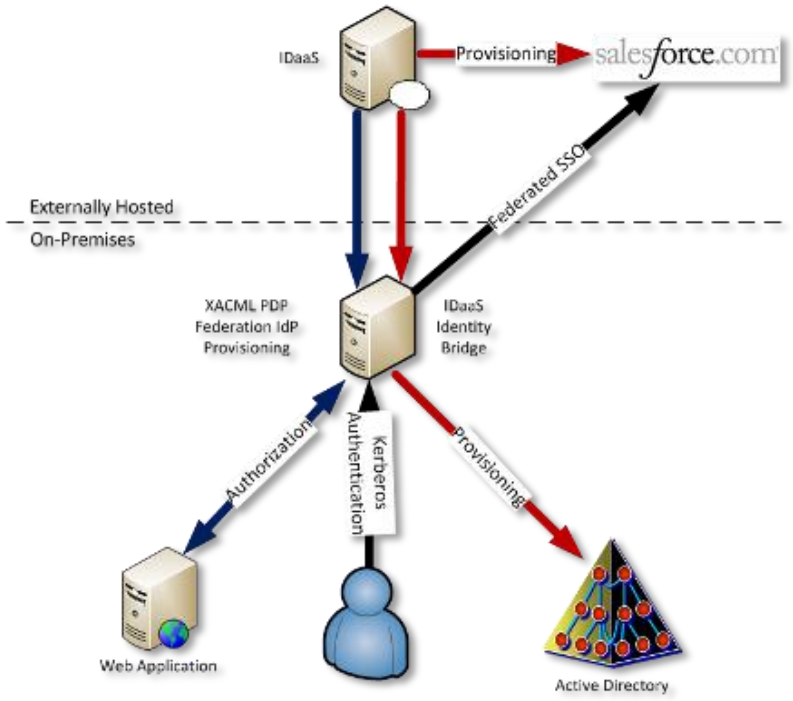

Abbildung 1: Verteilung der Identity-Management Funktionen [1]

Anhand eines Beispiels von Gartner Inc., Anbieter von Marktforschung und Analyse in der weltweiten Technologie-Industrie, wird IDaaS für die bekannte Cloud-Anwendung Salesforce.com eingesetzt. Benutzer werden in die Anwendung provisioniert; der Zugriff auf die Anwendung aus der Unternehmensinfrastruktur heraus erfolgt ebenso über die Integration mit dem IDaaS.

[1] Quelle Gartner

ipg AG
information process group
Jägerstrasse 2
CH-8406 Winterthur

Tel. +41 52 245 04 74
Fax +41 52 245 04 73
www.ipg-ag.com
info@ipg-ag.com

2. Ist die Zukunft für IAM in der Cloud schon da?

Beinahe in jeder Fachzeitschrift und sogar in Tageszeitungen sind Artikel und Kommentare darüber zu lesen; viele IT-Anbieter haben Cloud-Computing in ihre Wachstumsstrategie integriert und Unternehmen befassen sich zunehmend ernsthaft und intensiver mit diesem Thema. Klar ist: Cloud-Computing ist die wichtigste Innovation seit dem Mainframe- oder dem Client/Server-Modell und nutzt die Erfahrung aus diesen Ansätzen in Kombination mit der Internet-Technologie als Distributions-Plattform für IT-Dienstleistungen.

Abbildung 2: Von dem Mainframe bis zum Cloud-Computing[2]

Der Markt für Cloud-Computing jedenfalls entwickelt sich rasant und soll laut IDC ein jährliches Wachstum (Prognose bis 2014) von 30 % umfassen, das einem Umsatz von 16,5 Mrd. USD entspricht.

