Security als "Enabler" mobiler Strategien

Rüdiger Weyrauch
Oracle Deutschland B.V. & Co KG
Dreieich

Schlüsselworte

Mobile Security, Mobile Application Management, Mobile Access, Social Sign On, Digitalisierung, mobile Strategie, Nutzerwahrnehmung

Einleitung

Die Nutzung mobiler Geräte im Unternehmensbereich schreitet unaufhörlich voran, sei es für einfache Dienste wie Mail und Kalender aber auch für Genehmigungen und ganze Vertriebprozesse. Dieser Trend führt zu einer Verschiebung etablierter Sicherheitsmodelle vom Rechenzentrum hin auf das Endgerät. Wie immer bei Sicherheitsvorgaben entscheidet die gefühlte Flexibilität und Nutzerwahrnehmung über die Akzeptanz der Richtlinien. Dies beinhaltet ein Single-Sign-On auf dem Endgerät in die Unternehmensapplikationen genauso wie die Nutzung privater Endgeräte auch für den dienstlichen Gebrauch. Im Konsumentenbereich steht neben dem Datenschutz vor allem eine komfortable Nutzerwahrnehmung im Vordergrund, z.B. durch Nutzung von Identitäten sozialer Netze für Anmeldeverfahren. Über offengelegte Schnittstellen werden Unternehmensdienste der Entwicklergemeinschaft zur Verfügung gestellt, um neue Dienste für den Konsumenten anbieten zu können. Der Vortrag geht auf Kundenbeispiele aus verschiedenen Branchen ein und zeigt dabei auf, wie Access Management Technologien maßgeblich zum Erfolg dieser innovativen Lösungen beigetragen haben.

Mobile First!

Immer mehr Unternehmen ermöglichen ihren Mitarbeitern Zugriff auf Unternehmensdaten über ein mobiles Endgerät. Auch die wachsende Nutzung cloudbasierter Lösungen geht oft einher mit der Nutzung mobiler Applikationen. Warum forcieren die Unternehmen die Nutzung mobiler Geräte? Neben der Steigerung der Attraktivität als moderner Arbeitgeber wird eine erwartete höhere Produktivität meist als erster und vielleicht wichtigster Grund genannt. Entscheidungen können von „unterwegs“ im System getroffen werden (z.B. Genehmigung einer Beschaffung), Außendienstmitarbeiter geben zwischen zwei Einsätzen oder Kundenterminen bereits ihre Ergebnisse in den Systemen ein (z.B. einen Kundenauftrag) und Wartungsmitarbeiter erhalten stets aktuelle Bedien- oder Reparaturvideos auf ihr Tablet gespielt.

Wenngleich der Nutzer oftmals nur das mobile Frontend sieht und benutzt, gehören zu einer mobilen Strategie unter anderem die Integration in die bestehenden IT-Prozesse und Applikationswelten sowie technische wie organisatorische Vorkehrungen zur Sicherheit dieses neuen Zugriffsweges.

Waren in der vor-mobilen Internet-Welt die Rechenzentren meist über umfassende Schutzmaßnahmen an den Grenzen („Perimeter“) abgesichert, so muß diese Burgmauer-Mentalität neu überdacht werden. Mobile Applikationen ziehen Daten aus dem geschützten Rechenzentrum (mit neuen Protokollen) und kombinieren oder synchronsieren sie gegebenfalls mit weiteren Applikationsdaten in Cloud-Umgebungen. Diese potentiell unternehmenswichtigen oder auch personenbezogenen Daten werden auf einem kleinen Gerät gespeichert, welches allein in Deutschland im letzten Jahr über 236.000 mal als gestohlen gemeldet wurde. Der Perimeter, der Sicherheitspunkt der mobilen Welt, wird heute an dem Ort definiert, an denen Daten konsumiert werden.

Bevor wir uns anschauen, wie Sicherheitstechnologien neue mobile Services überhaupt erst ermöglichen, betrachten wir einige aktuelle Kundenbeispiele:

SuperValu, eine Supermarkt-Kette in den USA mit über 4.700 eigenen und franchise-betriebenen Märkten, rollt aktuell Tablets an die Marktleiter aus. Diese bekommen damit eine einfache – und mobile – Möglichkeit, direkt im Ladenbereich Echtzeit-Informationen über Lager- und Kassenbestände abzurufen und damit besser auf Kundenwünsche eingehen zu können. Die Produktivitätssteigerung durch einfache Applikationen ermöglichen dem Marktleiter, mehr Zeit im Verkaufsraum und damit im Kundendialog zu verbringen. Im Backend konnte SuperValu durch eine Konsolidierung von Daten und Servern weitere Effizienzsteierungen erzielen. Für Partner, Franchise-Nehmer und Kunden wird zudem eine Social Media Integration aufgebaut, um die Kommunikation mit dem Unternehmen noch einfacher zu gestalten.

