Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Nasazení mobilních zařízení do firemního prostředí se zaměřením na iOS zařízení

Bc. David Marek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. David Marek

Informatika

Název práce

Nasazení mobilních zařízení do firemního prostředí se zaměřením na iOS zařízení

Název anglicky

The deployment of mobile devices into the corporate environment focused on iOS devices

---

Cíle práce

Diplomová práce je zaměřena na problematiku začlenění mobilních zařízení do podnikové struktury. Hlavním cílem práce je představit nasazení mobilních zařízení do firemního prostředí se zaměřením na iOS zařízení. Dílčím cílem práce je provést analýzu trhu sledované problematiky a definovat pojmy z oblasti mobilních zařízení a jejich business zařazení. Dalším dílčím cílem je uvést možnosti správy a nutné zabezpečení pro využívání mobilních zařízení ve firemním segmentu. Práce bude směřována převážně na případovou studii nasazení iOS zařízení ve fiktivní společnosti. Studie bude obsahovat určení požadavků společnosti, výběru platformy zařízení, implementace a nasazení, aplikací a samotné využití včetně zahrnutí všech úskalí, které mohou nastat. Na závěr práce bude provedeno zhodnocení a diskuze současné situace včetně shrnutí s doporučeními pro implementaci mobilních technologií do firemního prostředí.

Metodika

Zpracování řešené problematiky se nejdříve věnuje analýze trhu s mobilními zařízeními, určení základních pojmů z oblasti řešené problematiky a bezpečnostním prvkům na základě informačních zdrojů. Studie možností správy zařízení je založena na dostupných řešeních, která splňují základní požadavky společností. Základní teoretická východiska jsou použita ve vlastním řešení případové studie, která bude zpracována v jednotlivých krocích od vývoje k nasazení mobilních zařízení ve fiktivní společnosti a využití na základě praktické znalosti z oboru řešené problematiky. Závěrečné zhodnocení a výsledná doporučení budou vycházet ze zkušeností získaných ve vlastním řešení práce a současným využitím teoretického základu z úvodní části práce.

Doporučený rozsah práce

50 – 60 stran

Klíčová slova

Mobilita, tablet, iOS, Mobile Device Management, zabezpečení, firemní prostředí, VPN, správa

---

Doporučené zdroje informací

CAMPAGNA, Rich, Subbu IYER a Ashwin KRISHNAN. Mobile device security for dummies. Chichester: John Wiley [distributor], 2011, xviii. ISBN 04-709-2753-4

DOHERTY, Jim, Mike CHAPPLE, David SEIDL a Sean-Philip ORIYANO. UNIVERSITY OF NOTRE DAME MIKE CHAPPLE. Wireless and mobile device security. Boston: Jones & Bartlett Learning, 2014. ISBN 12-840-5928-6

FINCH, Patrick. Mobile device management 35 Success Secrets – 35 Most Asked Questions On Mobile device management – What You Need To Know. Emereo Publishing, 2014. ISBN 9781488537882

JOHNSON, Michael. Mobile Device Management: What you Need to Know For IT Operations Management. Emereo Publishing, 2012. ISBN 978-1743042151

WELCH, John. IOS in the Enterprise: A hands-on guide to managing iPhones and iPads. San Francisco: Peachpit Press, 2011. ISBN 9780132736022

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 23. 03. 2017

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Nasazení mobilních zařízení do firemního prostředí se zaměřením na iOS zařízení" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 28. 3. 2017 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D, za vedení této diplomové práce, cenné rady, odborné konzultace a vstřícné jednání.

Nasazení mobilních zařízení do firemního prostředí se zaměřením na iOS zařízení

Souhrn

Cílem práce je představení problematiky začlenění mobilních iOS zařízení do firemního prostředí.

Teoretická východiska práce poskytují náhled do zkoumané tématiky definováním vybraných pojmů, platforem mobilních zařízení, jejich zabezpečení a aplikací. Dále je teoretická část práce zaměřena na klíčovou oblast diplomové práce, kterou je správa mobilních zařízení. V bližším detailu jsou představeny vybrané Enterprise Mobility Management platformy a zajímavé prostředky společnosti Apple.

Vlastní část práce krok za krokem provádí procesem začlenění iOS zařízení do fiktivní společnosti. Proces začlenění je založen na jednotlivých krocích, které mají logickou návaznost počínaje určením společnosti a jejich požadavků, přes vývoj, nasazení až po používání Enterprise Mobility Management nástrojů vč. zahrnutí vzniklých úskalí. Vybraná fiktivní společnost je situována do oblasti letectví, kritické v ohledu bezpečnosti a některých specifických požadavcích. Práce shrnuje poznatky z výběru, implementace a využívání EMM nástroje s ohledem na iOS zařízení v této fiktivní společnosti a přináší doporučení.