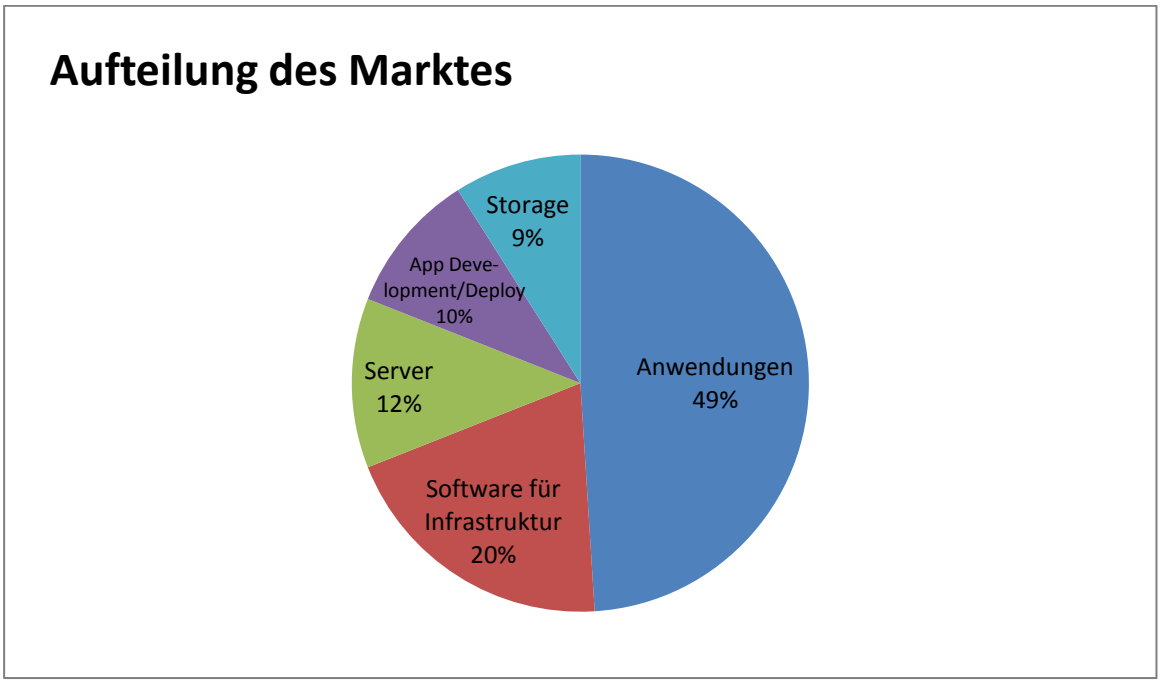

Abbildung 3: Aufteilung des Marktes für Cloud Computing nach IDC[3]

[2] Christian Metzger, Juan Villar 2011 - Cloud Computing, S.1

Durch diese Zahlen der Marktaufteilung kann man rückschliessen, dass sich Cloud-Computing einen sicheren Platz in der IT-Branche verschaffen könnte, wenn diese nicht sogar revolutioniert.

3. Identity Management zur korrekten Nutzung von Services, Systemen und Ressourcen

Identität und Management - daraus setzt sich der Begriff Identity Management zusammen. Die folgende Aussage definiert den Begriff Identität:

> *"…die Summe derjenigen Merkmale, anhand derer ein Individuum von anderen unterschieden werden kann."* [4]

Daher ist eine Identität als etwas Einzigartiges zu betrachten. Die Einzigartigkeit sichert die Unterscheidung zwischen den Individuen. Dies ist eine der Voraussetzungen, um Identity Management effektiv zu betreiben.

Unter anderem findet sich der Ursprung des Begriffes Management im lateinischen *„manus agere"* und hat die Bedeutung „an der Hand führen".[5] Identity Management lässt sich somit mit der Steuerung der Identität anhand deren Eigenschaften festlegen. Informationstechnologie und Prozesse sind weitere wesentliche Bestandteile von Identity Management. Zu den weiteren Aspekten im Identity Management gehören die Summe aller Massnahmen die notwendig sind, um Personen und Benutzer in IT-Systemen eindeutig zu erkennen sowie ihnen genau jene Zugriffe zu ermöglichen, die sie aktuell im Rahmen ihrer Tätigkeit benötigen. Dabei sind alle Massnahmen im Rahmen von standardisierten und nachvollziehbaren Prozessen durchzuführen.

Zusammengefasst ist Identity Management die bewusste Verwendung einer Identität, um die Nachvollziehbarkeit der Benutzung von Services, Systemen und Ressourcen - im Besonderen jene der Informationstechnologie - sicherzustellen. Damit wird gewährleistet, dass jeder Identität genau jene Ressourcen und Services zur Verfügung gestellt werden, die sie auch für ihre Tätigkeit im Unternehmen benötigt. Im Rahmen des Lebenszyklus einer Identität werden die Veränderungen einer Identität in Bezug auf die Ressourcen- und Services-Nutzung protokolliert. Somit ist im Sinne der IT-Compliance[6] jede Veränderung (Change) eindeutig - wie die Identität selbst - und nachvollziehbar und daher auch ebenso in einer Cloud-basierten Identity Management-Lösung realisierbar.