Beachbody, ein schnell wachsendes Unternehmen der Wellness- und Fitnessbranche mit über 6,5 Millionen Community-Teilnehmern und 200.000 Trainern, ermöglicht mit Hilfe einer konsolidierten Plattform für Web und Mobile seinen Kunden wie Coaches einen intuitiven wie sicheren Zugang zu personalisierten Inhalten. Zudem wurde der Online-Shop enger mit den Backend-Systemen integriert.

Ein Öl-, Gas- und Energieunternehmen mit mehr als 60.000 Mitarbeitern setzt eine mobile Strategie für verschiedene Geschäftsfelder um, bei der Mitarbeiter - gleich ob mit Firmengerät oder eigenem Gerät – sicheren Zugriff auf Mail- und Sharepoint-Inhalte erhalten. Insbesondere die verfolgte BYOD[1] Strategie konnte mit einer sicheren Trennung geschäftlicher und privater Inhalte umgesetzt werden. Über eingebaute Data Leakage Prevention Regeln wird zudem ein ungewollter Abfluß vertrauenswürdiger Daten, z.B. auf Cloudspeicher, verhindert.

Mobile? Security!

Bei der „Mobilmachung“ der Unternehmen haben oftmals die klassischen Ansichten der IT Security den Vorrang: Verhindern, was zu verhindern geht. Doch die oben beschriebenen Kundenbeispiele zeigen, wie durch die Nutzung von Identitäts- und Zugriffsmanagement sowie Management der Daten auf Endgeräten das potentielle Risiko von Datenmißbrauch und Datenverlust soweit reduziert werden konnten, dass die Mehrwerte der Nutzung mobiler Geräte ermöglicht werden konnten.

Beim mobilen Zugriff auf Unternehmensdaten stand bisher die Nutzung von Firmengeräten im Vordergrund, die mit Hilfe von Mobile Device Management (MDM) Lösungen 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:

1. Unternehmenseigene, stark in der Nutzung beschränkte Devices, die vollständig gemanagt werden: dies können Spezialgeräte sein, die von mehreren Mitarbeitern genutzt werden.
2. Unternehmenseigene oder private mobile Geräte, welchen 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. Die Daten sind sowohl im Container als auch auf dem Verbindungsweg ins Rechenzentrum verschlüsselt.

[1] BYOD: Bring Your Own Device

3. Ermöglichung des Zugangs zu Unternehmensressourcen auch ohne MDM/MAM Lösung: mit Hilfe der bestehenden Access Management Lösung werden die Zugriffe kontrolliert. Dabei spielt es keine Rolle, ob der Zugriff aus einer nativen App heraus oder über den Browser erfolgt.

Aus Konsumentensicht (wir erinnern uns: der Wettbewerb ist nur ein Klick entfernt) wird die Akzeptanz sozialer Identitäten wie Google oder Facebook durch die Unternehmen immer wichtiger: wer möchte schon für einfache Mehrwerte oder weniger sensible Informationen einen vollständigen Registrierungsmarathon (zumal auf einem kleinen Display) durchlaufen? Viele Konsumenten haben bereits entsprechende Benutzerkonten und treffen als angemeldeter Google Nutzer auf die Unternehmensangebote. Die Akzeptanz des Social Logins führt zu einer Win-Win-Situation: der (potentielle) 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.

Eine weitere technologische Neuerung, API Security, ermöglicht es Firmen, bestehende Dienste (z.B. als Web Services) über eine offengelegte Schnittstelle (API) Dritten zur Verfügung zu stellen. Dies kann an die Entwicklergemeinde gerichtet sein, die eigene mobile Applikationen auf dieses Services aufsetzen und damit dem Unternehmen mehr Sichtbarkeit, höhere Marktdurchdringung und letzten Endes mehr Kunden und Umsatz bringen. Geolokationsdaten und aktuelle Angebote von Schnellrestaurants oder Kaffehäusern sind hier nur zwei B2C Beispiele. Auch im B2B Bereich werden APIs genutzt um z.B. externe Shop-Anbieter mit den Logistik- und Vertriebsmodulen des Unternehmens zu koppeln. API Security Lösungen erweitern bestehene Webservice-Security Technologien um Perimeter-Lösungen, die schadhaften XML-Code erkennen können, Protokoll-Umsetzungen wie z.B. REST zu SOAP vornehmen oder durch Throttling-Mechanismen SLAs für API Nutzer umsetzen können.

