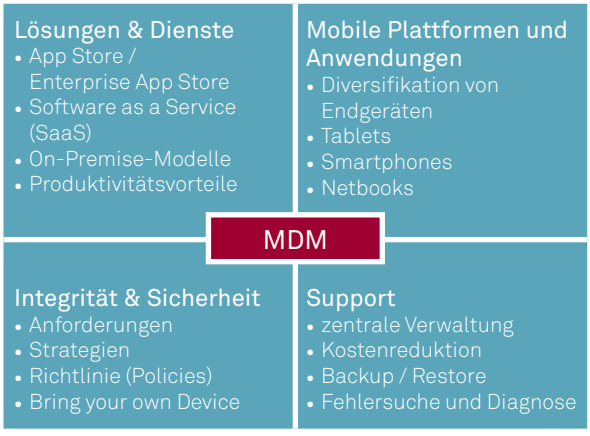
Mobile Device Management (MDM)

Zentrale Verwaltung von Mobilgeräten im Unternehmenseinsatz

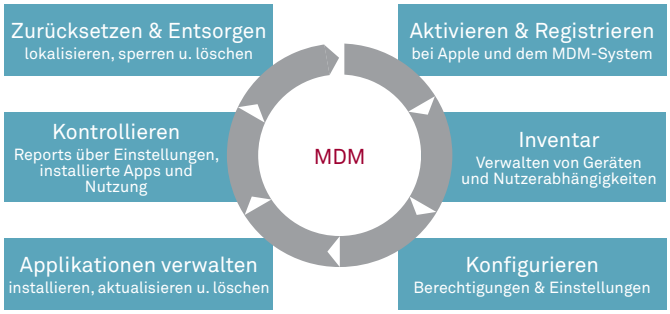
Der Siegeszug von Smartphones und weiteren mobilen Endgeräten hält unvermindert an. Sie sind als Kommunikations- und Produktivitätsplattform nicht mehr wegzudenken. Dabei entstehen aber auch neue Herausforderungen hinsichtlich Sicherheit und Nutzbarkeit, insbesondere beim Einsatz im Unternehmen.

Definition

Mobile Device Management ermöglicht die Verteilung von Anwendungen, Daten und Konfigurationseinstellungen für jegliche Art mobiler Endgeräte. Auch die Prozesse zur Inbetriebnahme dieser Geräte werden berücksichtigt. Jedes einzelne mobile Endgerät kann nach der Registrierung mit beliebigen Konfigurationen versehen werden. Hierbei sind alle Einstellungen denkbar, die das mobile Betriebssystem unterstützt. Zum Beispiel kann die Kamera deaktiviert oder der Besuch von öffentlichen AppStores unterbunden werden. Diese Funktionen sind allerdings stark abhängig von den jeweiligen Betriebssystemen und nicht mit allen Geräten möglich. iOS, Android oder auch Windows Phone unterscheiden sich hier teilweise erheblich.



Neben der Konfiguration bietet Mobile Device Management auch ein Mobile Application Management (MAM). MAM regelt die Verwaltung und Verteilung von Anwendungen, so genannten Apps, auf den registrierten Endgeräten. Mit Hilfe von MAM kann man



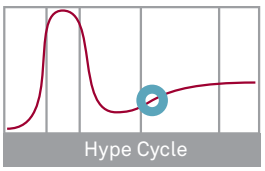
exakt steuern, welche Anwendung auf den jeweiligen Endgeräten ausgeführt werden dürfen.

Ein weiterer wichtiger Bestandteil von MDM-Lösungen besteht im Controlling und Reporting. MDM Systeme bieten einen Überblick über alle im Einsatz befindlichen mobilen Endgeräte, sowie deren Einstellungen, Profile, Netzwerknutzung und den installierten Anwendungen. Mit diesen Informationen lassen sich Benutzungsvorgaben für mobile Endgeräte einfach überwachen und protokollieren.

MDM unterstützt auch den Prozess bei der Entsorgung oder beim Zurücksetzen von einzelnen Endgeräten. Im Falle eines Verlusts oder Diebstahls lässt sich das Gerät über GSM- oder GPS-Ortung auffinden. Es kann aus der Ferne gesperrt oder bei Bedarf könnne alle Daten komplett gelöscht werden. Somit kann verhindert werden, dass sensible Daten unberechtigten Zugriff erlangen.

