Identity und Access Management: die Trends 2014

Michael Fischer und Rüdiger Weyrauch, ORACLE Deutschland B.V. & Co. KG

Die Analysten von Gartner beschrieben bereits Ende des Jahres 2012 mit den „Nexus of Forces“ (siehe „http://www.gartner.com/technology/research/nexus-of-forces“) das Zusammenwachsen der für sich allein schon mächtigen Strömungen „Mobile“, „Social“, „Cloud“ und „Information“ zu einem Markttrend, der umfassende Veränderungen und Umwälzungen mit sich bringt in der Art und Weise, wie wir arbeiten, kommunizieren und Geschäfte machen.

Aktuelle Beispiele zeigen, wie Hersteller von Sportschuhen heute von Millionen Läufern Informationen sammeln und darauf neue Business-Modelle aufbauen oder Dienste wie „myTaxi“ und „Uber“ etablierte Geschäftsmodelle überholen. Wichtig für viele dieser neuen Dienste sind adäquate Sicherheits-Architekturen zum Schutz vor Datenmissbrauch, aber auch intelligente und einfache Dienste, die die Nutzerwahrnehmung positiv beeinflussen und zu einer raschen Kundenbindung führen.

Tauscht man in den obigen Sätzen „Kunden“ durch „Mitarbeiter“, so ergeben sich vergleichbare Anforderungen für Unternehmen, die ihren Mitarbeitern ein modernes Arbeitsumfeld anbieten möchten. Hierzu zählen Konzepte wie „Work from Home“, Nutzung der eigenen Lieblingsgeräte (BYOD) und ein von überall erreichbares Netz. Lassen sich Unternehmen auf diese flexible Art der Arbeitsplatznutzung ein, entsteht häufig eine Win-Win-Situation. Der Mitarbeiter ist produktiver durch das angenehmere Arbeitsumfeld sowie die flexibleren Arbeitszeiten und -orte und er fühlt sich durch die eingeräumten Freiräume stärker wertgeschätzt. Beispiele hierfür sind die Nutzung von Tablets bei Marktleitern einer Supermarktkette, die damit direkt im Lager und Verkaufsraum flexibler arbeiten können, oder die Verwendung mobiler Endgeräte im Field Service, bei dem Schäden durch die Kamera aufgenommen und gegebenenfalls notwendige interne Genehmigungen und Anweisungen direkt und zeitsparend vor Ort eingeholt werden.

Im Konsumentenbereich ist der Konkurrent heute nur einen Klick entfernt: Ein Kunde kann heute Angebote von Firmen mit minimalstem Aufwand vergleichen, sodass neben dem Preis häufig das Benutzererlebnis immer mehr kauf- oder bindungsentscheidend wird. So wird eine mobile App beispielsweise nach langen Wartezeiten, Fehlversuchen oder aufwändigen Registrierungsschritten prompt gelöscht und zum Wettbewerb gewechselt. Das Nutzererlebnis aus Single Sign-on, die Akzeptanz von Social Logins und die geräteoptimierter Darstellung gilt es in Einklang zu bringen mit Funktionalität und Sicherheit.

Viele neue Initiativen in den Unternehmen werden aus den Fachbereichen und dem Marketing nicht nur initiiert, sondern immer häufiger auch direkt und ohne Beteiligung der IT umgesetzt. Dies führt ohne übergeordnete Kontrolle zu einer Vielzahl von IT- und damit auch Sicherheits-Silos. Nicht wenige Unternehmen haben daher aus verschiedensten Gründen mehrere Directory Server, Access Management oder sogar Provisionierungslösungen unterschiedlicher Hersteller im Einsatz, die langfristig teurer in Lizenzen und/oder Betriebskosten werden.

Mobile First!

Bei der Mobilmachung der Unternehmen haben oftmals die klassischen Ansichten der IT-Security den Vorrang: Verhindern, was zu verhindern geht. Beim mobilen Zugriff auf Unternehmensdaten stand bisher die Nutzung von Firmengeräten im Vordergrund, die mithilfe von Mobile-Device-Management-Lösungen (MDM) stark auf das Wesentliche reduziert wurden: Mail, Kalendar, Kontakte. Die Geräte wurden zentral verwaltet und bei Verlust oder Diebstahl komplett gelöscht. Wie passt das zu dem Trend, sein eigenes Gerät auch für die Arbeit nutzen zu wollen? Moderne Unternehmensstrategien sehen daher parallele Ansätze vor:

- Unternehmenseigene, stark in der Nutzung beschränkte Devices, die vollständig gemanagt werden: Dies können auch Spezialgeräte sein, die mehrere Mitarbeiter nutzen.
- Unternehmenseigene oder private mobile Geräte, denen der Zugang zu Unternehmensressourcen über einen sogenannten „Container“ ermöglicht wird, dem Mobile Application Management (MAM). Dabei wird unternehmensseitig nur ein Teil des Geräts, der Container, zentral verwaltet und im Falle des Falles gelöscht. Dies schafft Freiräume, auch Firmengeräte für die private Nutzung zu öffnen. „Data Leakage Prevention Policies“ regeln dabei auf App-Ebene, welche Daten zwischen Apps (oder eben externen Cloud-/Mail-Diensten) transferiert werden dürfen und welche nicht.
- Ermöglichung des Zugangs zu Unternehmensressourcen auch ohne MDM/MAM-Lösung: Die bestehende Access-Management-Lösung kontrolliert die

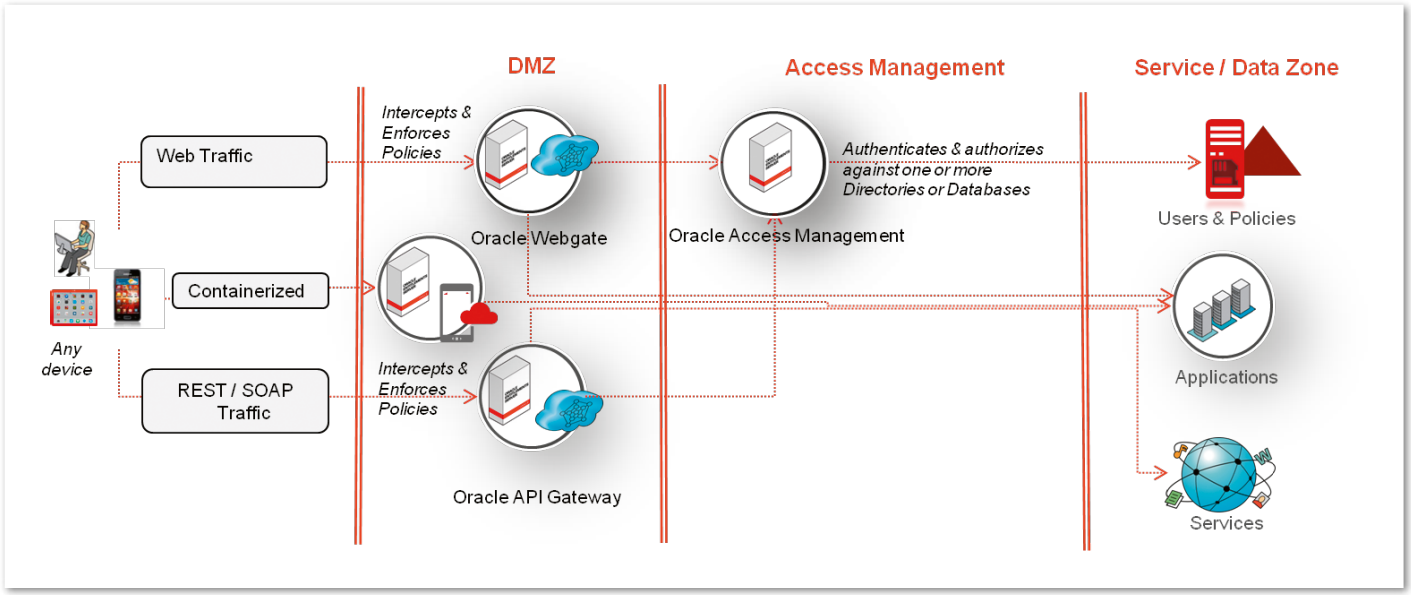

Abbildung 1: „Mobile Security" eingebettet in Access Management

Zugriffe. Dabei spielt es keine Rolle, ob der Zugriff aus einer nativen App heraus oder über den Browser erfolgt.

Aus Konsumentensicht wird die Akzeptanz sozialer Identitäten wie Google oder Facebook durch die Unternehmen immer wichtiger: Man möchte nicht schon für einfache Mehrwerte oder weniger sensible Informationen einen vollständigen Registrierungsmarathon (zumal auf einem kleinen Display) durchlaufen. Viele Konsumenten haben bereits entsprechende Logins und treffen als angemeldeter Google-Nutzer auf die Unternehmensangebote. Die Akzeptanz des „Social Logins" führt zu einer Win-Win-Situation: Der (potenzielle) Kunde bekommt ohne großen Aufwand mehr Informationen über das Angebot, das Unternehmen erhält im Gegenzug zumindest eine Wiedererkennung oder sogar eine gültige E-Mail-Adresse zur vertrieblichen oder marketinggesteuerten Nachbearbeitung. Gleichgültig mit welchem Gerät die Nutzung erfolgt, die Möglichkeiten sind – sofern vom Gerät unterstützt – unabhängig vom genutzten Kanal.