Klíčová slova: mobilní zařízení, mobilita, správa mobilních zařízení, mobilní platformy, Apple, iOS, Mobile Device Management, Enterprise Mobility Management, AirWatch, MobileIron

The deployment of mobile devices into the corporate environment focused on iOS devices

Summary

The aim of the Master thesis is to introduce issues of the integration of iOS mobile devices into the company environment.

The theoretical basis of the thesis provide insight into the investigated theme by defining selected terms, platforms of the mobile devices, their security and applications. Theoretical part is also focused on the key section of the Master thesis, which is management of the mobile devices. In closer detail are introduced selected Enterprise Mobility Management platforms and interesting tools of Apple enterprise.

Own part of the thesis follows step by step the process of the integration of iOS devices into the fictive company. The process of integration is based on individual steps, which are logically linked, starting by recognizing of the company and its requirements, through the development, implementation to the usage of the Enterprise Mobility Management tools including involvement of arising difficulties. The fictive company is situated into the aviation field, which is critical in matter of security and some other specific requirements. The thesis summarises information from the selection, integration and utilization of the EMM tool considering iOS devices in this fictive company and brings recommendations.

Keywords: mobile device, mobility, management of mobile devices, mobile platforms, Apple, iOS, Mobile Device Management, Enterprise Mobility Management, AirWatch, MobileIron

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

AD – Active Directory

BES – BlackBerry enterprise service/server

BIS – BlackBerry internet service

BBM – BlackBerry messenger

BYOD – Bring Your Own Device

CAL - Client Access License

DEP – Device Enrollment Program (Apple)

DMZ - Demilitarized Zone

EAS - Exchange ActiveSync

EFB - Electronic Flight Bag

EMM – Enterprise Mobility Management

HW – Hardware

MD – Man day

MDM – Mobile Device Management

MAM – Mobile Application Management

MCM – Mobile Content Management

MS - Microsoft

PC – Personal Computer

PDA - Personal Digital Assistant

VSP - Virtual Smartphone Platform (MobileIron)

VPP - Volume Purchase Program (Apple)

WP – Windows Phone

1 Úvod

Historie mobilních zařízení započala v roce 1973 prvním funkčním prototypem mobilního telefonu od společnosti Motorola. Takzvaný „brick phone“, první komerčně dostupný mobilní telefon Motorola DynaTAC 8000x, vážil téměř jeden kilogram a měl délku přibližně 30 cm bez délky antény.[2]

První skutečný tablet tak, jak je chápán dnes, byl představen v roce 1956. Rok 1985 přinesl první komerčně dostupné tablety, modely společností Pencept a CIC s operačním systémem MS-DOS.[3]

Vývoj v oblasti mobilních technologií za posledních několik let urazil velmi dlouhý kus cesty. Stále se posouvají limity zařízení a z dříve pouze tlačítkových telefonů sloužících k psaní textových zpráv, volání, organizaci kalendáře či poznámek se stávají plnohodnotné vysoce výkonné stroje, schopné konkurovat v některých ohledech klasickým PC a notebookům. Jedním z příkladů může být tablet s operačním systémem Windows, který je plnohodnotnou náhradou klasických notebooků.

Mobilní technologie vstupují do soukromých životů v různých podobách, od telefonů, přes tablety až po přenosné PC po chytré domácnosti. V moderní společnosti je trendem smartphone nebo tablet vlastnit a tento požadavek se objevuje také ve firemním segmentu.

Firemní oblast je zasažena už několik let vzrůstem užívání smartphonů a tabletů v podobě vlastních zařízení zaměstnanců, nebo jako vlastních firemních nástrojů. V okamžiku kdy ve firemním prostřední bude zavedena mobilní technologie, která bude určena pro zpracování a uchovávání firemních dat, je nezbytné nastavit dostatečné bezpečnostní politiky a procesy pro jejich zařazení.

Nasazením mobilních zařízení do společnosti se zabývá každé IT oddělení, řeší problematiku různými způsoby dle svých možností. Velký tlak musí ustát zejména ze strany požadavků zaměstnanců a jejich zkušeností ze soukromých životů, které se snaží prosadit ve společnosti tak, aby mohli používat svůj oblíbený smartphone pro pracovní účely.