4. Cloud Computing und Services

Das *National Institute for Standards and Technology* (NIST) veröffentlichte 2009 eine Definition für Cloud Computing, die im Wesentlichen die Cloud Service Modelle und Liefermodelle beinhaltet[7]:

Cloud Computing („Rechenleistung aus der Wolke") verfolgt den Ansatz, abstrahierte IT-Infrastrukturen - wie z.B. Rechenkapazität, Datenspeicher (IaaS=*Infrastructure as a Service*), fertige Software (SaaS=*Software as a Service*) und Programmierumgebungen (Paas=*Plattform as a Service*) - dynamisch an den Bedarf

[3] Christian Metzger, Juan Villar 2011 - Cloud Computing, S.7
[4] Mezler-Andelberg 2008 – Identity Management, S.9
[5] Vgl. Wikipedia: Management, http://de.wikipedia.org/wiki/Management [Stand: 14. Februar 2012]
[6] Vgl. Wikipedia: IT-Compliance, http://de.wikipedia.org/wiki/IT-Compliance [Stand: 14. Februar 2012]
[7] Vgl. NIST Definition of Cloud Computing, http://www.slideshare.net/crossgov/nist-definition-of-cloud-computing-v15

angepasst über ein Netzwerk zur Verfügung zu stellen. Die dynamische Anpassung erfolgt in erster Linie über die Bündelung von Infrastrukturleistungen. Essentielle, charakteristische Bestandteile des Cloud-Computing sind in der folgenden Tabelle dargestellt:

On Demand Self-Service	• In Anspruchnahme eines Cloud-Services ohne menschliche Interaktion mit dem Service-Provider
Breitbandiger Netzwerkzugang	• Grundsätzliche Verfügbarkeit der Dienste über das Internet
Schnelle Elastizität	• Rasche und bedarfsgerechte Vergrösserung der IT-Services
Ressourcen-Pooling	• Die IT-Ressouren des Anbieters sind im Rahmen eines „Multi-Tenancy“-Modells dynamisch zur Verfügung gestellt
Messbare Services	• Messen, kontrollieren und optimieren von verwendeten Ressourcen

Neben den angeführten Cloud-Servicemodellen werden wir uns im folgenden Kapitel dem IDaaS (Identity Management as a Service) Servicemodell widmen, das in seiner Ausprägung ein SaaS ist, und primär für die Verwaltung, Provisionierung und Nachvollziehbarkeit des Lebenszyklus (Audit) von Identitäten implementiert und zur Verfügung gestellt wird.

5. IDaaS: Nutzen für den Dienstleister und Anwender

Der IDaaS ist ein Szenario, bei dem der Cloud-Provider die Identity Management Software in der Cloud-Infrastruktur implementiert hat und auf Basis eines SaaS dem nutzenden Unternehmen bereitstellt, so dass in letzter Konsequenz keine Investitionen für *On-Premise*-Anwendungen getätigt werden müssen. Auf Unternehmensseite ist daher der Aufbau von entsprechend ausgebildetem Fachpersonal, wie auch die laufende Betreuung des Systems und die kontinuierliche Anpassung der technischen Prozesse obsolet geworden. Trotzdem braucht es dennoch IAM-Experten natürlich auf Seiten der Cloud-Provider, die sich um die technisch fachgerechte Bereitstellung und laufende Betreuung der Services kümmert.

Das Management von Identitäten in der Cloud ist demnach als eine spezielle Form eines SaaS innerhalb der Cloud zu betrachten. Es ist für jede der drei Servicemodelle Plattform, Infrastruktur und Software sowie für die wichtigsten beiden Liefermodelle, die Private- und die Public-Cloud, geeignet und einsetzbar.

