VON MOBILE DEVICE MANAGEMENT (MDM) ZU ENTERPRISE MOBILITY MANAGEMENT (EMM)

DI Dr.techn. Franz PACHA

Inhalt

- *Traditionelles MDM*
- *Was ist Enterprise Mobility Management (EMM)*
- *Implementierungsmöglichkeiten und Nutzen*
- *Zusatzaspekt: BYOD*
- *Juridische Aspekte*

MDM traditionelle Aufgabenstellung

- *Produktivität von Außendiensmitarbeitern erhöhen*
- *Mobile Endgeräte betriebsbereit machen/halten*
- *Einzelne Unternehmensanwendungen zu ermöglichen*
- *Sicherheitseinstellungen zu erzwingen*

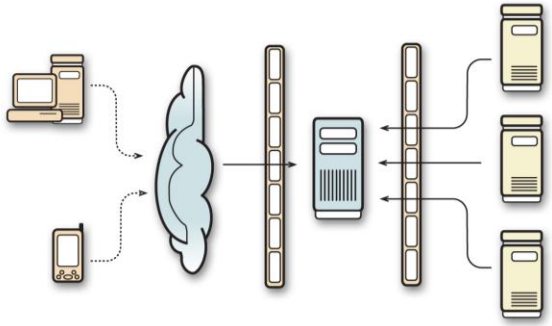
- *Help-Desk Aufwand klein halten*
- *Funktionsumfang beschränken*
- *Gerätevielfalt reduzieren*

MDM - Funktionen

- *Gerätekonfiguration*
  - Zugangspunkte (Datenverbindung, WLAN, ..)
- *Inventar*
  - Geräteinformationen HW & SW
- *Sicherheitseinstellungen*
  - Passwortsperre, Verschlüsselung, …
  - Löschen
- *PIM-Einstellungen*
  - Email, Kontakte, Kalender, …
- *OTA File-/Anwendungstransfer*

MDM - Aufbau

- *Gerät steht im Mittelpunkt*
  - IMEI zur Identifizierung
- *MDM - Server in DMZ oder Intranet*
- *Deployment zentral gesteuert*
- *Verbindungsaufnahme mit MDM-Server*
  - Vom Server durch SMS getriggert
  - Vom Client durch User-Interaktion
- *Userdaten sind Attribute des Gerätes*



- BYOD kein Thema
  - Geräte nicht attraktiv
  - fehlende Apps für persönlichen Nutzen

Der Smartphone Boom …

- Neue Betriebssysteme (iOS, Android, etc.)
- Neue Gerätetypen (Tablet & Phablet)
- Neue Funktionen (GPS, NFC, ..)
- Neue SW-Architekturen (Sandbox, ..)
- Neue Infrastrukturen (Appstores, Push-Services,..)
- Neue Kollaborations-Werkzeuge (Twitter, IM, …)
- Neue Cloud-Services (Dropbox, Instagram, …)

- scheinbar „kostenfrei“ zur persönlichen Nutzung verfügbar

… bringt neue Möglichkeiten für Unternehmen …

- *Mobile Erweiterungen von Unternehmensanwendungen*
- *Prozessketten ohne Medienbruch*
- *Höhere Mitarbeiterproduktivität*
- *Rasche Reaktionsketten*
- *Genauere Informationserfassung*
- *Bessere Entscheidungsgrundlagen*