Reifegrad

Mobile Device Management ist bereits etabliert. Es existiert eine Vielzahl an Anbietern für MDM-



Lösungen, die eine Geräte- und Betriebssystemübergreifende Verwaltung erlauben. Apple iOS und Android Endgeräte bieten hierbei die größte Konfigurationsvielfalt im Vergleich zu Microsoft Windows Phone.

Marktübersicht

Die Produkthersteller von MDM-Lösungen konzentrieren sich überwiegend auf iOS und Android, gefolgt von Windows Phone und Blackberry. Neben den Basisfunktionalitäten bieten sie auch die Integration in eine bestehende Infrastruktur (SAP, SharePoint usw.). Weitere Möglichkeiten wie beispielsweise die Fernortung, das Erkennen von manipulierten Endgeräten (JailBreak-Detection) oder eine integrierte Benutzerverwaltung (LDAP, MS-AD) stehen zur Auswahl. Die Funktionen lassen sich als Cloud-basierte Lösung, als „Software as a Service" (Saas) oder auch als Server-Applikation realisieren. Je nach Sicherheitsrelevanz, zum Beispiel bei VPN- oder Mail-Passwörtern, kann das Unternehmen entscheiden, in welchem Rahmen sie ihre Daten ablegen will.

Gartner hat in diesem Jahr den kalifornischen Hersteller **MobileIron** als den führenden Anbieter im Bereich Mobile Device Management eingestuft, gefolgt von **GOOD**, **SAP (Sybase)**, **Fiberlink**, **Zenprise** und **Airwatch**. Wie im gesamten IT-Sektor ist auch der Markt für MDM Lösungen sehr schnelllebig, eine Konsolidierung ist in vollem Gange.

Alternativen

Für kleine Unternehmen bietet Apple einfache Applikationen an. Einstellungen und Richtlinien (Policies) werden direkt auf die Geräte per USB-Kabel oder XML-Download verteilt. Auch Microsoft Exchange unterstützt bereits grundlegende MDM-Funktionalitäten wie die Verteilung von Passwort-Policies oder die Fernlöschung von Geräten. Grundsätzlich lassen sich Apps auch über einen eigenen Webserver, der als App-Store dient via Download verteilen. Der relativ hohe Verwaltungsaufwand der mit diesen Lösungen entsteht, ist aber nur bis ca. 20 Endgeräte vertretbar.

Referenzszenario

Führende Industrieunternehmen, insbesondere die Automobilebranche oder bekannte Handelsketten setzen auf MDM-Lösungen um die administrativen Geschäftsabläufe effizient zu automatisieren. Die Verteilung der Anwendungen an die Mitarbeiter wird sicher gestellt. Die IT-Abteilungen können mit geringem Administrationsaufwand für eine sehr hohe Sicherheit der Unternehmenddaten und für die Einhaltung von Prozessen sorgen.

Business Impact

Für die Auswahl der richtigen MDM Lösung ist es wichtig, die wirklich notwendigen Sicherheitsanforderungen zu erkennen. Ein Unternehmen, welches mit einer ausgeprägten Außendienstvertriebsstruktur agiert oder hochsensible Daten offline zur Verfügung stellt, muss weit reichende Sicherheits-Richtlinien durchsetzen. Wird eine „Bring your own Device" Strategie verfolgt, muss ein liberaleres, weniger restriktives Policy-Modell etabliert werden.

Pro	Contra
Daten- und Zugriffssicherheit erhöht die Transparenz der verwendeten Endgeräte und der darauf laufenden Anwendungen (Apps)	Unter Umständen starke Einschränkung der Nutzungsmöglichkeiten (wirkt einer ByoD Strategie entgegen)
Kosten und Nutzung kontrollieren, Inventarisierungsmöglichkeiten	Beschränkung auf ein Minimum von Device-Typen bzw. OS-Plattformen

msg systems ag
Robert-Bürkle-Straße 1 | 85737 Ismaning/München
Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113
www.msg-systems.com | info@msg-systems.com

Stand: September 2012
http://www.msg-systems.com/techrefresh
XT-180-1209-1