In der Fachwelt ist man sich darüber hinaus noch nicht ganz einig, welchen Funktionsumfang IDaaS umfasst oder umfassen wird. Bisher haben wir das Management von Identitäten betrachtet; in die gleiche Kerbe schlägt die CSA (Cloud Security Alliance) mit ihrer Definition:

> *„…IDaaS refers to the management of identities in the cloud, apart from the applications and providers that use them.“* [8]

[8] Vgl. CCSK-Guide: Defining IDaaS, http://ccskguide.org/2011/03/cloud-identity as a Service-idaas/ [Stand: 14. Februar 2012]

ipg AG
information process group
Jägerstrasse 2
CH-8406 Winterthur

Tel. +41 52 245 04 74
Fax +41 52 245 04 73
www.ipg-ag.com
info@ipg-ag.com

Ein weiterer Aspekt, der im Rahmen eines IDaaS freilich zu berücksichtigen sein wird, behandelt das Zugriffsmanagement auf die Cloud-Services. Dies kann durch Identity Federation (Federated Single Sign On) als eine der möglichen Optionen realisiert werden (siehe Kapitel 7.).

6. Vorteile von IDaaS

Wie bei allen anderen Servicemodellen auch, gibt es beim Identity Management in der Cloud erhebliche Vorteile beim Betreiben und Nutzen des vereinbarten Services. Grundsätzlich haben Unternehmen nur zwei Gründe sich für eine Cloud-Lösung zu entscheiden: *Kosten* und *Ressourcenbindung.*

Während die Investitionen und Betriebskosten für eine *On-Premise*-Lösung das Risiko des Betriebes nicht verringert, sind der Aufbau und die „Haltung" von Personal-Ressourcen, die über spezielles Wissen verfügen, als Risikopotenzial ebenso nicht von der Hand zu weisen. Letztendlich geht es immer um Kosten.

Das Outsourcing (oder Sourcing) ist als Möglichkeit Kosten zu sparen nicht neu. Dennoch muss man sich bewusst machen, dass neben dem Vorhalten von Hard- und Software, auch Backup- und Failover Szenarien, Planungsmechanismen für das Upgrade oder die Testfälle sowie kontinuierlich die technischen Prozesse im Auge zu behalten (KVP = *Kontinuierliche Verbesserungsprozesse*), gewichtige Gründe für den Weg in die Cloud sind.

Die Anzahl der Anbieter (ASP = *Application Service Provider*) von Cloud-Services wächst stetig. Die Kunden haben die Möglichkeit, Angebote zu vergleichen und sich für den besten Partner zu entscheiden. Da über einen ASP die Services über ein *Service Level Agreement* (SLA) mit sehr speziellen Parametern verhandelt wird, muss sich der Kunde, wie bei seinen *On-Premis*-Lösungen, nicht mit Details wie oben dargestellt auseinandersetzen. Durch den Wettbewerb ist der Cloud-Anbieter gezwungen, technologisch auf dem neusten Stand zu sein. Dies bietet auch dem Kunden einen weiteren positiven Aspekt, denn auch er muss seinerseits up-to-date auf den Markt reagieren. Für einen IDaaS ist eine *Multi-Tenancy*-Umgebung (Multiple Mandanten) unerlässlich. Viele Kunden nutzen in diesem Fall die gleiche Identity Management-Plattform auf unterschiedlich bereitgestellten Instanzen gemäss des vereinbarten Servicevertrages. Dynamische Veränderungen oder Anpassungen (siehe Kapitel 3.) an der Architektur (Upgrades, Release Wechsel, neue Funktionen) sowie auch an der Kundenkonfiguration liefern unterbrechungsfrei und rascher Ergebnisse als bisher bei *On-Premise*-Architekturen, die das Wartungsfenster z.B. am Wochenende alle sechs Wochen abwarten mussten.

Ein IDaaS kann vollständig in der Cloud als Private oder Public implementiert und bereitgestellt werden (natürlich auch andere Modelle, die wir aber hier nicht behandeln) und als Add-On für die drei Servicemodelle PaaS-, IaaS- und SaaS-Anwendung finden. Somit kann neben der Kerngeschäftsanwendung oder der Entwicklungsplattform ebenso das Management der Identitäten und auch die Verwaltung der Zugriffe derer auf die Anwendungen oder auf eine DIE (Entwicklungsumgebung) als Service bereitgestellt und genutzt werden.

