DER WEG ZUR ENTERPRISE-CLOUD

Prof. Dr. Andreas Heberle, Prof. Dr. Rainer Neumann
Fakultät für Informatik und Wirtschaftsinformatik
Hochschule Karlsruhe – Technik und Wirtschaft
Moltkestr. 30, 76133 Karlsruhe, Deutschland
Email: Andreas.Heberle@hs-karlsruhe.de, Rainer.Neumann@hs-karlsruhe.de

STICHWORTE

Cloud Services, Web-Services, Identity Management, Prozessmanagement, Service-Orientierte Architektur, Enterprise Integration.

KURZFASSUNG

Ein großer Teil der heute entstehenden innovativen Software erscheint als Online-Dienst im Web – sei es als hochinteraktive Web-Anwendung, oder als Backend-Dienst für kleine Anwendungen wie mobile Apps oder übliche Client-Anwendungen. Unternehmen können sich durch die effektive Nutzung dieser Dienste Vorteile verschaffen, die sich entweder in reduzierten Kosten (TCO) oder in effizienteren Prozessen zeigen.

Voraussetzung hierfür ist ein klares Verständnis der notwendigen Aufgaben und der mit der Nutzung verbundenen Probleme. Diese lassen sich in drei Gruppen einteilen: Zugang zu Cloud-Diensten, Schutz der Daten in der Cloud und Integration verschiedener Cloud-Dienste zu sinnvollen und effektiven Prozessen.

Dieser Beitrag beschreibt die Aufgaben und Fragestellungen und gibt Hinweise, wie die Vielzahl verschiedener Dienste in einem Unternehmen zu einer virtuellen Enterprise-Cloud zusammengestellt werden kann: Wie können Zugänge zu Cloud-Diensten effektiv verwaltet werden? Welche Aspekte sind bei der Bereitstellung von Daten in der Cloud zu beachten? Wie sind Abläufe über mehrere Dienstumgebungen sinnvoll möglich?

EINLEITUNG

Das Thema Cloud Computing ist in aller Munde. Technische Plattformen von unterschiedlichen Anbietern (u.a. von Amazon, Google, Microsoft) sind entstanden und haben ihre Kinderkrankheiten überwunden. Im Moment entsteht ein neuer Markt für Software-as-a-Service (SaaS). Dienste werden über das Internet bereitgestellt und Kunden haben schon bzw. werden zukünftig die Auswahl haben, wessen Dienst sie zu der Lösung einer fachlichen oder organisatorischen Aufgabe verwenden wollen. Damit werden Dienste und Dienstanbieter austauschbar.

Auf der anderen Seite, haben Unternehmen existierende Prozesse und besitzen Software und Infrastruktur, die diese Prozesse automatisiert oder unterstützt. Zusätzlich haben die Unternehmen natürlich auch bestimmte Anforderungen sowohl an ihre Software, als auch an den Betrieb der Software. Hier erfordert die Nutzung von Cloud Computing doch einige Anpassungen. Während früher die Prozesse „innerhalb der Burg“ hinter Firewall und unter voller Kontrolle des Unternehmens abliefen, sollen nun externe Dienste eingebunden werden.

Die spannende Frage ist, wie passen die beiden Welten zusammen und wie kann dieser Markt an Diensten von Unternehmen so genutzt werden, dass sie auf der einen Seite profitieren, alle Anforderungen an Sicherheit und spezifische Eigenschaften ihres Business erfüllt sind und die Integration mit der existierenden Anwendungslandschaft sichergestellt ist, um getätigte Investitionen zu sichern.

Das Thema Sicherheit wird in Bezug auf die Verwendung von Cloud-Diensten immer als erstes Hindernis genannt. Das ist sicher berechtigt, aber man muss als Unternehmen schon genau analysieren, wo man tatsächlich ein Sicherheitsproblem hat und in welchen Punkten die Cloud vielleicht sogar „sicherer“ ist. Offensichtlich ist der Schutz von z.B. Kundendaten problematisch, aber welches kleinere oder mittelständische Unternehmen kann schon mit Sicherheit sagen, dass es seine Dienste sicherer betreibt als ein großer Anbieter, der das für viele Kunden macht. Weitere wichtige Fragen entstehen bezüglich Identity and Access Management sowie der Integration von Cloud-Diensten zur Automatisierung von Geschäftsprozessen.

In dieser Arbeit beleuchten wir die Nutzung von Cloud-Diensten in Unternehmen. Wir definieren unsere Sicht auf zukünftige Enterprise Clouds, diskutieren Herausforderungen und gehen auf Lösungsansätze ein.

