Úvod

From Wikipedia, the free encyclopedia:

> **Enterprise mobility management** (**EMM**) is the set of people, processes and technology focused on managing the increasing array of mobile devices, wireless networks, and related services to enable broad use of mobile computing in a business context.

Na první pohled vypadá uvedená věta jako krásné shrnutí, při bližším prozkoumání čtenář snadno odhalí, že jde ve skutečnosti o nic neříkající kus textu. V následujících řádcích bych se proto rád pokusil vysvětlit, co se pod zkratkou EMM skrývá, a jaké jsou nejzásadnější součásti a nejaktuálnější problémy uvedené problematiky.

Poznámka:

V následujícím textu budu pracovat se zkratkou **EMM**. Český ekvivalent pro název článku **Použití a správa přenosných zařízení v podnikovém prostředí** je trochu krkolomný na použití v textu. Pokud vás ale napadne nějaký hezký a výstižný český termín, uveďte ho prosím v komentáři.

Motivace

K čemu to je dobré

S tablety, či aspoň chytrými telefony, pracuje denně každý z nás. Většinou je používáme hlavně pro osobní potřebu a pro zábavu. Jaké výhody by ale mělo použití těchto zařízení v zaměstnání?

1. Zefektivnění práce zaměstnanců:
   - přístup k mailu, firemnímu chatu a komunikace vůbec,
   - organizace schůzek, porad a jiných meetingů,
   - snadná práce s poznámkami a úkoly.
2. Zvýšení dostupnosti:
   - zaměstnanců,
   - dokumentů,
   - organizačních nástrojů.
3. Zrychlení odezvy v komunikaci:
   - jednak mezi zaměstnanci,
   - ale i ve vztahu zákazník <-> zaměstnanec.
4. Snížení nákladů:
   - zefektivněním komunikace,
   - za tisk dokumentů,
   - příp. výdajů za méně efektivní systémy.

Ideální případ

Míra a způsob využití mobilních technologií se samozřejmě liší podle velikosti a zaměření organizace i podle mnoha dalších faktorů. Ale například použití mobilních zařízení pro vnitrofiremní komunikaci lze uplatnit ve většině podniků. Na to, abyste si mohli vyřídit e-maily od šéfa, chat s kolegy nebo popohnat maníky z IT oddělení nepotřebujete počítač. Stejně tak se může hodit možnost zaslat zprávu spolupracovníkům odkudkoli, kde se zrovna budete nacházet, ať už to bude cizí kancelář, zasedací místnost nebo služební cesta.

Rychlá organizace pracovních schůzek se může hodit kdykoli. Pokud se zaseknete v ranní špičce, jednoduše přesunete schůzku o hodinu později a pošlete krátké upozornění všem účastníkům. Není třeba vyřizovat tucet telefonních hovorů, ani nikoho pověřovat, aby vám s řešením takové záležitosti pomohl.

Možnost přečíst si důležitý firemní dokument, nebo aspoň nahlédnout do nejkritičtějšího odstavce, aniž by došlo k jakémukoli zdržení také není od věci.

Co tomu brání

Z předchozích odstavců by se mohlo zdát, že použití mobilních zařízení ve firmách je skvělé a úžasné, a že je vlastně s podivem, že to tak ještě všude nefunguje. Bohužel nasazení a použití mobilních systémů v podnikovém prostředí není tak jednoduché, jak to vypadá. Masovému rozšíření moderních technologií brání mnoho faktorů, z nichž jsou nejvýznamnější:

1. **Náklady** - Zřejmě nejzásadnější problém v jakémkoli podniku. Správa mobilních zařízení, vývoj firemních aplikací, vytvoření potřebných rozhraní, údržba celého systému a poskytování podpory si žádají nemalé finanční částky. U malých firem mohou značně převyšovat jakýkoli přínos ze zavedení mobilních technologií do firemní infrastruktury. U velkých podniků se pak může prodražit správa celého systému.
2. **Integrace** do stávajícího systému. Zajistit spolupráci letitých informačních systémů, léta neudržovaných docházkových a finančních systémů, rozličných komunikačních nástrojů a nebo naopak nejnovějších ticketovacích a plánovacích systémů s mobilními zařízeními nemůže být nikdy zcela jednoduché. Čím více různých systémů je třeba integrovat do mobilního řešení, tím rychleji rostou nároky na finance (viz bod 1).
3. **Změny** - Málokdo to přizná, ale všichni se jich bojí. Změnit zaběhnutý pořádek věcí a procesů uvnitř podniku zavedením nových mobilních řešení nelze ze dne na den. Komplexní systém vyžaduje zaškolení a zaučení zaměstnanců, změnu vedení jednotlivých procesů a rovněž mu musí předcházet analyzování, důsledné testování, odborné nasazení a důsledná podpora. Což v důsledku vede opět na bod 1.
4. **Rozmanitost zařízení** - Pokud se nebavíme o podniku, kde je všem zaměstnancům zakoupen totožný model chytrého telefonu, ale o tzv. BYOD (Bring Your Own Device), kdy zaměstnanci používají ve firemním prostředí svá vlastní zařízení, je třeba vytvořit takový systém, který si poradí s různými typy a verzemi OS zařízení, tablety, telefony i notebooky. Rovněž se liší spektrum aplikací používaných na jednotlivých zařízeních. S rostoucí rozmanitostí zařízení rovněž vznikají vyšší nároky na bezpečnost, které jsem se rozhodl věnovat následující kapitolu.