Je alarmující, že v některých společnostech není tato problematika vyřešena a nefungují základní principy a procesy. Hrozba úniku informací, ztráty dat při odchodu zaměstnance nebo při pouhém zcizení přístroje je vysoká.

Cílem práce je přinést obecný náhled na současný stav mobilních technologií a jejich řešení ve firemním prostředí. Část práce se bude věnovat případové studii orientované na konkrétní případ nasazení iOS zařízení do fiktivní společnosti.

2 Cíl práce a metodika

2.1 Cíl práce

Diplomová práce je zaměřena na problematiku začlenění mobilních zařízení do podnikové struktury.

Hlavním cílem práce je představit nasazení mobilních zařízení do firemního prostředí se zaměřením na iOS zařízení. Dílčím cílem práce je provést analýzu trhu sledované problematiky a definovat důležité pojmy z oblasti mobilních zařízení a jejich business zařazení. Dalším dílčím cílem je uvést možnosti správy a nutné zabezpečení pro využívání mobilních zařízení ve firemním segmentu. Práce bude směřována převážně na případovou studii nasazení iOS zařízení ve fiktivní společnosti. Studie bude obsahovat určení požadavků společnosti, výběru platformy zařízení, implementace a nasazení, aplikací a samotné využití včetně zahrnutí všech úskalí, které mohou nastat. Na závěr práce bude provedeno zhodnocení a diskuze současné situace včetně shrnutí s doporučeními pro implementaci mobilních technologií do firemního prostředí.

2.2 Metodika

Zpracování řešené problematiky se nejdříve věnuje analýze trhu s mobilními zařízeními, určení základních pojmů z oblasti řešené problematiky a bezpečnostním prvkům na základě informačních zdrojů.

Studie možností správy zařízení je založena na dostupných řešeních, která splňují základní požadavky společností. Základní teoretická východiska jsou použita ve vlastním řešení případové studie, která bude zpracována v jednotlivých krocích od vývoje k nasazení mobilních zařízení ve fiktivní společnosti a využití na základě praktické znalosti z oboru řešené problematiky. Závěrečné zhodnocení a výsledná doporučení budou vycházet ze zkušeností získaných ve vlastním řešení práce a současným využitím teoretického základu z úvodní části práce.

3 Teoretická východiska

Nasazení mobilních zařízení do firemního prostředí zahrnuje znalost důležitých pojmů z této oblasti, porovnání jednotlivých platforem, zabezpečení, pro firemní segment důležité aplikace. Samostatnou část zaujímají možnosti správy, které lze rozdělit na vlastní možnosti a konkrétní řešení Mobile Device Management.

3.1 Pojmy

Určení základních pojmů je důležité pro náhled a pochopení řešené problematiky. V rozsahu práce není možné definovat všechny známé pojmy na poli mobilních zařízení. Kapitola se věnuje často diskutovaným pojmům, na které je možné v tomto segmentu narazit a také pojmům, které jsou v dalších částech práce používány.

3.1.1 Mobilní zařízení

Mobilní zařízení lze definovat jako přenosné bezdrátové výpočetní zařízení, mající vlastní napájení pomocí baterie, převážně dotykový displej, v některých případech opatřený klávesnicí a vážící méně než 1 kg. Výhodou tabletů by měla být delší výdrž na baterii, snadná přenositelnost, rychlost operačního systému.[4]

Do skupiny mobilních zařízení spadají jak smartphony, tak tablety. Skupina ale není omezena pouze na tyto zařízení. Patří sem také například mobilní terminály z oboru logistiky, čtečky knih, ne další specifická zařízení PDA.

Tablety jsou stejně jako notebooky navrhnuty na přenášení. Největší rozdíl je v absenci hardwarové klávesnice a dotykové obrazovce. Lze tak psát na virtuální klávesnici a pomocí dotyku prstu ovládat funkce zařízení. Někteří uživatelé nemohou plně přejít na tablety, primárně používají notebook nebo desktop, tablet plní roli druhého počítače. Některé rozdíly mezi notebooky a tablety se dnes snižují, notebooky mají dotykové obrazovky, k tabletům je možné připojit bezdrátové HW klávesnice. Vznikají kombinace, notebook, respektive Tablet PC, který působí jako klasický notebook, ale dotykovou obrazovku lze odpojit a použít ji samostatně jako tablet.

