ENTERPRISE MOBILITY MANAGEMENT

Das ändert sich mit iOS 8 und Android L für Unternehmen

14.10.2014 | von Christopher Dreher (Autor) und Mark Zimmermann (Autor)

War vor wenigen Jahren noch der kanadische Anbieter Blackberry das Maß aller Dinge im Firmenumfeld, hat sich dies spätestens seit der Einführung von ersten Enterprise-Funktionen in Apples iOS geändert. Mittlerweile ist auch Google aufgewacht und buhlt mit Apple um die Vorherrschaft im Business.

Mit iOS 8 legte Apple in Sachen Business-Tauglichkeit weiter nach. Foto: Apple

Die Anforderungen an das Enterprise Mobility Management (EMM) steigen mit jedem Jahr. Eine zunehmend wichtiger werdende Komponente im EMM-Umfeld ist die Trennung von persönlichen und Unternehmensdaten. Dies ermöglicht es dem Unternehmen, sowohl Firmengeräte zur privaten Mitnutzung ("Choose your own Device" oder "Corporate Owned. Personally Enabled") frei zu geben, als auch private Endgeräte im Firmennetzwerk zu integrieren ("Bring your own Device").

Als erster Vertreter hatte Blackberry mit der Funktion Balance in Blackberry 10 eine Möglichkeit der Trennung vorgeführt (Dual Persona). Android hatte diese Trennung bisher nur auf Samsung-Geräten mit der Funktion Samsung Knox und Apple führte eine Trennung auf App und Datenebene bereits mit iOS 7 ein.

Mit einer neuen Generation von Betriebssystemen wollen Apple und Google diesen hart umkämpften Enterprise-Markt jeweils für sich gewinnen - und stellen die EMM-Landschaft damit vor neue Herausforderungen. Ein Überblick:

iOS 8: Mehr APIs, mehr Möglichkeiten

iOS 8 wurde im September offiziell an die Endanwender und somit auch an die Nutzer im Enterprise-Umfeld verteilt. Die über 4000 neuen API-Aufrufe geben Entwicklern und Administratoren neue Möglichkeiten, was das System für den Einsatz im Unternehmen noch interessanter macht. So wurden Sicherheit, Performance und Integrierbarkeit in die Unternehmenslandschaft mit iOS 8 weiter ausgebaut, EMM-Hersteller können ihre Systeme um eine Reihe neuer IT-Policies erweitern. Diese neuen Richtlinien bedienen dabei sowohl die klassische Geräteverwaltung als auch die erweiterte Verwaltung von so genannten Managed Apps.

Neue Funktionen und Technologien in iOS 8 1/14

Touch ID

: In iOS 8 stellt Apple die Fingerabdruckerkennung auch fremden Apps zur Verfügung.

Foto:

Apple hatte bereits mit iOS 7 die Möglichkeit eingeführt, Apps für den Unternehmenseinsatz zu definieren, spezifische VPN Konfigurationen (App-VPN) pro App zu konfigurieren und per unternehmenseigene Single-Sign-On-Lösung (SSO) zu verbinden. Diese Business-Container auf Basis definierter Apps unterliegen im Anschluss der Restriktion, dass Daten nur innerhalb und durch diesen Container ausgetauscht werden können. Über Managed Apps und Domains können die native E-Mail-Anwendung sowie der Safari-Browser in den Container eingebunden werden.

Mit iOS 8 geht Apple hier noch einen Schritt weiter. Neben den Managed Apps lassen sich jetzt Dokumente wie PDFs, ePubs und iBooks per EMM verteilen und verwalten. Revisionsthemen werden nun ebenfalls stärker ins Auge gefasst. So

können Administratoren über das EMM festlegen, dass der Nutzer sein Endgerät nicht eigenständig löschen oder um eigene Konfigurationen erweitern kann.

Das vor einem Jahr bereits angekündigte Device-Enrollment-Program hat nun auch mit iOS8 endlich finalen Einzug gehalten. Dies erlaubt es die initiale Anbindung an ein EMM im Einrichtungsassistenten von iOS8 zu hinterlegen. Der Nutzer erhält auf diese Art ein Endgerät im originalverpackten Zustand, alle Konfigurationsvorgaben finden auf der Seite von Apple statt. Durch die Registrierung des Gerätes bei Apple wird dabei sichergestellt, dass im Rahmen der Einrichtung die Konfiguration des EMM erfolgen muss. Für den Nutzer erfolgt dies transparent und integriert in dem iOS-Betriebssystem.

Eine weitere zentrale Neuerung bezieht sich auf die Sicherheit der Daten auf einem iOS-8-Endgerät: Bisher konnte Apple auf ausgewählte Daten (SMS, Fotos, Kontakte, Audio-Aufnahmen und die Anrufliste, nicht jedoch E-Mails und Kalendereinträge) zugreifen, die auf einem Gerät mit iOS 7 (oder älter) gespeichert waren. Die Strafverfolgungsbehörden machten sich das zunutze, indem sie Apple die konfiszierten Geräte übergaben und per richterlichen Beschluss die Datenherausgabe einforderten. Möglich war das, weil diese Daten nur hardwareseitig verschlüsselt waren. Sobald das Endgerät das Betriebssystem gestartet hatte, waren die Daten zugänglich.