Pokud na tomto místě někoho napadlo využívání mobilních zařízení k účelům naprosto nevhodným v pracovním prostředí, pak bych rád upozornil, že nedostatečná morálka zaměstnanců není důvodem k zamítnutí této technologie, ale spíše k napomenutí či eliminaci dotyčného zaměstnance (v krajním případě). Samozřejmě takovým jevům zabránit nelze, ale nejedná se o problém EMM.

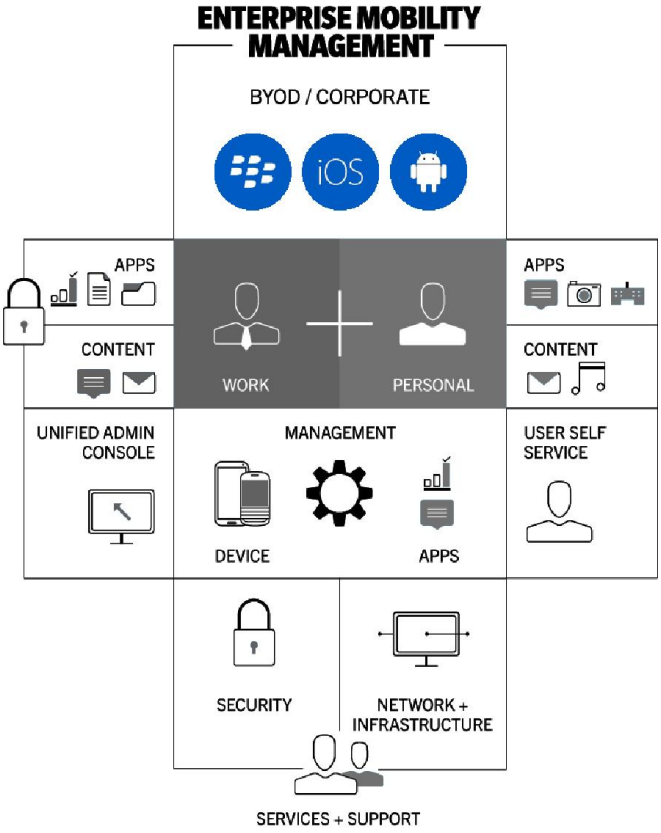
Bezpečnost

Při použití mobilních zařízení je třeba dbát na bezpečnostní stránku systému daleko více než při použití klasických počítačů. Jedním z důvodů může být už jen fakt, že přijít o mobilní zařízení je daleko snažší, ať už se jedná o zapomenutý mobilní telefon nebo ukradený notebook. Dalšími podstatnými aspekty bezpečnosti jsou citlivost dat a zabezpečení bezdrátové komunikace zařízení. Všechna zmíněná hlediska budou rozebrána v následujících odstavcích.

Základní přístupy

BYOD - Zaměstnanci používají v práci vlastní zařízení. Netýká se to jen mobilních telefonů a tabletů, ale třeba i notebooků. Tento přístup klade větší nároky na bezpečnost, neboť je třeba oddělit firemní data od dat zaměstnance. Nejčastější je tak využití tenkých klientů či přímo webových služeb, u kterých se data do zařízení zaměstnance nedostanou a jsou bezpečně uložena na firemním serveru.

Poskytnutí zařízení zaměstnavatelem - V takovémto případě je třeba zařízení kompletně zabezpečit. Předpokládá se, že většinu dat na zařízení tvoří firemní (a tedy citlivá data). Přístup limitovaný různými úrovněmi oprávnění v rámci firemní struktury je základním předpokladem. Stejně tak i šifrování dat odpovídající jejich citlivosti.