7. Informationssicherheit und Datenschutz; zwei zentrale und bedeutende Themen

Seit der Kommerzialisierung der Internet-Technologie sind Überlegungen zur Sicherheit und zum Schutz der Daten ein essentieller Bestandteil jedes Informationssystems. Seit der Innovation des Cloud-Computing

ipg AG
information process group
Jägerstrasse 2
CH-8406 Winterthur

Tel. +41 52 245 04 74
Fax +41 52 245 04 73
www.ipg-ag.com
info@ipg-ag.com

aber führen Experten kontroverse Diskussionen zu diesem Thema. Informationssicherheit ist nicht gleich Datenschutz. Während Informationssicherheit die Vertraulichkeit, Verfügbarkeit und Integrität sicherstellt[9], behandelt der Datenschutz den Schutz personenbezogener Daten auf deren missbräuchliche Verwendung[10]. Daher kann man davon ausgehen, dass die Cloud-Anbieter mit ihren Rechenzentren und ihren Partnern für IDaaS durchaus den gleichen, wenn nicht sogar höheren Standard für Informationssicherheit bieten, als dies bei *On-Premise*-Anwendungen der Fall ist.

Beim Datenschutz ist grundsätzlich nationales Recht anzuwenden, d.h. die jeweiligen Kunden und die Cloud-Anbieter müssen die gesetzlichen Bestimmungen des Landes einhalten, in dem auch die Daten gespeichert sind. Jedoch soll, gemäss der Europäischen Datenschutzrichtlinie (EU-DSRL), aber innerhalb des europäischen Binnenmarktes der Umstand einer grenzüberschreitenden Datenverarbeitung kein rechtliches Hindernis mehr darstellen[11]. Europäische Bestimmungen zum Schutz personenbezogener Daten sind ungleich stärker als jene in den USA, die bis heute noch kein geeignetes Datenschutzgesetz verabschiedet haben. Das ist auch der Grund warum sich europäische Unternehmen scheuen, ihre Daten in einer US-amerikanische Cloud zu speichern; EU- und Schweizer-Recht sind in den USA belanglos[12]. In der Schweiz, Deutschland und Österreich besteht die Auskunfts-, Informations-, Löschungs- sowie Richtigstellungspflicht für personenbezogene Daten.

8. Dienstleistungen im Umfeld von IDaaS

Die Benutzerverwaltung

Viele Unternehmen haben Kunden und Partner, die mit ihnen kooperieren möchten und Zugriff auf Onlineportale benötigen. IDaaS lässt sich in diese Anwendungen integrieren und kann auf diese Weise cloudbasierte Funktionen für die Identitätsverwaltung wie Benutzer-Self-Service, Profilerstellung, Passwortzurücksetzung und Verteilung vergessener Benutzernamen bereitstellen.

Die Benutzerprovisionierung

IDaaS automatisiert die Vorgänge zum Hinzufügen, Ändern und Löschen von Benutzerkonten einschliesslich der Benutzerattribute und Rollenverknüpfungen, die für die Zuweisung von Berechtigungen für Zielsysteme verwendet werden können. Der Service kann gleichermassen für die Kontoprovisionierung für cloudbasierte und für *On-Premise*-Anwendungen bzw. bei hybriden Modellen für beide Typen verwendet werden.

Die Bereitstellungsverwaltung und Self-Services

Wenn Benutzer Zugriff auf Unternehmensanwendungen benötigen, wenden sie sich dafür häufig direkt an die IT oder den Help-Desk. Das ist oft teuer und ineffizient. IDaaS bietet Benutzern die Möglichkeit, solche Anforderungen online zu senden. Der Cloud-Service leitet die Anforderungen dann anhand definierter

[9] Vgl. Wikipedia: Informationssicherheit, http://de.wikipedia.org/wiki/Informationssicherheit [Stand: 15.Februar 2012]

[10] Vgl. Wikipedia: Datenschutz, http://de.wikipedia.org/wiki/Datenschutz [Stand: 15.Februar 2012]

[11] Quelle: https://www.datenschutzzentrum.de/cloud-computing/

[12] Vgl. SearchSecurity.de: Datenschutzgesetz, http://www.searchsecurity.de/themenbereiche/sicherheits-management/compliance/articles/281960/ [Stand: 16.Sept. 2010]

ipg AG
information process group
Jägerstrasse 2
CH-8406 Winterthur

Tel. +41 52 245 04 74
Fax +41 52 245 04 73
www.ipg-ag.com
info@ipg-ag.com

Richtlinien durch den Genehmigungsworkflow und kann den Benutzer gegebenenfalls automatisch für diese Systeme provisionieren.