Oracle unterstützt Firmen bei ihrer zukunftsorientierten Mobility-Strategie mit folgenden voneinander unabhängigen Bausteinen:

- Mobile Apps für zahlreiche Oracle-Enterprise-Applikationen (BI, HCM, JD Edwards)
- Ein Mobile-Application-Framework, um eine Cross-Plattform-Entwicklung von Apps oder HTML5-Anwendungen für mobile Devices zu ermöglichen
- „Mobile Access"-Komponenten, die die Zugriffsmöglichkeiten von registrierten vs. nicht registrierten Geräten individuell steuern und soziale Protokolle wie „Oauth" zur Verfügung stellen
- Ein Authentifizierungs-Framework (SDK) zur Entwicklung von nativen Apps, das die einfache Integration in das bestehende Access Management und Single Sign-on (SSO) auf dem Gerät ermöglicht
- Eine Container-Lösung, die einen verschlüsselten, sicheren Container auf einem mobilen Gerät für Applikationen und Mails bereitstellt

Abbildung 1 zeigt eine vollständige Architektur für den sicheren mobilen Zugriff auf Unternehmensdaten. Ein weiterer Anwendungsfall ist die Nutzung des mobilen Geräts als zweiter Kanal bei der Authentisierung/Autorisierung. Statt herkömmlicher Hardware-Tokens kann mit einer auf dem Endgerät angezeigten, sich ständig aktualisierenden Pin der Zugang zu Systemen ermöglicht werden. Oracle hat mit dem „Mobile Authenticator" die entsprechende Oracle-Access-Management-App (Android, Apple) als Service bereitgestellt.

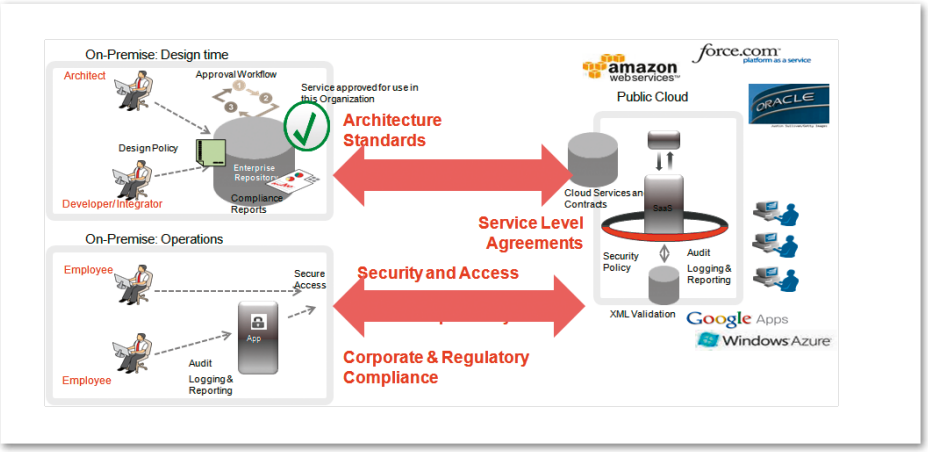

Abbildung 2: „Cloud Security" eingebettet in Identity Management

Cloud Services/Cloud Access

Im Rahmen von Konsolidierungen oder neuen Geschäftsstrategien erfolgt immer häufiger die Nutzung von „Software as a Service"-Lösungen, sei es für Kunden-/Personal-Management, Customer Service oder Marketing. Sind die grundlegenden Datenschutzbedürfnisse geklärt, geht es anschließend um die sichere Integration dieser Services in die bestehende Infrastruktur inklusive der Kopplung an das Identity Management. *Abbildung 2* zeigt ein mögliches Szenario.

Aus Endbenutzer-Sicht erscheint dabei ein eigentlich abgeschafftes Problem wieder auf der Bühne: Neue Benutzernamen und Passwörter sind zu merken, da die externen Lösungen nicht in bestehende SSO-Systeme eingebunden sind. Mit dem Access Portal hat Oracle im aktuellen Release eine Verbindung der drei notwendigen Technologien hergestellt: Federation Standards wie SAML, Web Access Management oder automatisches Füllen von Anmeldeformularen werden genutzt, um dem Endbenutzer Desktop- und Device-unabhängig wieder eine Single-Sign-on-Wahrnehmung zu gestatten. Dabei ist die Portal-Seite als Webseite wiederum für alle Formfaktoren (PC, Smartphone, Tablet) geeignet, um über alle Kanäle eine einheitliche Nutzererfahrung zu ermöglichen.