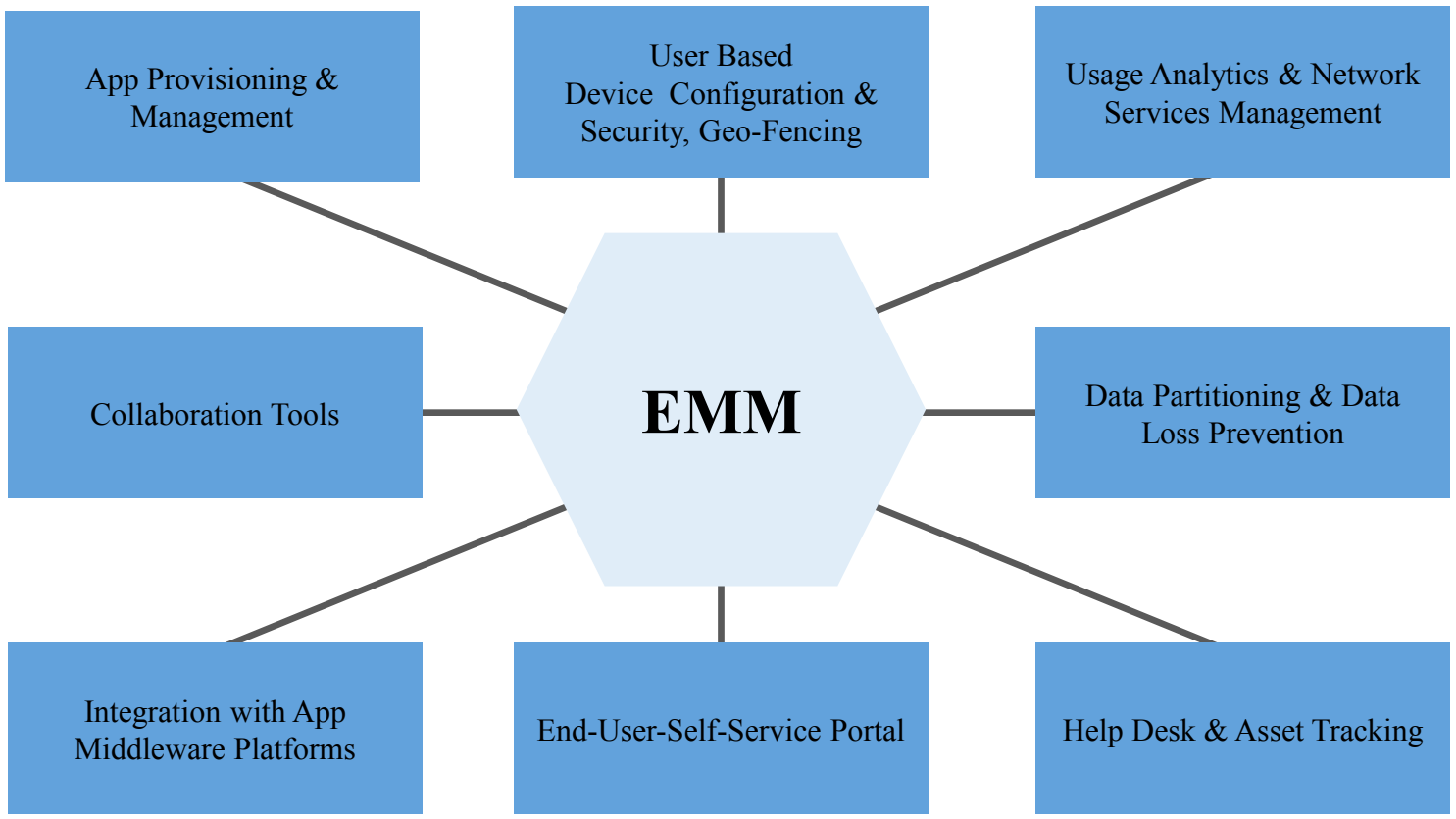
… und neue Herausforderungen

- *Anwendungen und Anwendungskonfiguration*
- *User-Authentifizierung vs. Geräte-ID*
- *Zertifikatmanagement*
- *Dokumentenmanagement*
- *Zeit-, Ort-, und Personenbezogene Profile für Security und Nutzung*
- *User-Self-Service*
- *PIM-/Email Zugang und Attachements*
- *Trennung privater Daten/Anwendungen von Unternehmensdaten/Anwendungen*

