

## Identity & Access Management aus der Cloud – Risiken und Lösungen



**Prof. Dr. Dr. G. Rossa**

iSM - Institut für System-Management

### Identity & Access Management aus der Cloud – Risiken und Lösungen

Mag sich der Begriff auch wieder ändern, so sind sich die Experten aus Wirtschaft, Wissenschaft und Politik inzwischen einig: das Konzept des Cloud Computing hat Zukunft und ein grosses Entwicklungspotential.

Cloud Computing birgt neben zahlreichen Chancen und Vorteilen (erwähnt seien hier die Aktualität von Anwendungen und Technik; Skalierbarkeit; Optimierung, Effizienz- und Qualitätserhöhung der IT-Umgebung und -Prozesse; Nutzung und Abrechnung nach tatsächlichem Bedarf mit variablen Betriebskosten statt fixer Investition und Kapitalbindung; Kostentransparenz und Kostensenkung; der professionelle IT-Betrieb durch Spezialisten mit Schonung eigener personeller Ressourcen; eine Katalysatorwirkung für Unternehmensinnovation; die verbesserte Energie- und Umwelteffizienz von IKT - Infrastrukturen und Diensten u.v.m.) aber auch erhebliche Risiken und zwar in erster Linie ein erhöhtes Sicherheitsrisiko.

### Cloud und Security - ein Widerspruch in sich?

Halten sich Unternehmen trotz der bekannten Vorteile gegenwärtig mit dem Einsatz von Cloud Computing und Software als Service noch zurück, so liegt der Grund dafür in erster Linie

in ihrer Sorge um die Sicherheit ihrer Daten.

Das Thema Sicherheit ist schon im abgeschlossenen Firmennetz eine grosse Herausforderung. In einer Zeit, in der die IT - Strukturen in Unternehmen umwälzende Änderungen erfahren (Cloud Computing), in der Infrastruktur (IaaS), Plattformen (PaaS) und Software (SaaS) als Dienste über das Internet bezogen und Un-

### Cloud Security

Ein Schwerpunktthema an der 8. security-zone von 10. und 11. Oktober 2011 in der Börse Zürich.

Details [hier ...](#)

ternehmensdaten aus den Firmennetzen ausgelagert und durch Dritte (Service Provider) verarbeitet und gespeichert werden, steigt die Angst der Anwender um die Sicherheit ihrer Daten vor potenziellen Bedrohungen und realen Gefahren zwangsläufig weiter und das Risiko- bzw. Sicherheitsmanagement erlangt eine neue Dimension.

### IT - Risikomanagement in der 4. Dimension

Die grundsätzlichen Anforderungen an Compliance, Informationssicherheit, Datensicherheit und Datenschutz haben

sich durch Cloud Computing ja nicht verändert, müssen aber in Cloud-Infrastrukturen anders gemanagt werden. Es geht also darum, die Unterschiede zur Inhouse-IT und die neuen Risiken im Cloud-Umfeld zu identifizieren, analysieren und dann zu reduzieren bzw. eliminieren, d.h. es ist eine SaaS-spezifische, konsistente Sicherheitsarchitektur zu schaffen. Dadurch kann sich Security künftig vom Cloud-Bremser sogar zum Cloud-Enabler entwickeln.

Abgesehen davon, dass die Unternehmen natürlich primär ein

## IdM / IAM-as-a-Service aus der (TRUSTED!) Cloud

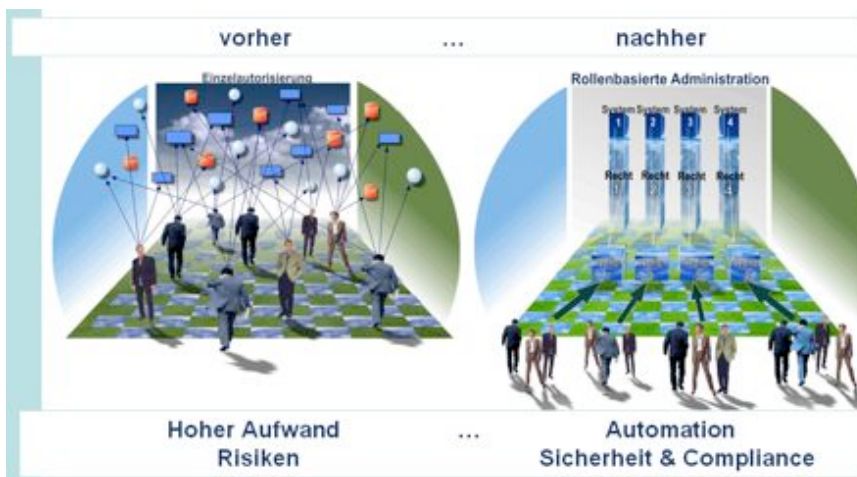
Ein wesentlicher Baustein und Garant für die Durchsetzung und Einhaltung von Gesetzen, Richtlinien und unternehmensspezifischen Sicherheitsvorschriften, egal ob nun im Firmen-Netz oder in der Cloud, ist der Einsatz einer leistungsfähigen Security Softwarelösung für das Identity, Authorization und Access Management, Provisioning, starke Authentifizierung, Passwortmanagement und Single Sign-On.