Jak ukazuje obrázek výše, je třeba při použití mobilních zařízení striktně oddělit pracovní a osobní data, aplikace a další obsah v zařízení. Pokud zaměstnanec používá vlastní zařízení, je třeba počítat s tím, že jej bude využívat i k jiným než pracovním účelům.

Firemní obsah je proto třeba náležitě zabezpečit, aby nemohlo dojít k jeho odcizení a zneužití. V případě aplikací je problém řešitelný zavedením autentifikace uživatele, obvykle jeho přihlášením pomocí firemního účtu. V případě zabezpečení dat je problém obecně složitější. Musí být zajištěn jednotný přístup k zařízením zaměstnanců a jejich kontrola, aby se případným problémům předešlo. A veškerá firemní data je třeba šifrovat, aby nemohlo dojít k jejich vynesení mimo domovskou společnost.

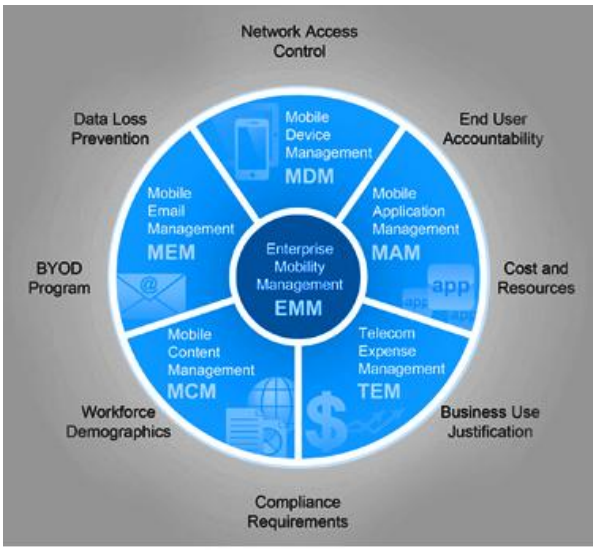
Rovněž je potřeba zajistit šifrování veškeré firemní komunikace, která by mohla vést k nechtěnému úniku informací. Obecně je zajištění bezpečnosti dat v mobilních zařízeních problematické, neboť přísná kontrola zařízení může vést k zásahu do soukromí zaměstnance. Přílišné zásahy a přehnaná kontrola ze strany zaměstnavatele pak mohou vést k tomu, že se zaměstnanec cítí sledován na každém kroku. V důsledku tak vzniká neochota používat mobilní zařízení pro jiné než soukromé účely, což v extrému eliminuje jakýkoli přínos EMM.

V rámci zabezpečení přístupu je třeba dbát i na spolehlivost zařízení. Různí výrobci a různé OS obsahují přímo v zařízení/software určitý stupeň zabezpečení (Blackberry, Samsung Knox). Zatímco s telefonem značky Blackberry vybaveným čtečkou otisků prstů a speciálním šifrovacím SW bude zabezpečení relativně jednoduché. U zařízení na platformě android od neznámého čínského výrobce, na kterém si uživatel navíc provedl root může být situace trochu složitější.

Co dále patří pod EMM

Ačkoli je bezpečnost velmi podstatnou otázkou, skládá se EMM i z jiných částí, které se bezpečnosti týkají méně nebo více. Rád bych tedy udělal malý výčet těchto podoblastí EMM s krátkým popisem.