Tablet je vhodný pro pracovníky v terénu, pro práci na cestách a konferencích, ne vždy je ale dostatečný pro nahrazení klasického notebooku, jeho výpočetního výkonu, odolnosti a HW klávesnice.[5]

3.1.2 BYOD

Používání vlastních soukromých zařízení zaměstnanců ve firemním prostředí s sebou nese pojem BYOD. Bring Your Own Device (BYOD) je vzrůstajícím trendem, který znamená, že si zaměstnanci mohou nosit svá soukromá zařízení (jako jsou notebooky, smartphony, tablety) do firemního prostředí. BYOD zvyšuje tlak na bezpečnost, kterou sám o sobě velmi znesnadňuje a vytváří rozpor mezi bezpečností, produktivitou a pohodlím zaměstnanců.[6]

Jednotlivé hrozby BYOD zařízení [7]:

- autorské právo,
- licence,
- sektorová regulace,
- ochrana osobních údajů,
- obchodní tajemství, důvěrnost,
- pracovněprávní aspekty.

Problematika užívání BYOD zařízení se řídí převážně následujícími zákony:

- zákonem č. 89/2012 Sb., občanským zákoníkem (NOZ), kterým jsou upraveny vztahy mezi podnikatelem a jeho zákazníky,
- zákonem č. 121/2000 Sb., o právu autorském (AZ), který se aplikuje na užívaný software,
- zákonem č. 262/2006 Sb., zákoník práce (ZP).

Zavedení BYOD musí předcházet pečlivá příprava skládající se z nastavení pravidel pro užívání BYOD zařízení zaměstnanci a identifikace rizik pro dostatečnou prevenci. Příprava zahrnuje několik základních nastavení pravidel [8]:

- zabezpečení přístupu k BYOD zařízení, provedením vyžadovaného hesla pro přístup do zařízení,
- zavedení platnosti přístupového hesla,
- vynucením časového limitu při nečinnosti zařízení, po kterém dojde k zamčení zařízení,
- použití zabezpečených šifrovaných přenosových kanálů,
- zásady pravidelné aktualizace operačního systému,

- vymezení jaké aplikace budou přes BYOD zařízení dostupná a jaká firemní data budou zařízení dostupná,
- nastavení politiky zálohování dat,
- souhlas uživatele vlastnící BYOD zařízení pro kontrolu a zásahy do zařízení, provádění změn nastavení a také souhlas s možným vzdáleným smazáním zařízení a možnému smazání soukromých dat,
- souhlas uživatele se zpracováním osobních údajů.

Velmi důležitou oblastí před povolením BYOD zařízení, je uzavření dohody mezi zaměstnancem a zaměstnavatelem ohledně závazku o dodržování nastavených pravidel BYOD. Nastavená pravidla musí být následně prosazována a kontrolována.[8]

Při identifikaci rizik by mělo dojít k zmapování procesů, u kterých může nastavení BYOD ovlivnit vztahy a cíle společnosti, musí být zajištěn plán pro hrozby plynoucí z BYOD zařízení, například odcizení. Zavedením BYOD se očekává zvýšení flexibility zaměstnanců, kdy je umožněn kontinuální přístup k pracovním aplikacím a službám v ideální čas pro zaměstnance. Ten tak může pracovat kdykoliv a odkudkoliv v čase, který mu vyhovuje. BYOD je také spojován se snížením nákladů, v případě nákupu zařízení jsou náklady sdíleny a firemní zdroje jsou šetřeny. Provozní náklady lze ročně snížit o 18 až 20 procent.[9] [10]

Zavedením politik BYOD není cílem zaměstnance odradit, nastavit politiky složité, naopak je žádoucí velmi jednoduchá a pochopitelná politika, tak aby byla co nejlépe přijata, když už se společnost pro povolení BYOD rozhodne. Pro oddělení IT je největší hrozbou zařízení připojené do firemní sítě, k firemním aplikacím nebo službám, o kterém neví.[11]

3.1.3 CYOD

Pojem CYOD (Choose Your Own Device) vyjadřuje další z modelů vlastnictví a používání mobilních zařízení ve firemním segmentu. Organizace používá model CYOD, pokud svým zaměstnancům nabízí pro práci výběr zařízení, na místo vydávání jediného telefonu nebo tabletu. CYOD je obecně spojován s označením COPE, který je dále vysvětlen. Strategie CYOD se soustředí na požadavky zaměstnanců, kteří chtějí používat zařízení, která si vyberou sami ze zadané firemní nabídky. [12]

3.1.4 COPE

Další model použití mobilních zařízení ve firemní oblasti je označován COPE (Corporate-Owned, Personally-Enabled). Princip fungování COPE spočívá v tom, že mobilní zařízení vlastní společnost, ale je povoleno zaměstnancům používat mobilní zařízení pro osobní aktivity. S COPE má uživatel větší flexibilitu, než například s modelem COBO, ale společnost má stále pod kontrolou bezpečnost, náklady a další potenciální rizika z právní a personální oblasti.[12], [13]