GRUNDLAGEN

Hinter dem Begriff Cloud Computing verbirgt sich das Bereitstellen von IT-Infrastrukturen und Diensten über das Internet. Dabei stellen Anbieter den Nutzern dynamisch skalierbare verteilte Infrastrukturen (Hardware und Software) auf Abruf zur Verfügung, die entsprechend der Nutzung abgerechnet werden.

Es lassen sich vier Arten von Clouds unterscheiden. In einer *Public Cloud* stellt ein Anbieter seine Dienste mehreren Nutzern öffentlich zur Verfügung. Anbieter sind hier z.B. Amazon, Google oder Microsoft. *Private Clouds* befinden sich innerhalb eines Unternehmens, das damit auch volle Kontrolle über Daten und Zugriff auf Dienste hat. Man spricht über eine *Hybrid Cloud*, wenn ein Unternehmen eine Private Cloud besitzt und eine Public Cloud benutzt, um z.B. Lastspitzen auszugleichen oder sicherheitsunkritische Funktionalitäten von extern zu beziehen. In einer *Community Cloud* schließen sich Unternehmen derselben Branche zusammen und machen ihre Private Clouds nur den Mitgliedern der Community zugänglich.

Für Clouds gibt es unterschiedliche Servicemodelle, die auf einander aufbauen. *Infrastructure as a Service (IaaS)* stellt Speicherplatz, Rechenkapazität, Server, Switches usw. dem Kunden zur Verfügung. Bei *Platform as a Service (PaaS)* stellt ein Anbieter neben Infrastruktur auch Software inklusive Lizenzen, Wartung und Support bereit. Eigene Anwendungen können damit komplett in der Cloud entwickelt werden. Bei *Software as a Service (SaaS)* wird Software angeboten, z.B. Office-Lösungen, aber auch komplette CRM-Systeme, die über das Internet benutzt werden kann.

Die Vorteile für Unternehmen bei der Cloud-Nutzung sind vielfältig. Eine Cloud erlaubt die bedarfsgesteuerte Bereitstellung von Rechen- und Speicherkapazitäten, ohne selbst die Infrastruktur für Lastspitzen zu betreiben. Bezahlt wird nach Nutzung der Dienste. Außerdem muss sich ein Unternehmen nicht um die Wartung installierter Software sowie den Schutz vor z.B. Viren kümmern. Damit realisieren Unternehmen vor allem Kostenvorteile und können die eigene IT vereinfachen.

SaaS-Anbieter decken heute schon die meisten Anwendungsbereiche von Unternehmen ab. Das Angebot an Diensten kann in drei Kategorien unterteilt werden (siehe [KKLS12]):

- klassische Anwendungsgebiete wie z.B. Dokumentenmanagement, E-Procurement oder Marketing,
- Teilgebiete von Anwendungsbereichen wie z.B. Reisekostenabrechnung oder Web-Conferencing
- Branchenlösungen z.B. für Logistikunternehmen oder Steuerberater.

Die Anbieter sind vielfältig. Einer der Markführer ist Salesforce.com, das mittlerweile über 100000 Kunden hat[1]. Auch der Markt in Deutschland wächst. Zum Beispiel listet der SaaS-Lösungskatalog des SaaS-Forums 237 SaaS-Anbieter ([SaaS11]).

Technisch betrachtet werden diese Dienste auf unterschiedliche Arten angeboten: In der einfachsten Form sind sie nur über eine web-basierte Benutzeroberfläche zugänglich. Typischerweise stellen die Anbieter die Dienste zusätzlich als Web-Services entweder auf Basis von SOAP[2] und WSDL[3] (siehe [Papa07]), oder nach dem etwas einfacheren REST-Architekturstil (siehe [Fiel00]) zur Verfügung. Mobile Mini-Anwendungen (Apps), wie sie heute für die erfolgreichen Cloud-Anwendungen fast unumgänglich sind, benötigen genau diese Schnittstellen.

Das Vorhandensein solcher programmatisch nutzbarer Schnittstellen ermöglicht die Abbildung von Geschäftsprozessen auf Basis der Cloud-Dienste und lässt damit die Vision der Service-Orientierten Entwicklung greifbar werden – Organisationen könnten effizient Funktionalitäten aus der Cloud nutzen und zu sinnvollen Abläufen (Workflows) zusammenschalten.