	• **MDM -** Správa mobilních zařízení jako takových. Zastřešující všechny typy



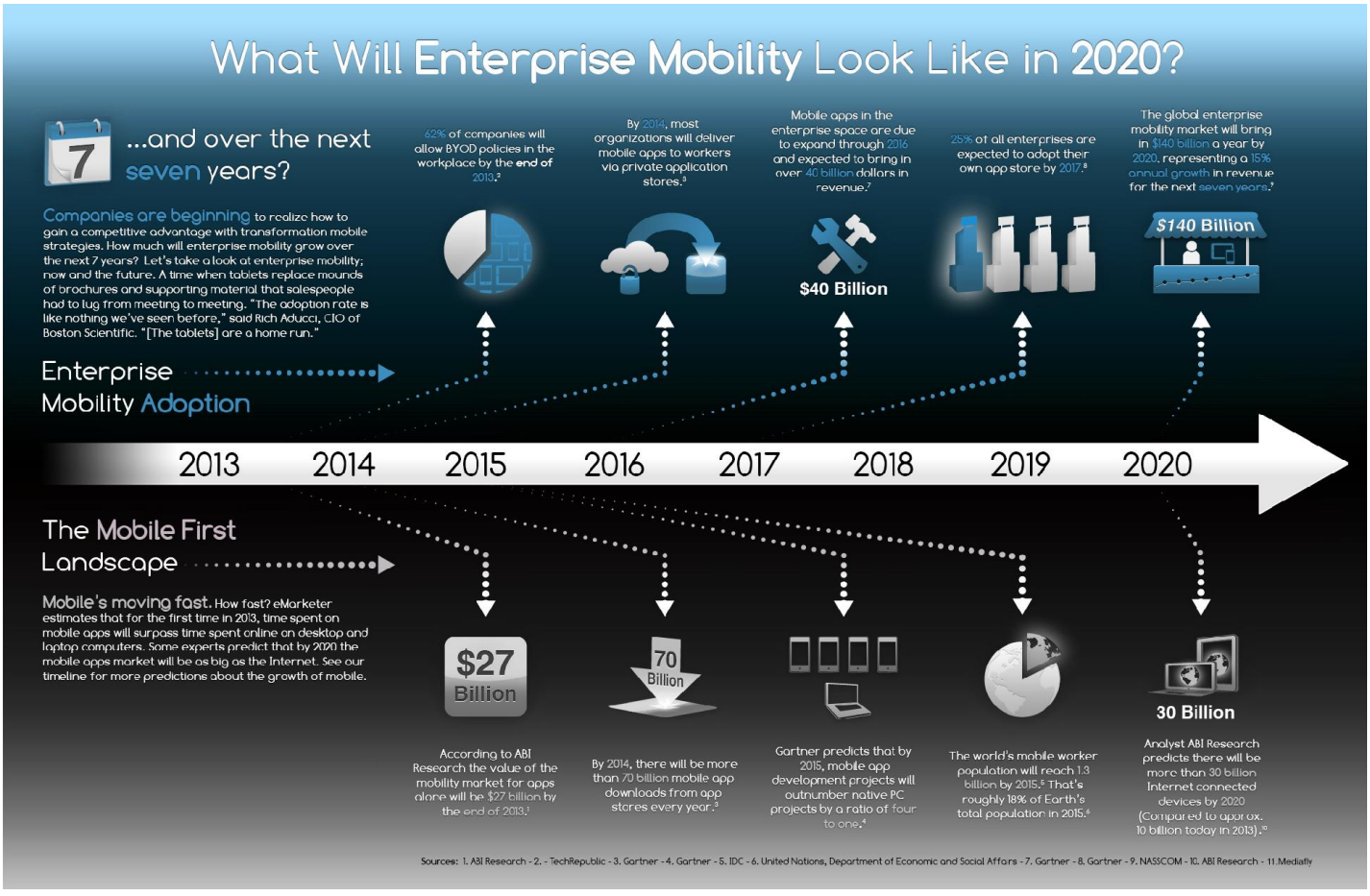
Source: Globo PLC

zařízení a OS. Řeší zabezpečení fyzických zařízení, uložení dat na zařízeních nebo například dálkové zablokování zařízení či smazání jeho obsahu.

- **MAM** - Správa aplikací, zejména tvorba a údržba firemních aplikací pro přístup k ostatním systémům (včetně např. CRM). A zajištění bezpečnosti takového přístupu.
- **TEM** - Správa výdajů za telekomunikační služby. I když je využití individuální, je potřeba jednotné řešení pro celý podnik.
- **MCM** - Určuje míru firemního obsahu, ke kterému je možné z daného zařízení přistupovat. (*Co lze vynést mimo firmu*). Rovněž řeší kontrolu a případné odstranění takových dat.
- **MEM** - Správa firemní pošty. Opět je kladen důraz na zabazpečení přenosu i dat. Zároveň je třeba umožnit pohodlnou práci s poštou srovnatelnou s klasickým klientem.
- V obrázku je dále vidět, jaké činnosti spadají pod jednotlivé součásti EMM.

Závěr

Závěrem bych ještě rád uvedl několik předpovědí pro vývoj EMM do budoucna.



A vcelku zajímavá infografika z veletrhu CeBit 2014, kde bylo jedním z hlavních témat i mobile.

Zdroje

Indická společnost zabývající se vývojem webů a mobilních aplikací:

http://www.srishtis.com/blog/embracing-enterprise-mobility-management/

Pohled Blackberry na EMM:

http://us.blackberry.com/enterprise/solutions/emm.html

Úryvek z článku zabývajícího se EMM:

http://www.slideshare.net/professorbanafa/challenges-and-trends-in-enterprise-mobility-management

Společnost zabývající se vývojem EMM řešení na míru:

http://www.mobileforcesoftware.com/future-state-enterprise-mobility/