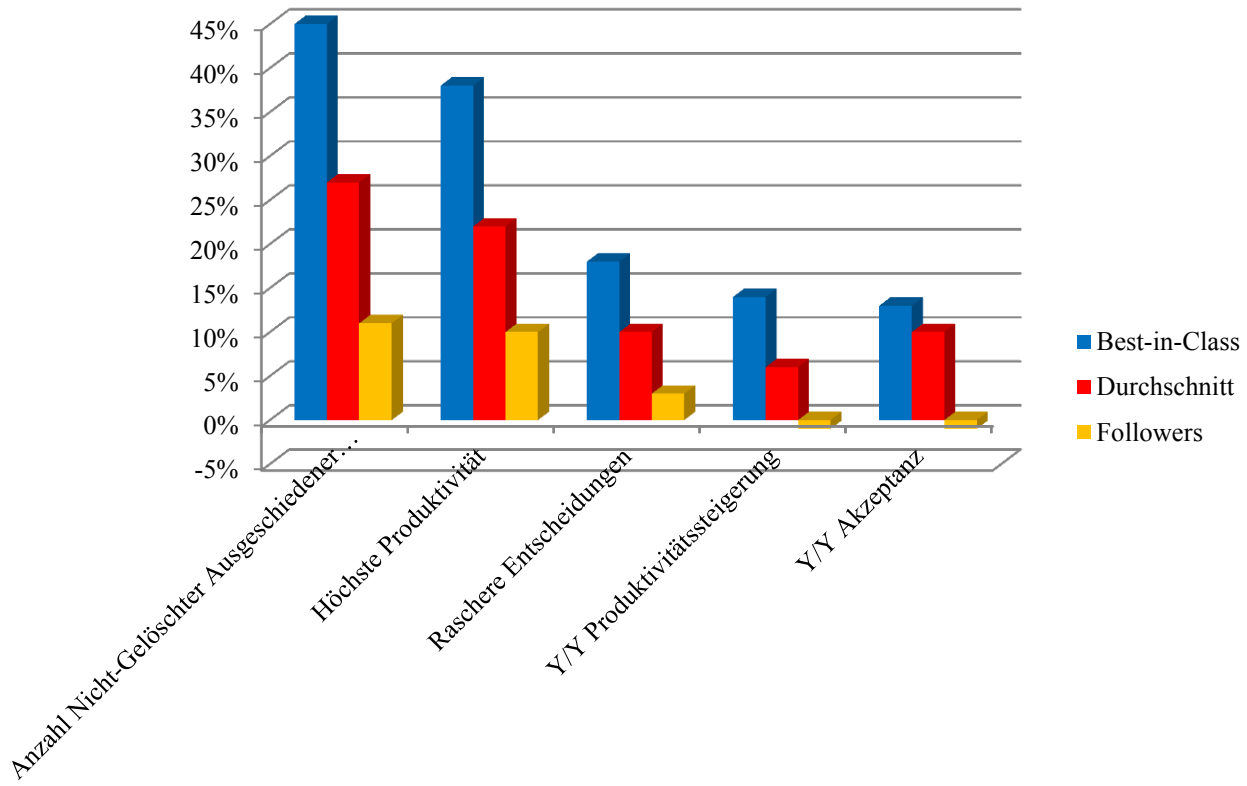
„Neue“ Fachbegriffe

- **MAM:** Anwendungsmanagement
  - Appstore und Unternehmensanwendungen
- **DLP:** Dokumentenmanagement/Data Loss Prevention
- Mobile **Collaboration** Tools
- **Geofencing**: Ortsabhängige Profile/Berechtigungen
- Netzwerkmanagement/-Monitoring
  - Intranetzugriff, Malware, Roaming, Hotspots
- **PII**: Schutz privater Daten (Pers. Ident. Information)
- **Analytische** Funktionen