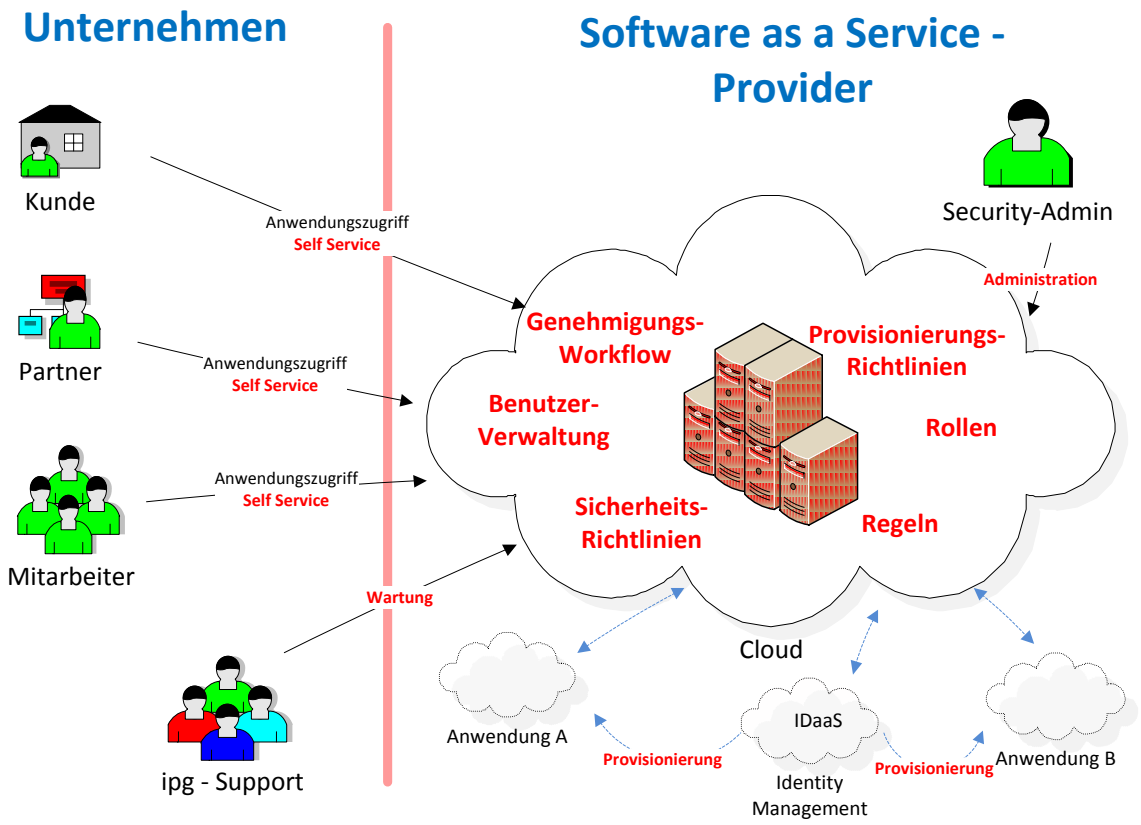

Abbildung 4: Konzeptionelle Architektur IDaaS - Identity Management[13]

Zugriffsmanagement und Single Sign On

Die Identitäten wurden in die Cloud-Anwendungen provisioniert und über Richtlinien der entsprechende Zugriff erteilt. Der sichere Zugriff auf die Cloud-Services durch Identity Federation und auch Federated Single Sign On erfolgt durch die Implementation des Service-Providers (SP) in der Cloud; der Identity Provider (IdP) als *On-Premise*-Implementation sorgt für die Authentisierung des Benutzers und Übermittlung der Benutzerdaten (ohne Passwort) an den Service-Provider in der Cloud.

Der in Abbildung 4. dargestellte Ansatz beschreibt die standardisierte Methode Identity Federation mittels SAML (Security Assertion Markup Language) zu implementieren. SAML ist ein XML-basierter Kommunikationsmechanismus zum Austausch von Benutzerdaten zwischen unterschiedlichen Organisationen (hier Unternehmen und SaaS-Provider).