DER WEG ZUR ENTERPRISE CLOUD

Der Markt für Dienste aus der Cloud entwickelt sich stark. Inzwischen gibt es vielfältige Dienste und Lösungen aus der Cloud, vom einfachen E-Mail-Dienst über Kommunikationsinfrastruktur bis hin zur Komplettlösung. Unternehmen haben damit die Möglichkeit ihre Fertigungstiefe bezüglich Software zu verringern, Best-of-Breed oder Standardsoftware aus der Cloud zu konsumieren und sich bei der Entwicklung eigener Software auf geschäftskritische Funktionalitäten und Kernprozesse zu konzentrieren.

Für die Nutzung sind unterschiedliche Szenarien möglich. Entweder kauft ein Unternehmen Komplettlösungen bei Anbietern, wie z.B. SAP mit BusinessByDesign oder die CRM-Suite von Salesforce. Oder es kauft einzelne Dienste, um Lücken im existierenden Software-Portfolio zu schließen bzw. um kostenintensive, selbst betriebene Software abzulösen.

Ein Problem mit Cloud-Diensten ist, dass es wenig Standardisierung gibt und die Dienste in die existierende Landschaft eingebunden werden müssen. Dafür benötigt ein Unternehmen eine geeignete technische Architektur und Infrastruktur, die die Integration einfach möglich macht. Weitere Optionen ergeben sich, wenn ein Unternehmen eine Private Cloud betreibt, um Sicherheitsprobleme zu umgehen, und zusätzlich Dienste aus Public Clouds nutzt.

---

[1] http://www.salesforce.com/de/customers/
[2] http://www.w3.org/TR/soap/
[3] http://www.w3.org/TR/wsdl

Abbildung 1: Schritte auf dem Weg zur Enterprise Cloud

Ein Unternehmen auf dem Weg in die Enterprise Cloud muss folgende Fragen klären bzw. folgende Schritte (siehe Abbildung 1) ausführen:

1. **Identifikation und Auswahl potenzieller Dienste**

   Hierbei geht es um die Frage, welche Dienste aus der Cloud funktionale Lücken der bestehenden Softwarelandschaft schließen. Dieser Schritt sollte also mit einer Schwachstellenanalyse im Haus beginnen.

   Bei der Auswahl der Dienste muss sich ein Unternehmen überlegen, wie stark es sich an den Anbieter bindet – ist dieser in einer wirtschaftlich ausreichend stabilen Situation und passen die gesetzlichen Rahmenbedingungen zur Nutzung? Gerade der letzte Punkt ist in Hinblick auf vertragliche Regelungen und Datensicherheit bzw. Datenschutz von großer Bedeutung.

2. **Wirtschaftlichkeitsanalyse**

   Die Abrechnungsmodelle in der Cloud variieren sehr stark – Benutzerbezogene Modelle werden oftmals mit Datentransfervolumina und Speicherkapazitäten gemischt – ein objektiver Vergleich verschiedener Anbieter fällt hier schwer, sollte aber gerade deshalb sorgfältig durchgeführt werden. Insbesondere für die Faktoren Verfügbarkeit, Leistung und Skalierbarkeit müssen vorab geeignete Erwartungswerte definiert werden.

3. **Technische Erschließung der Dienste**

   Auf technischer Seite muss geklärt werden, wie sich die Cloud-Services in die eigene Infrastruktur integrieren lassen. Im einfachsten Fall ist dies die Nutzung von Web-Seiten des Anbieters, etwas aufwändiger ist die Integration in automatisierte Abläufe. In jedem Fall muss jedoch der Zugang zu den Diensten und das damit verbundene Identity und Access Management erstellt werden.

4. **Kontrollierte Cloud-Nutzung**

   Die Nutzung von Cloud-Diensten muss aus Unternehmenssicht dahingehend überwacht werden, dass eine Bewertung der tatsächlichen Nutzungsanforderungen erfolgen kann: Sind die vertraglichen Rahmenbedingungen eingehalten? Passen die angefallenen Kosten zu den in Anspruch genommenen Leistungen?

Ein Unternehmen begegnet bei diesen Schritten schiedlichen Herausforderungen, auf die wir im den eingehen werden.

HERAUSFORDERUNGEN FÜR UNTERNEHMEN

Neben dem Thema Sicherheit, das Verantwortlichen als erstes in den Sinn kommt, geht es bei der Nutzung von Cloud-Diensten auch um die Frage, wie man den Zugriff auf Cloud-Dienste kosteneffizient und sicher gestalten kann. Außerdem müssen die externen Dienste so integriert werden, dass die Prozesse geeignet unterstützt werden.