Funktionsumfang eines umfassenden Enterprise Management Systems

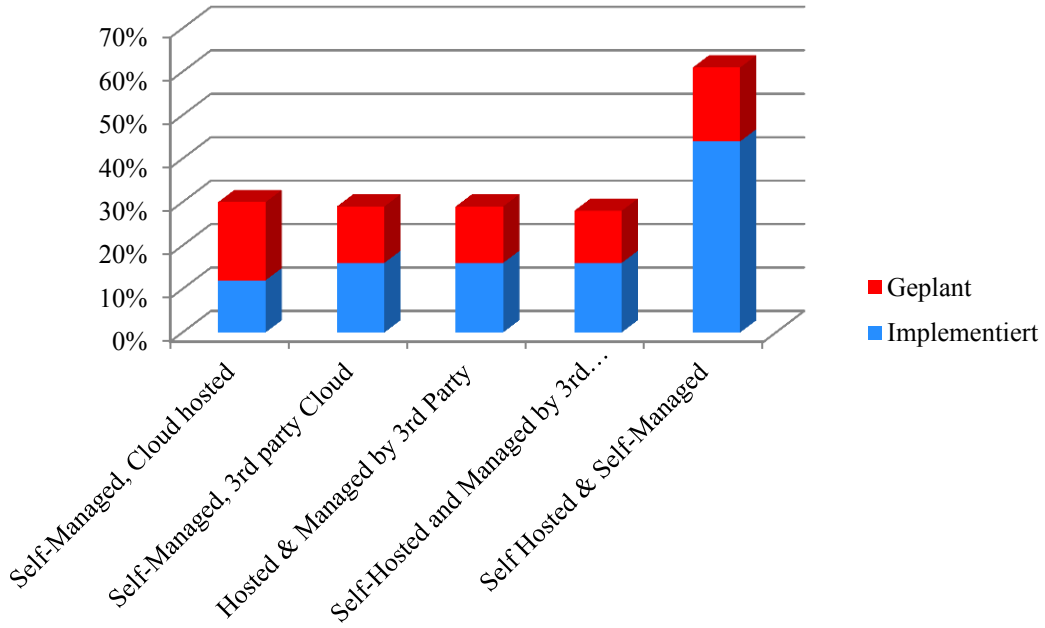


Nutzen von EMM „Best Practise“



Lt. Aberdeen Group, Juli 2012

Delivery- Modell EMM



Lt. Aberdeen Group, Juli 2012

Implementierungsstrategie für EMM-System

- Use-Case-Analyse (lt. Gartner)
  - A1: öffentliche Unternehmen mit Schwerpunkt PIM
  - A2: öffentliche Unternehmen
  - B: private Unternehmen mit allgemeinen mobilen Ansprüchen
  - C: Unternehmen mit Schwerpunkt auf Kostenstruktur
  - D: Unternehmen, die auf mobile Lösungen angewiesen sind

Kriterien für EMM-Implementierung

Produktfunktion	Overall	A1	A2	B	C	D
Device Diversity	10%	5%	1%	20%	1%	5%
Policy Enforcement	10%	5%	10%	5%	0%	5%
Security	10%	5%	10%	5%	0%	5%
Containerization	10%	70%	5%	0%	0%	0%
Inventory	10%	5%	5%	9%	20%	15%
Software Distribution	10%	1%	55%	15%	0%	10%
Reporting/Analysis	10%	1%	2%	40%	20%	20%
IT Service Management	10%	2%	10%	4%	5%	40%
Network Management	10%	5%	1%	1%	53%	0%
Delivery Model	10%	1%	1%	1%	1%	0%
Total	100%	100%	100%	100%	100%	100%

Laut Gartner

Zusatzaspekt: BYOD

- *Bring Your Own Device*
  - Gerät des Mitarbeiters
  - Apps des Mitarbeiters
  - Providervertrag des Mitarbeiters
  - Apps und Appsnutzung des Unternehmens
  - Abgeltung mit Pauschalzahlungen

Warum BYOD?

Warum BYOD?

- *Mitarbeiter wollen persönliche Produktivitätstools im Unternehmen nutzen*

Warum BYOD?

- *Mitarbeiter wollen persönliche Produktivitätstools im Unternehmen nutzen*
- *Reduktion des Help-Desk-Aufwands durch Identifizierung Mitarbeiter mit dem Gerät*

Warum BYOD?