Defragmentierung

Viele Anwendungen und Systeme nutzen konstruktions- oder historisch bedingt Accounts und Berechtigungen auf eigenen Repositories. Die Pflege von Accounts geschieht oft manuell, etwa über Administratoren oder Helpdesks. Die Grundlage der Tätigkeiten ist meist ein gesprochener oder schriftlicher Antrag, sodass ein Nachweis eines Berechtigungsursprungs aufwändig werden kann.

Mit einem übergreifenden Unified Identity Management kann die Verwaltung manuell und/oder automatisiert über alle Systeme hinweg erfolgen. Zudem kann es für weitere Aufgaben genutzt werden, etwa Zeitreisen, Soll/Ist -Vergleiche, periodische Berechtigungsüberprüfungen (Rezertifizierungen) oder die Überwachung kritischer Berechtigungskombinationen (Segregation of Duties) sowie zeitlich begrenzte Urlaubsvertretungen.

In dieses System kann auch die Verwaltung von ausgelagerten Applikationen beim Outsourcer oder Cloud Provider integriert werden. Entsprechende Schnittstellen sind im Markt etabliert (wie SAML, SCIM) beziehungsweise lassen sich auch in halbautomatischen Verfahren nutzen (wie webbasierte Anträge und Datenabgleiche), falls eine direkte Integration nicht gewünscht oder nicht möglich ist.

Idealerweise lassen sich alle Kanäle, auch die mobile Welten, in das Identity Management integrieren. Damit können von einem Punkt aus Richtlinien angeordnet und durchgesetzt (etwa bei Entlassungen oder Data Leakage Prevention) sowie das Benutzererlebnis über alle Systemzugänge identisch gehalten werden. Ein übergeordnetes System kann so viele Bearbeitungsschritte automatisieren und helfen, neue Nutzungsszenarien oder Geschäftsideen umzusetzen.

Fazit

„Mobile", „Social", „Cloud" und eine informationszentrische Sicht ändern bestehende Geschäftsabläufe und -strukturen nachhaltig. Security und Identity Management sind wichtige Begleiter dieser Trends und gehören gleich zu Beginn einer neuen Initiative mit auf die Agenda. Bestehende Regeln und Identitätsspeicher wiederzuverwenden und neue Silos zu vermeiden, ist sinnvoll und möglich. Kontextbasierte Entscheidungen (Ort, Gerät, Zeit, Historie) und die feingranulare Steuerung auf den Zugriff von Dokumenten und Daten sowie die verschlüsselte Ablage und Übertragung von Daten auf mobile Endgeräte sind einige der zahlreichen neuen Features, um die Oracle die bestehenden Lösungen in den vergangenen Releases ergänzt hat. Weitere Informationen unter www.oracle.com/identity.

Michael Fischer
michael.fischer@oracle.com

Rüdiger Weyrauch
ruediger.weyrauch@oracle.com

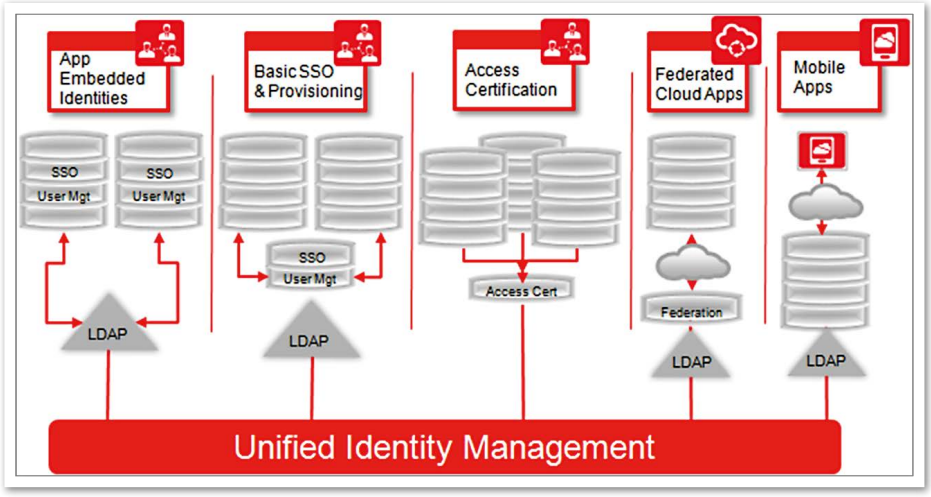

Abbildung 3: Unified Identity Management