[13] Quelle: ipg AG (Stand 2012)

ipg AG
information process group
Jägerstrasse 2
CH-8406 Winterthur

Tel. +41 52 245 04 74
Fax +41 52 245 04 73
www.ipg-ag.com
info@ipg-ag.com

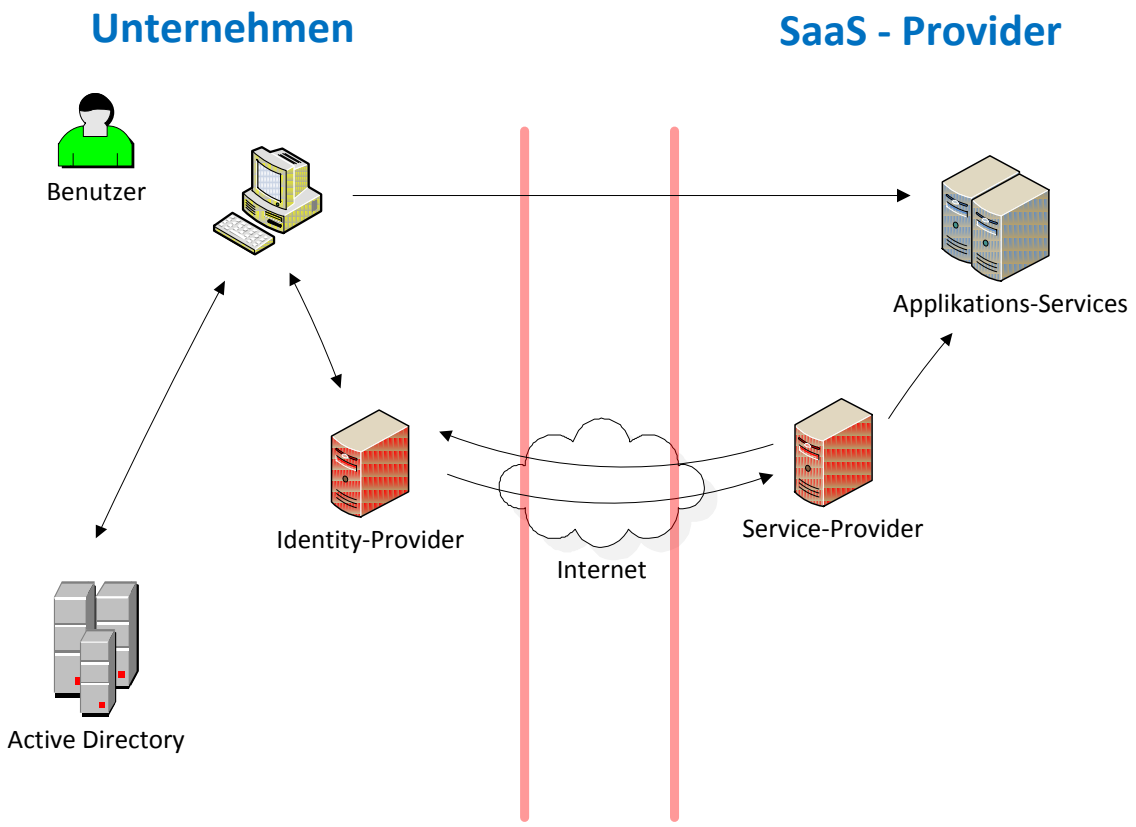

Abbildung 5: Konzeptionelle Architektur IDaaS - Identity Federation[14]

Der Benutzer stellt einen Request an den Service-Provider durch Klicken eines Links auf dem Unternehmensportal. Der Identity-Provider authentisiert den Benutzer und erzeugt ein verschlüsseltes XML-basiertes Informationspaket (SAML Assertion) und sendet dieses an den Service-Provider. Der IdP und SP stehen in einer Geschäftsbeziehung zueinander, daher erfolgt der Informationsaustausch. Der Service-Provider öffnet die SAML Assertion und erzeugt eine gültige Session für den Benutzer, der den zuvor aufgerufenen Service benutzen kann. Ist die Sitzungsinformation gültig, darf der Benutzer Anwendungen im gleichen Kontext benutzen, ohne sich nochmals anzumelden (Single Sign On).

Vordefinierte Prozesse im Rahmen der Vereinbarung zwischen Dienstleister (Service-Provider) und dem nutzenden Unternehmen sind das Regelwerk, über die sich die Services für die IAM-Infrastruktur steuern lassen.