Sicherheit

Bei der Diskussion von Sicherheitsfragen in der Cloud muss man unterscheiden zwischen Problemen, die man allgemein in Netzwerken und mit der eigenen IT-Infrastruktur hat, und zwischen Cloud-spezifischen Bedrohungen.

Zu den gemeinsamen Bedrohungen gehören u.a. sichere Übertragung von Informationen, Distributed-Denial-of-Service Attacken, bedrohliche Insider, Account und Service Hijacking ([ClSA10]) und natürlich auch technische Pannen, die zu Systemausfällen führen können. Diese Probleme hat man sowohl mit internen Systemen (sofern sie nicht vollkommen abgeschottet sind) als auch in Kombination mit Cloud-Diensten. Allerdings kann man davon ausgehen, dass Cloud-Anbieter erkannte Schwachstellen schneller erkennen und schließen werden.

Die Nutzung von Cloud-Diensten führt dazu, dass Software und Daten, die bisher durch Firewall, DMZ und andere Sicherheitsmechanismen geschützt waren, nun außerhalb liegen. Damit stehen Nutzer und potentielle Angreifer auf einer Stufe.

Datensicherheit

Datensicherheit hat mehrere Aspekte: sicherer Zugriff auf die Daten, sichere Übertragung sowie sichere Verarbeitung und Lagerung der Daten. Die Datenübertragung in und aus der Cloud wird über sichere Protokolle und Kanäle durchgeführt. Die Kontrolle des Zugriffs auf Daten hängt an der Umsetzung von Rollen und Berechtigungskonzepten.

Bei der Lagerung von Daten kann man unter Sicherheitsgesichtspunkten erwarten, dass die Daten verschlüsselt abgelegt werden. Die Verarbeitung von Daten ist kritisch, da die meisten Ansätze unverschlüsselte Daten für die Verarbeitung erwarten. Den Problemen wird unterschiedliche begegnet:

- Unternehmen lagern nur unkritische Daten in die Cloud aus, geschäftskritische und wertvolle Daten werden intern verwaltet und bearbeitet.
- Sensible Daten werden verschlüsselt und verteilt abgelegt. Hier gibt es unterschiedliche Ansätze. Zum Beispiel wird bei MimoSecco – Middleware for Mobile and Secure Cloud Computing ([Mimo12]) Sicherheit unter Verwendung von Hardware-Tokens verbessert. OmniCloud ([Frau12a]) ermöglicht per Software die sichere Verwendung von Cloud-Storage Diensten und bietet auch einen Umzugsservice, damit man nicht von einem Anbieter abhängig ist.
- Mittels Homomorphic Encryption ([LaNV11]) können Berechnungen direkt auf den verschlüsselten Daten durchgeführt werden. Nur der Besitzer der Daten kennt den Schlüssel. Der Cloud-Anbieter, der mit den Daten rechnet, kennt die entschlüsselten Daten dabei nicht.

Eine aktuelle Studie des Fraunhofer SIT besagt, dass die Cloud-Anbieter die Frage nach Sicherheit sehr ernst nehmen, aber Probleme mit der durchgängigen Umsetzung haben [Frau12b]. Hier besteht also noch Verbesserungsbedarf.

Vertrauenswürdigkeit der Cloud-Anbieter

Die Verwendung von Cloud-Diensten setzt voraus, dass der Anbieter vertrauenswürdig ist. Der erste Schritt ist, dass Anbieter und Nutzer eine Vertragsbeziehung eingehen und Service Levels vereinbaren.

Zusätzlich gibt es Standards, die für Cloud-Anbieter relevant sind, z.B. ISO/IEC 27001 für Netzwerksicherheit. Außerdem sind Zertifizierungsprogramme entwickelt worden. Z.B. hat der Verband der deutschen Cloud Computing-Industrie das EuroCloud Star Audit Certificate für SaaS entwickelt ([EuDe11]). Allerdings müssen sich die Zertifikate erst noch bewähren.

Operationale Sicherheit

Für den Kunden ist die Dienstqualität, Verfügbarkeit, Performance etc., die ein Cloud-Anbieter zusichert wichtig, da unter Umständen Geschäftsprozesse nicht ablaufen können, wenn ein Dienst nicht verfügbar ist. Die Abmachung und vertragliche Zusicherung von Service Level Agreements ist daher essentiell.

Wichtig ist außerdem die Zuverlässigkeit und wirtschaftliche Situation des Anbieters. Hier stellen sich die Fragen was würde z.B. mit den Daten passieren, wenn der Anbieter den Betrieb einstellt oder eine Katastrophe ein Rechenzentrum des Anbieters lahmlegt. Zusätzlich muss geklärt sein, ob und wie Daten bei einem Anbieterwechsel umgezogen werden können.