Oracle Identity & Access Management für die mobile Welt

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

- mit mobilen Apps für zahlreiche Oracle Enterprise Applikationen (BI, HCM, JD Edwards),
- mit einem Mobile Application Framework, um eine plattformübergreifende Entwicklung von Apps oder HTML5 Anwendungen für mobile Geräte zu ermöglichen,
- mit Mobile Access Komponenten, die die Zugriffsmöglichkeiten von registrierten vs. nicht registrierten Geräten individuell steuern und soziale Protokolle wie OAuth zur Verfügung stellen,
- mit einem Authentifizierungs-Framework (SDK) zur Entwicklung von nativen Apps, das die einfache Integration in das bestehende Access Management ermöglicht und SingleSignOn (SSO) auf dem Gerät ermöglicht sowie
- mit einer Containerlösung, die einen verschlüsselten, sicheren Container auf einem mobilen Gerät für Applikationen und Mails bereitstellt und damit eine sichere Trennung geschäftlicher und privater Daten ermöglicht
- mit einem Mobile Authenticator, der die Nutzung des mobilen Gerätes als zweiten Kanal bei der Authentisierung/Autorisierung ermöglicht. Statt herkömmlicher Hardware-Tokens kann mit einer auf dem Endgerät angezeigten, sich ständig aktualisierenden Pin der Zugang zu Systemen hergestellt werden.

Abbildung 1 veranschaulicht eine vollständige Architektur für den sicheren mobilen Zugriff auf Unternehmensdaten.

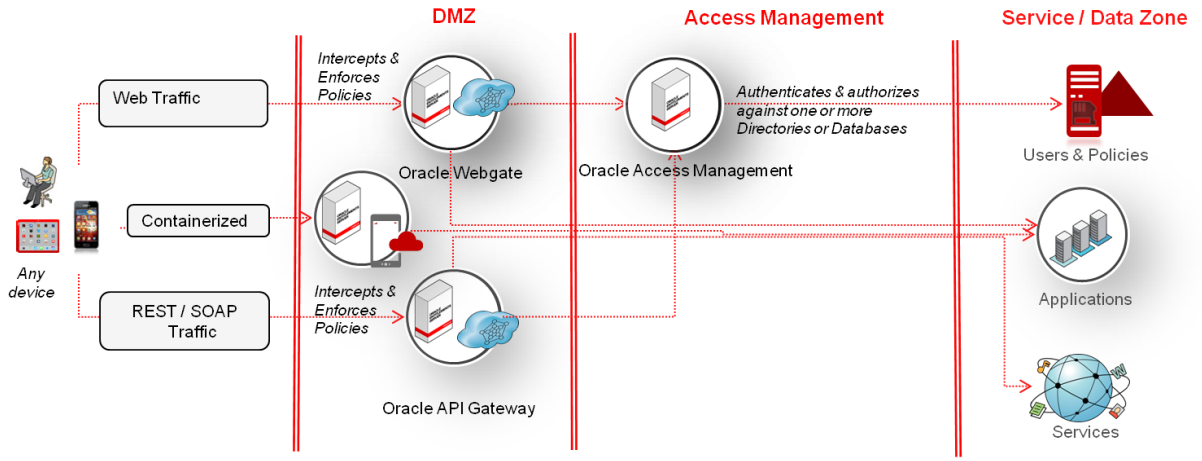

Abbildung 1: Mobile Security eingebettet in Access Management

Fazit

Trends und Studien zeigen, dass mobile Endgeräte und damit der mobile Zugriff auf Unternehmensdaten weiter stark wachsen werden. Traditionelle Sicherheitsverfahren sind hierfür nur unzureichend gerüstet oder erweitern die bestehenden IT-Architektur oftmals um ein weiteres Silo. Oracle‘s Strategie ist es, im Unternehmen etablierte Verfahren für Identitäts- und Zugriffsmanagement sowie bestehende Rollen- und Rechtekonzepte um die mobile Welt zu erweitern. Dies ermöglicht ein integriertes Sicherheits- und Zugriffskonzept für die Unternehmenswelt, als auch für mobile Endgeräte.

Kontaktadresse:

Rüdiger Weyrauch

Oracle Deutschland B.V. & Co KG
Robert-Bosch-Strasse 5
D-63303 Dreieich

Telefon: +49 (0) 6103 397 661
E-Mail ruediger.weyrauch@oracle.com
Internet: www.oracle.de