- *Mitarbeiter wollen persönliche Produktivitätstools im Unternehmen nutzen*
- *Reduktion des Help-Desk-Aufwands durch Identifizierung Mitarbeiter mit dem Gerät*
- *Technologiefortschritte rascher nutzen*

Warum BYOD?

- *Mitarbeiter wollen persönliche Produktivitätstools im Unternehmen nutzen*
- *Reduktion des Help-Desk-Aufwands durch Identifizierung Mitarbeiter mit dem Gerät*
- *Technologiefortschritte rascher nutzen*
- *Kostenersparnis*

Kriterien für EMM-Implementierung

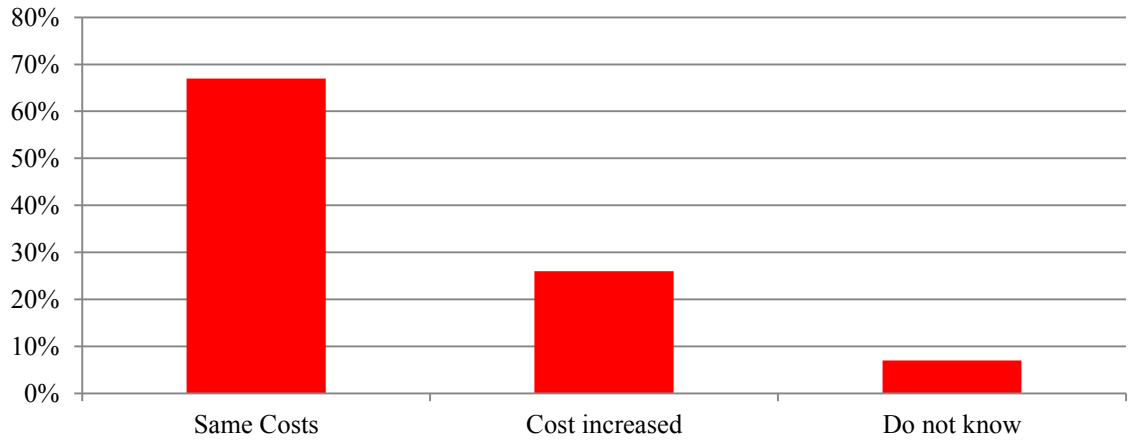
Produktfunktion	Overall	A1	A2	B	C	D	BYOD
Device Diversity	10%	5%	1%	20%	1%	5%	20%
Policy Enforcement	10%	5%	10%	5%	0%	5%	5%
Security	10%	5%	10%	5%	0%	5%	10%
Containerization	10%	70%	5%	0%	0%	0%	20%
Inventory	10%	5%	5%	9%	20%	15%	5%
Software Distribution	10%	1%	55%	15%	0%	10%	15%
Reporting/Analysis	10%	1%	2%	40%	20%	20%	10%
IT Service Management	10%	2%	10%	4%	5%	40%	5%
Network Management	10%	5%	1%	1%	53%	0%	0%
Delivery Model	10%	1%	1%	1%	1%	0%	10%
Total	100%	100%	100%	100%	100%	100%	100%