Für den Kunden ist Transparenz zu Verbrauch und Kosten inklusive einem entsprechenden Reporting wünschenswert. Die einzelnen Anbieter stellen zwar Reportingfunktionalität zur Verfügung, aber diese ist über die Anbieter hinweg nicht standardisiert, so dass in einem Multi-Cloud-Szenario zusätzliche Integrationsaufwände anfallen.

Rechtssicherheit

Grundsätzlich gehen Anbieter und Abnehmer eine Vertragsbeziehung ein. Das Vertrauen ergibt sich aus dem Vertrag. Allerdings gibt es in den unterschiedlichen Ländern rechtliche Unterschiede, so dass der Gerichtsstand bei Streitigkeiten relevant ist. Außerdem unterscheiden sich die Auflagen bzgl. Vorratsdatenspeicherung und Aufbewahrungsfristen.

Zum Beispiel müssen in Deutschland Rechnungen für 30 Jahre aufbewahrt werden. Der Service-Anbieter muss das dann auch garantieren. Kritisch ist auch das Thema Datenschutz. Deutschland hat z.B. ein sehr viel restriktiveres Datenschutzgesetz als die USA. Vor allem der USA Patriots Act [USCo01] ist für deutsche Firmen kritisch.

Auch wenn die Daten eines amerikanischen Service-Anbieters außerhalb der USA lagern, dann können US-Behörden Zugriff auf diese Daten erlangen [Sawa11]. Im Moment sind bzgl. Datenschutz unterschiedliche Reformbemühungen und Gesetzesanpassungen im Gange, z.B. [Euro11].

Identity & Access Management

Ein Unternehmen hat üblicherweise eine Benutzerverwaltung inklusive existierender Rollen und Berechtigungen im Einsatz. Dort werden neue Mitarbeiter mit der zur Job-Beschreibung passenden Rollen eingetragen oder bei Austritt aus der Firma gelöscht. Hier kommen in Firmen Werkzeuge wie ein LDAP Directory oder z.B.

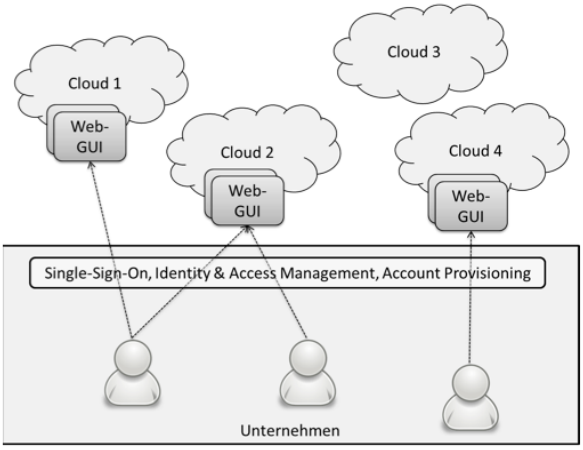

Abbildung 2: Identity & Access Management

Active Directory von Microsoft zum Einsatz. Werden externe Dienste eingesetzt, dann müssen Benutzer und Rollen des Dienstes mit existierenden Benutzerstrukturen verbunden werden. Abbildung 2 veranschaulicht die Aufgaben des Identity & Access Managements.

Single-Sign-On

Benutzt man Dienste mit Geschäftsbezug, dann erfordert das üblicherweise ein Login des Anwenders. Allerdings soll ein Anwender sich genau einmal am System anmelden müssen, auch wenn im Hintergrund unterschiedliche Dienste mit eigenen Logins zum Einsatz kommen. Hierfür gibt es unterschiedliche Single-Sign-On Lösungen. Im Falle von Web-Anwendungen wird oftmals wird die einfachste Variante des automatischen Ausfüllens von Formulardaten durch den Browser genutzt. Innerhalb der Microsoft Systemlandschaft sind Lösungen basierend auf Active-Directory und den dort genutzten Protokollen (z.B. SPNEGO, Kerberos) weit verbreitet.

Integration der eigenen Benutzerverwaltung

Die Integration der Benutzer und Rollen eines externen Dienstes ist Voraussetzung für die richtige Nutzung des Dienstes. Teilweise bringen Cloud-Dienste schon die Integration mit einem Unternehmens-LDAP mit. Außerdem gibt es schon Standards wie z.B. OpenID, mit denen man Identitäten zwischen Anbietern verifizieren kann. Setzt man allerdings Cloud-Dienste unterschiedlicher Anbieter ein, dann muss die Integration üblicherweise von der internen IT durchgeführt werden.