Mit diesem Werkzeug weiss der Anwender jederzeit, wer, wann,

ihre Geschäftsprozesse in der IT-Benutzer- und Rechteverwaltung deutlich optimieren und automatisieren und dadurch für mehr Sicherheit, Compliance, Nachvollziehbarkeit, Transparenz und Verlässlichkeit aller Vorgänge in diesem Bereich sorgen. Zum einen kann ein IdM als Metadirectory und Datendrehscheibe fungieren und angebundene Systeme automatisiert mit Änderungsdaten (User, Rechte, Organisation) versorgen (Provisionierung).

Zum anderen muss es, um das einer IdM-Lösung grundsätzlich innewohnende hohe Automatisierungs- u. Einsparpotential zu realisieren, über ein leistungsfähiges und praktikables Rollen- u. Prozessmodell mit Regelwerk verfügen. Eine leistungsstarke IdM-Lösung mit intelligentem Business Layer ist in der Lage, bis zu 80% Aufwandreduzierung durch massive Entlastung von Administration u. UHD zu erzielen.

Da jeder automatisierte Prozess (z.B. Antrags- und Genehmigungsverfahren, automatischer Mitarbeiterein- und austritt, Wechsel im Unternehmen, Rezertifizierung bereits erteilter Berechtigungen etc.) zu mehr Sicherheit beiträgt, ist eine IdM-Lösung in Konsequenz auch ein mächtiges Instrument für das Security und GRC Management, d.h. die Einhaltung interner u. externer IT-Sicherheitsrichtlinien, Funktionstrennung (z.B. mittels einer durchgängigen Security Classification), Nachvollziehbarkeit und die Aufdeckung und Vermeidung von Risiken (detective & preventive controls, z.B. mittels Internem Kontrollsystem): wichtig besonders für Vorstände und deren strafrechtliche Verantwortung!



grosses Eigeninteresse daran haben, ihre sensiblen Unternehmensdaten in der Cloud vor unberechtigtem Zugriff zu schützen, so bleiben sie bei der Auslagerung, Verarbeitung und Speicherung ihrer Daten durch Dritte ausserhalb des Firmen-Netzwerks auch weiterhin für die Corporate Governance (=> Überwachung der ordnungsgemässen Unternehmensführung), Compliance (=> Regelkonformität) als auch die Einhaltung der Datenschutzbestimmungen verantwortlich.

warum, welchen Zugang zu welchen Anwendungen besitzt und wer ihm dies genehmigt hat.

Ein doppelt positiver Effekt wird erzielt, wenn auch diese wichtigen IdM - Funktionen in Form von Cloud - Services einfach integriert, eingesetzt und verwaltet, also on demand genutzt werden können!