Ob nun ein neuer Mitarbeiter Zugriff auf die für ihn relevanten Anwendungen benötig Berechtigungen bestellen möchte oder einfach nur das Passwort zurücksetzen will; ein Administrator eine neue Anwendung in den Anwendungsverbund integrieren muss: All diese Vorgänge sind in Dienstleistungen verpackt und entsprechend der Anforderungen des nutzenden Unternehmens definiert.

Änderungen am Dienstleistungs-Umfang sind jederzeit möglich und unabhängig von der Unternehmens-Infrastruktur und somit auch rascher und zielgerechter umgesetzt.

[14] Quelle: ipg AG (Stand 2012)

ipg AG
information process group
Jägerstrasse 2
CH-8406 Winterthur

Tel. +41 52 245 04 74
Fax +41 52 245 04 73
www.ipg-ag.com
info@ipg-ag.com

9. ipg`s IAM as a Service - Expertenwissen und Projekterfahrung

Wachsende Zahlen von Benutzern sowie Systemen auf die diese zugreifen müssen, zieht die Explosion digitaler Identitäten nach sich, die verwaltet werden müssen. Die Identitätsverwaltung über den gesamten Lebenszyklus beinhaltet eine Vielzahl von Aspekten wie die Kontoerstellung, die Zuweisung von Zugriffsrechten, die Verarbeitung von Zugriffsanforderungen und die Verwaltung zugehöriger Identitätsattribute. Unternehmen benötigen eine Lösung, die ihnen die zentrale Zusammenführung und Kontrolle von Identitäten für die gesamte IT- und Cloud-Umgebung erlaubt - und das liefert ipg`s IAM as a Service als Ausprägung eines IDaaS:

- ipg AG konzipiert, baut und betreibt IAM-Infrastrukturen zentral oder dezentral
- Mit hochwertigen Dienstleistungen schafft ipg AG eine nachhaltige Kundenzufriedenheit und realisiert Lösungen nach gängigen Best-Practice-Ansätzen
- Die Mitarbeiter von ipg AG übernehmen den Betrieb und den Weiterausbau der Kunden-IAM-Organisation

Abbildung 6: ipg`s IAM as a Service stack[15]

Im Rahmen des IAMaaS Consulting-Portfolios bietet IPG AG einen ganzheitlichen Ansatz als kompetenter Partner für „Ihren“ Weg in die Cloud. Wir beraten, stellen den Reifegrad der IT fest, definieren die geschäftlichen sowie technischen Anforderungen an die IT und unterstützen mit folgenden Consulting Leistungen:

- Erarbeiten von unternehmensspezifischen Architekturen und Lösungskonzepten für Federated Identity Management (FIM)
- Erstellen von Sicherheitskonzepten und -Richtlinien für die Nutzung von IAMaaS
- Einbinden von Identity & Access Management Services in die Unternehmens-IT

[15] Quelle: ipg AG (Stand 2012)

ipg AG
information process group
Jägerstrasse 2
CH-8406 Winterthur

Tel. +41 52 245 04 74
Fax +41 52 245 04 73
www.ipg-ag.com
info@ipg-ag.com

- Implementieren von Identity & Access Management Software „as a Service“; für alle Themen der Access Governance wie Rollenmodellierung (Role-Mining), Attestation (Berechtigungsprüfung, Re-Zertifizierung) oder SoD-Kontrollen (Segregation of Duties = Funktionstrennung)

- Cloud Authentication Services

10. Fazit

Der IDaaS ist längst als spezielle Ausprägung eines Software as a Service Servicemodells am Markt angekommen und birgt grosses Potenzial, nachhaltig Ressourcen- sowie Kosteneinsparungen vorzunehmen. Dank der Flexibilität der unterschiedlichen Liefermodelle in Bezug auf die Kombinierbarkeit mit den durch die Jahre gewachsenen *On-Premise*-Architekturen, ist eine schrittweise Transformation nicht nur empfohlen sondern auch ein logischer Schritt.

Mit ipg AG und ihrem IAM as a Service-Lösungsportfolio bietet ein unabhängiger Partner mit umfangreichem Know-How der wichtigsten Industriestandards und Anbieter für IAM-Dienstleistungen, die entsprechenden Bausteine für diesen Weg in die Cloud an.