Laut Gartner, BYOD F.Pacha

Kostenauswirkungen BYOD

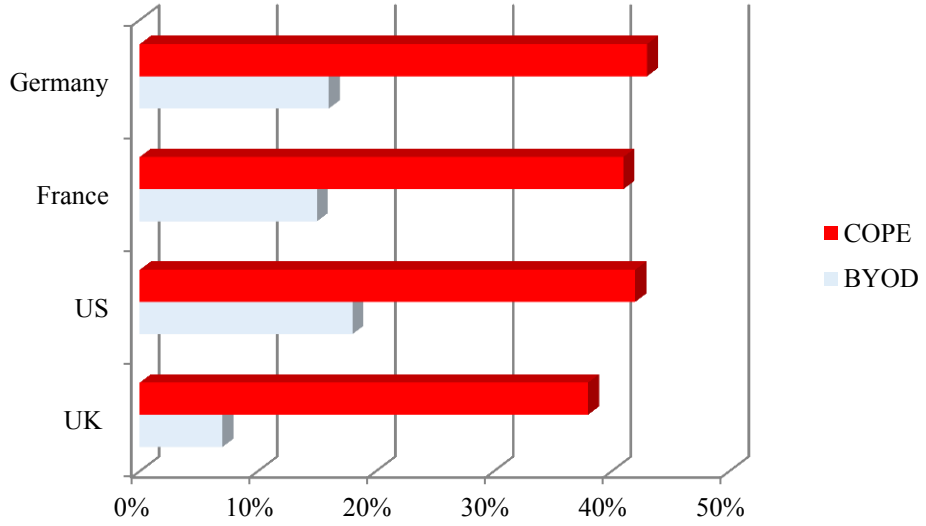
- *Kostenersparnis?*

Lt. Studie Mind Commerce, Jänner 2013



Alternativmodell: COPE

- *COPE = Corporate Owned Personally Enabled*
  - Lt. Mind Commerce, Jänner 2013



  - 2015 werden 70% der Unternehmen dem COPE Modell folgen

The Mobile Enterprise

20. Februar 2013

Bring Your Own Device ...
juristisch betrachtet

Rechtsanwalt
Mag. Markus Gaderer, LL.M.

HASLINGER NAGELE

Interessen des Mitarbeiters vs Interessen des Unternehmens

Einerseits:

- Kommunikationsgeheimnis -

  Wahrung durch den Unternehmer

- Persönlichkeitsschutz

  Auslesen von Informationen über den Mitarbeiter: Welche Apps installiert, Standortdaten, Instant-Messages, Fotos etc)

Interessen des Mitarbeiters vs Interessen des Unternehmens

Einerseits:

- Abgeltung der Unternehmensnutzung
- Keine Nutzungseinschränkungen
- Keine sonstige Einflussnahme des Arbeitgebers

  (welches Gerät, welche Software, etc)

Interessen des Mitarbeiters vs Interessen des Unternehmens

Andererseits:

- Datenschutz

  Haftung des Unternehmens ohne Möglichkeit auf das Gerät zuzugreifen…

- Geheimnisschutz

- Urheberrecht

  Haftung für Verstöße der Mitarbeiter „im Betrieb des Unternehmens“

Was tun?

- Vereinbaren Sie mit dem Mitarbeiter klare Regeln!
  - schriftlich
  - vorab
- Faktische „Regelung“ durch technische Maßnahmen

  zB: Strikte Trennung privater und geschäftlicher Daten

  Beispiel E-Mails am Smartphone; „Vermischung“ Privat- und Geschäftskonto

HASLINGER NAGELE

Was regeln:

- Wer, wie, wann und in welcher Form kann auf die Daten am Gerät bzw auf das Gerät seitens des Unternehmens Zugriff nehmen

- Mindest-Sicherheitsmaßnahmen (Passwort, automatisches Sperren des Bildschirmes/Geräts etc)

Was regeln:

- Mitteilungspflichten (bei Verlust, Verkauf, Nutzung im Ausland etc)

- Einsatz von Monitoringwerkzeugen durch den Unternehmer (Geräteortung, Telefonie-Verbindungsdaten, Gerätestatus jailbroken? etc)

- Verlust

  Wann dürfen Daten (alle?) am Gerät vom Unternehmen gelöscht werden?

Was regeln:

- Beschränkungen des Privateinsatzes (zB kein Siri, kein iCloud etc)
- (keine!) Nutzung durch Dritte
- Haftungsverteilung zwischen Mitarbeiter und Unternehmer

Wir sehen uns beim Round Table!

HASLINGER / NAGELE & PARTNER
RECHTSANWÄLTE GMBH

Mölker Bastei 5, 1010 Wien
Tel 01 / 718 66 80

Roseggerstraße 58, 4020 Linz
Tel 0732 / 78 43 31

markus.gaderer@haslinger-nagele.com

HASLINGER
NAGELE