Provisioning von Cloud Services

Entscheidet sich ein Unternehmen für die Verwendung eines Cloud-Service, dann ist die Benutzung üblicherweise an eine Rolle gebunden. HR-Services sollten z.B. nur von HR-Mitarbeitern verwendet werden können. Das bedeutet aber, dass man bei Neunutzung eines Dienstes die entsprechenden Mitarbeiter freischalten muss, neue Mitarbeiter müssen nachgetragen werden, ausscheidende Mitarbeiter müssen entfernt werden. Werden diese Aufgaben manuell ausgeführt, dann bedeutet das relevante Kosten für ein Unternehmen. Automatisierung ist erwünscht, allerdings gibt es noch nicht viele Werkzeuge bzw. Anbieter für solche Lösungen.

Automatisierung von Geschäftsprozessen mit Cloud Services

Cloud-Dienste können entkoppelt und autonom verwendet werden. Das ist das heute noch übliche Geschäftsmodell von vielen Anbietern. Den größten Nutzen aus dem SaaS-Ansatz kann ein Unternehmen allerdings ziehen, wenn die Cloud Services für die Automatisierung bzw. Unterstützung von Geschäftsprozessen eingesetzt werden und mit der existierenden internen Software nahtlos integriert sind. Cloud-Dienste werden also als Teile einer Service-orientierten Architektur (SOA) betrachtet.

Integration interner und externer Dienste

Früher haben Firmen viel in die Integration von Anwendungen investiert (Enterprise Application Integration). Das war notwendig, weil Anwendungen, die aus Geschäftssicht zusammenspielen sollten, mit unterschiedlichen Technologien, auf unterschiedlichen Plattformen, aber auch mit unterschiedlichen Datenmodellen entwickelt wurden und deshalb nicht richtig zusammengepasst haben. Die Integration findet dabei auf unterschiedlichen Ebenen statt: auf der Datenebene, auf der funktionalen Ebene und auf der Präsentationsebene.

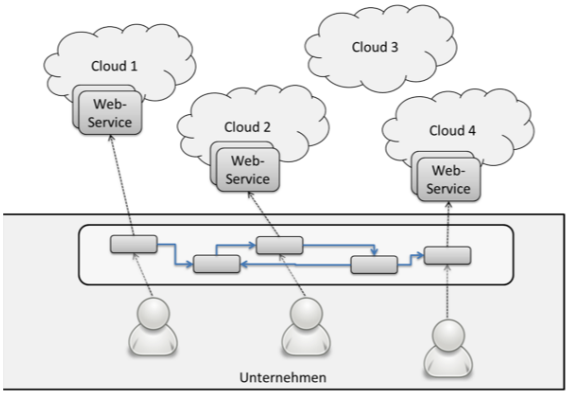

Abbildung 3: Prozessorientierte Verschaltung von Diensten

Ähnliche Integrationsaufgaben hat man nun auch der, wenn man Internet-Dienste unterschiedlicher teller einbinden will. Ein Anbieter definiert sein eigenes Datenmodell (hat z.B. sein eigenes Kundenobjekt), hat seine Technologie (z.B. SOAP Web Services) und bestimmt, wie die Interaktion mit Menschen über User Interfaces (z.B. ein HTML 5 mit vorgegebenem Layout) funktioniert. Bindet man mehrere Dienste unterschiedlicher Anbieter ein, dann vergrößert sich die Integrationsaufgabe.

Eine Service-orientierte Architektur ist dann schon fast Voraussetzung, da Dienste als Bausteine bereits vorgesehen sind, die Infrastruktur z.B. in Form eines Enterprise Service Bus Integrationsunterstützung bietet und damit Dienste einfacher eingebunden werden können.

Ein wichtiger Aspekt bei der Integration externer Dienste ist Sicherheit. Technisch muss eine sichere Übertragung, Authentifizierung und möglicherweise die End-to-End-Verschlüsselung sensibler Daten sichergestellt werden. Hier bieten SOAP Web Services mehr Möglichkeiten als RESTful Web Services.