## Mögliche Benefits von IdM / IAM im Allgemeinen...

Mit einer Identity Management-Lösung können Unternehmen

Zentralisierung und Automatisierung bewirken i.d.R. zudem auf allen Ebenen und in allen Bereichen eine Kostensenkung. Einige Beispiele seien hier aufgezählt: Mitarbeiter nutzen Self-Service-Portale für Passwort-Resets und zur Beantragung von Kompetenzen und Ressourcen und entlasten dadurch die Administration. Durch die rechtzeitige Versorgung der Mitarbeiter mit den für ihre Arbeit erforderlichen Ressourcen und Rechten reduzieren sich die Bereitstellungskosten (Opportunity costs). Bei einem prozessgesteuerten Entzug von Rechten beim Mitarbeiteraustritt oder Abteilungs-, bzw. Unternehmenswechsel besteht keine Gefahr (wie es oft bei einer manuellen Verwaltung der Fall ist), dass die Deprovisionierung (Rechte-Entzug) ganz unterbleibt, wodurch es entweder zu sog. „Berechtigungsleichen“ oder zu einer Anhäufung von unzulässigen Rechten und damit zu einem eklatanten Sicherheits- bzw. Compliance-Problem kommt. Lizenz- bzw. Ressourcenoptimierung sind hierbei ein positiver Nebeneffekt der Workflows. Durch ein umfassendes und schnelles Reporting, also Auskunftsbereitschaft „per Knopfdruck“, lassen sich Kosten für die interne Revision und Wirtschaftsprüfung senken. Verfügt die IdM-Lösung über ein integriertes SSO (Single Sign-On) und Funktionen für eine gesicherte Authentifizierung und Kennwortrücksetzung, so lässt sich einerseits der Benutzerkomfort und die Sicherheit erhöhen, andererseits wiederum gravierend Administration und UHD entlasten. Eine integrierte transparente Kostenkontrolle fördert letztlich den bewussten Umgang mit

Berechtigungen für IT-Ressourcen. Technologisch führende IdM-Lösungen verfügen über ein mehrdimensionales Rechte-Management und sind in der Lage, Berechtigungen sowohl über die Aufbauorganisation, als auch in dynamischen Team- bzw. Projektorganisationen zu verwalten, sowie selbständige Units (Lieferanten, Händler- und Konzernstrukturen) zu integrieren. Sie sind Voraussetzung für SOA und unterstützen Portallösungen im Unternehmen.

### **... und von IdM-as-a-Service aus der (Trusted) Cloud im Besonderen:**

Unternehmen können starke IdM - Funktionalitäten ohne Bindung von Kapital und personellen Ressourcen nutzen. Sie sparen Lizenzkosten durch nutzungsbasierte Abrechnung und können das Produkt- und Serviceangebot bedarfsgerecht dynamisch erweitern. Dadurch wird der Einsatz von IdM-Lösungen auch für mittelständische Unternehmen interessant weil leistbar.

Die Implementierung, Integration, fachliche Begleitung und Betreuung erfolgt durch IdM - Experten, die eine langjährige Erfahrung im Bereich Security, Software-Entwicklung und Projektmanagement mitbringen sollten. Dadurch reduziert sich der Support- und Administrationsaufwand erheblich.

### **Security Business Intelligence (SBI) von IdM / IAM-Lösungen**

Aus dem Cloud-Umfeld ergeben sich neue, grössere Herausforderungen an die Security Business Intelligence von IdM - Tools bzw. IdM-Services. Sicherheitskonzepte sind an die veränderten „Umweltbedingun-

gen“ anzupassen und neue Risiken zu berücksichtigen. Das heisst: Ein mehrdimensionales Sicherheitskonzept ist unerlässlich und umfasst viele verschiedene technische und organisatorische Komponenten bzw. Aspekte wie die Eigensicherheit des IdM-Systems, die Sicherheitsarchitektur bei Web Services, ein gesichertes Betriebskonzept, gesicherte Authentifizierung, ein ausgereiftes (Fach-) Rollen- und Prozessmodell, umfassendes Compliance Monitoring und Reporting, SoD (Separation of Duties) und ein IKS (Internes Kontroll-System), ein durchgängiges Datenschutzkonzept mittels Security Classification an allen Identitäten und Objekten, Schutz vor Datendiebstahl (Datenverschlüsselung und -segmentierung, Zugriffschutz), sichere Kommunikationskanäle (auch bidirektional), Filetransfers, u.v.m.

### **Fazit:**

Werden die nötigen Voraussetzungen geschaffen (SaaS-spezifische Schutzmassnahmen, SaaS-spezifisches Sicherheitskonzept, Sicherheitsmanagement und gesicherte Umgebung beim Service Provider sowie Einsatz eines leistungsfähigen Identity Management Tools mit intelligentem Business Layer (Organisations-, Rollen- und Prozess Management), kann ein Sicherheits - Level erreicht werden, den die meisten Unternehmen eigenständig so nicht erzielen und dauerhaft aufrecht erhalten können. Somit können speziell kleine und mittlere Firmen ihre IT-Sicherheit mit SaaS und IAM als SaaS-Lösung aus der (Trusted!) Cloud sogar verbessern!