Prozessautomatisierung

Geschäftsprozesse werden von Fachexperten definiert, sind an der Strategie orientiert und ändern sich, wenn sich z.B. der Markt oder das Angebot verändert oder wenn es neue gesetzliche Regelungen gibt. Geschäftsprozesse eines Unternehmens können in unterschiedli-

chen Varianten ausgeprägt sein, z.B. um länderspezifische Eigenheiten in internationalen Tochterfirmen abzubilden. Daher ist es wichtig, Geschäftsprozesse möglichst flexibel und einfach anpassbar zu implementieren.

Die Dienste einer Service-orientierten Architektur entsprechen dabei einzelnen Prozessaktivitäten, Teilprozessen oder sogar kompletten Prozessen. Um einen Geschäftsprozess abzubilden, werden existierende Dienste passend verschaltet und die Logik zur Ansteuerung der Dienste wird durch eine Process Engine ausgeführt. Die Process Engine startet Prozesse (z.B. durch Eingang eines Urlaubsantrags), verwaltet unterschiedliche Prozessinstanzen (z.B. Urlaubsanträge der Mitarbeiter Müller und Maier) und initiiert die nächsten Schritte einer Prozessinstanz (z.B. Manager Schmidt muss den Antrag von Herrn Maier genehmigen).

Der Einsatz einer Business Process Management Suite (BPMS) in Kombination mit einer Business Rules Engine ermöglicht die schnelle Umsetzung und einfache Anpassung von Prozessen. Änderungen werden dabei vor allem an den Prozessmodellen (in Business Process Model and Notation [ObMG11] beschrieben) und an den Geschäftsregeln vorgenommen. Durch den Austausch kompletter Dienste kann neue Geschäftslogik eingebunden werden.

Die BPMS bietet auch noch Funktionalität für das Monitoring der Prozessausführung und ist damit eine Informationsquelle für die Prozessoptimierung.

Cross-Cloud-Workflows

Cloud-Services können oftmals bereits mit anderen Cloud-Services interagieren – die Authentifizierung mit Mechanismen wie Open-ID ist ein sehr rudimentäres Beispiel, bei dem ein Service-Anbieter Dienste eines anderen nutzt. Weitere Beispiele findet man z.B. bei der Integration von Mail-Services oder Archivlösungen.

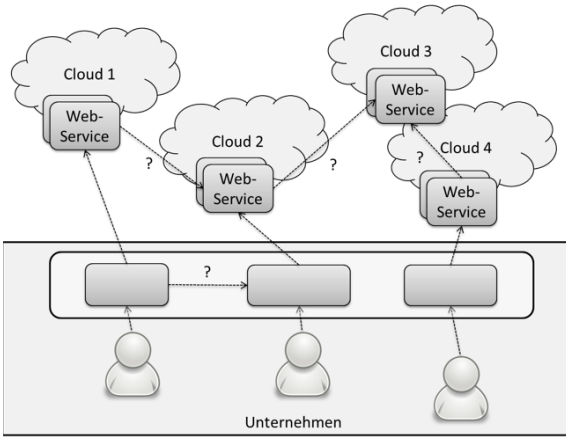

Abbildung 4: Cross-Cloud Workflows

Im Gegensatz zu den elementaren Diensten finden sich in der Cloud also bereits Teilabläufe, die – geschickt kombiniert – zu größeren und effizienten Workflows kombiniert werden können. Dazu müssen die genutzten Cloud-Services geeignet konfiguriert werden, wofür es in der Regel jedoch keine geeignete Programmierschnittstelle gibt, da diese Art der Kombination von der aktuellen Anbietern oft nicht vorgesehen ist.

Unter anderem stellt sich hier das Problem der Identity Propagation – wie werden Abläufe aus einer Cloud von der ausführenden Person in einer anderen Cloud angestoßen und unter welchem Namen erfolgt das? Abbildung 4 veranschaulicht die Situation.

ZUSAMMENFASSUNG UND AUSBLICK

Wir haben in diesem Beitrag vorgestellt, wie Unternehmen zukünftig unterschiedlichste Dienste von unterschiedlichen Anbietern aus ihrer Enterprise Cloud in ihre Anwendungslandschaft integrieren können. Ein Benutzer arbeitet zukünftig mit einem Prozessportal oder stellt sich sein User Interface nach eigenen Vorlieben zusammen (z.B. als Mashup) und sollte gar nicht merken, dass er Dienste aus unterschiedlichen Quellen des Internets konsumiert. Der zukünftig zu erwartende Markt für Dienste ermöglicht dann sogar den Austausch funktional äquivalenter Services.

Wichtig für den Erfolg der Enterprise Cloud ist, dass bestimmte Herausforderungen gelöst werden. Dazu gehören neben Sicherheitsproblemen auch Betriebsfragen, z.B, wie man das Service-Provisioning und die Abrechnung sicher und weitestgehend automatisiert vornehmen kann. Eine weitere Herausforderung liegt in der nahtlosen und sicheren Integration der (Web) Services und die weitestgehend werkzeugunterstützte Automatisierung von Geschäftsprozessen unter Verwendung dieser Dienste.

In dieser Arbeit haben wir für einen Teil der Herausforderungen Antworten bzw. Lösungen vorgestellt. Für andere Probleme, z.B. zur sicheren Verarbeitung sensitiver Daten, gibt es zwar schon Lösungsansätze, diese müssen sich in der Praxis allerdings erst noch bewähren. Speziell beim Thema Cross-Cloud Workflows müssen geeignete Lösungen erst noch entwickelt werden.

Wir sind jedoch davon überzeugt, dass zukünftig kleine, mittlere und große Unternehmen die Enterprise Cloud nutzenbringend einsetzen werden.

LITERATUR

[ClSA10] *Cloud Security Alliance*: „Top Threats to Cloud Computing“. cloudsecurityalliance.org. 2010, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. Abruf am 2012-05-12

[Euro11] *Europa Press Release*: „EU-Justizkommissarin Viviane Reding und Bundesverbraucherministerin Ilse Aigner setzen sich gemeinsam für einen stärkeren Datenschutz auf EU-Ebene ein“. In: Europa Press Releases Rapid. 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/762&format=HTML&aged=0&language=DE&guiLanguage=en. Abruf am 2012-05-12

[EuDe11] *EuroCloud Deutschland_eco e.V*: „SaaS Gütesiegel 1.0 - Kurzinformation“. 2011, http://www.saas-audit.de/files/2011/03/quick-reference_de.pdf. Abruf am 2012-05-12

[Fiel00] *Fielding, Roy Thomas*: „Architectural Styles and the Design of Network-based Software Architectures.“. UNIVERSITY OF CALIFORNIA, IRVINE, Dissertation, 2000.

[Frau12a] *Fraunhofer-Institut für Sichere Informationstechnologie*: „OmniCloud - Sicheres Datenbackup in beliebigen Storage-Clouds“. 2012, http://www.sit.fraunhofer.de/de/kompetenzfelder/projekte/omnicloud.html. Abruf am 2012-05-12

[Frau12b] *Fraunhofer-Institut für Sichere Informationstechnologie*: „On the Security of Cloud Storage Services.“ 2012, http://www.sit.fraunhofer.de/content/dam/sit/en/studies/Cloud-Storage-Security_a4.pdf. Abruf am 2012-05-12

[Henk11] *Henkel, Markus*: “OmniCloud: verschlüsselte Daten außerhalb der Cloud”. In: Enterprise Efficiency - The Efficient Information Technology Community. 2011,

http://de.enterpriseefficiency.com/author.asp?section_id=1292&doc_id=234344. Abruf am 2012-05-12.

[KKLS12] *Kleemann, Sascha; Leiker, Viktor; Künle, Tobias und Schwald Daniel*: „Services und servicebasierte Anwendungen aus der Cloud“. Seminararbeit, Hochschule Karlsruhe – Technik und Wirtschaft, Fachbereich Wirtschaftsinformatik. 2012.

[LaNV11] *Lauter, Kristin; Naehrig, Michael und Vaikuntanathan, Vinod* : „Can Homomorphic Encryption be Practical?”. In CCSW ´11Proceedings of the 3rd ACM workshop on Cloud computing security workshop.

[Mimo12] *Projektkonsortium MimoSecco*: MimoSecco – Middleware for Mobile and Secure Cloud Computing. 2012, http://www.mimosecco.de/. Abruf am 2012-05-12

[ObMG11] *Object Management Group*: Business Process Model and Notation (BPMN) – Version 2.0. 2011, http://www.omg.org/spec/BPMN/2.0/. Abruf am 2012-05-12.

[Papa07]*Papazoglu, Michael*: „Web Services: Principles and Technology”. Prentice Hall. 1st edition, 2007.

[SaaS11] *SaaS-Forum*: „SaaS-Forum Lösungskatalog“, 2011

[Sawa11] *Sawall, Achim*: „USA Patriot Act: Europäische Cloud-Daten nicht vor US-Zugriff sicher“. In: golem.de IT-News für Profis. 2011, http://www.golem.de/1106/84620.html. Abruf am 2012-05-12

[USCo01] *US Congress*: „H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT)“. In: The Library of Congress. 2001, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:. Abruf am 2012-05-12