COPE a CYOD

Pokud je zaměstnancům nabídnut model COPE doplněn o CYOD, je velká pravděpodobnost, že u zaměstnanců nová strategie bude přijata s úspěchem. Nevýhodou takového nasazení je požadavek zaměstnanců na nejnovější a „trendy“ přístroje, který zvyšuje náklady na pořizování takových přístrojů. Oproti nákladům na nákup požadovaných zařízení je možné vyčíslit náklady za potenciální ztrátu dat z nezajištěných soukromých zařízení. Volba strategie COPE / CYOD znamená pro organizaci dlouhodobou strategickou investici. Dává do rukou zaměstnance prostředek, který je pohodlný pro práci, a tím se zvyšuje produktivita a výkonnost. To všechno v souladu s bezpečnostní politikou organizace. Navíc pokud společnost bude dodržovat pravidelné cykly obnovy zařízení, bude moci využít stále rostoucí výpočetní výkon nových zařízení, pro zvýšení škály aplikací a služeb, které budou moci zaměstnanci využít.[14]

3.1.5 COBO

Model COBO (Corporate Owned Business Only) byl jedním z prvních z řady modelů v přístupu k mobilním zařízením v organizacích. Uživatelé od společnosti dostanou přidělené mobilní zařízení s omezením použití pouze pro firemní účely. Často si taková zařízení nemohou zaměstnanci ani vybrat. Tento model nenásleduje požadavky uživatelů na flexibilitu a využívání jediného zařízení pro firemní i soukromou oblast. COBO je model zastaralý, využívaný převážně u společností, které nenásledují současné trendy a nejsou příliš striktní na bezpečnost. Neznamená to, že v některých společnostech stále nemá model COBO své opodstatnění. Tento model mohou ocenit uživatelé, používající firemní mobilní zařízení pouze jako pracovní nástroj, a kteří chtějí striktně oddělit práci a soukromý život.

Model COBO se zdá z hlediska bezpečnosti a správy dat nejméně rizikový, nicméně uživatel, který není spokojený, se bude snažit najít řešení, které mu bude vyhovovat a v důsledku toho často dochází k převracení modelu COBO zpět na BYOD.[12]

3.1.6 Cloud

Obecně se uvádí definice pojmu cloud computing.

„Cloud computing je model, který je přístupný bez omezení a překážek na základě vyžádání uživatele. Uživatel má přístup ke sdíleným konfigurovatelným výpočetním zdrojům (jako například sítě, servery, uložiště, aplikace a služby). Zdroje jsou k dispozici velmi rychle a to s minimální nutnou správou nebo interakcí poskytovatele služby.“[15]

Pro účely mobilních zařízení je důležité zmínit pouze část, a to cloudovou službu datových úložišť (webových disků).

Cloudových úložišť existuje několik, přičemž řada velkých společností jako Google a Microsoft mají vlastní řešení. Mezi nejznámější veřejná cloudová úložiště patří OneDrive, Google Drive, Dropbox, MEGA, BOX. Poskytovatel dává k dispozici vyhrazený prostor, kam je možné ukládat data, součástí jsou pak aplikace pro přístup k úložišti, pro nahrávání dat, synchronizaci a pro celkovou práci s daty a úložištěm. Aplikace mohou být mobilní nebo pro PC.[16] [17]

Z pohledu firemního řešení by měla být upřednostněna varianta privátního cloudového úložiště, ta by měla být určena pro účely ukládání citlivých firemních dat. Ostatní veřejná řešení přinášejí vyšší riziko kompromitace dat.

Uživatelé mobilních zařízení by měli být seznámeni s rozdílem privátního a veřejného cloudu.[18]

Velmi zajímavou variantou je užívání licencí Office 365, tedy plánu, který zahrnuje také prostor 1TB úložiště OneDrive, pro firmy, pro každého uživatele.[19]

Cloudová úložiště mají největší výhodu v dostupnosti odkudkoliv, kde je dostupné připojení do internetu a nejen na mobilním zařízení. Je možné si určité složky sdílet a synchronizovat mezi klasickým počítačem a mobilním zařízením.

3.1.7 EAS – Exchange ActiveSync

Možnosti správy zahrnují jako jednu z možností protokol Active Sync a zjednodušenou správu zařízení pomocí MS Exchange. Protokol Exchange ActiveSync (EAS) prodělává každou změnou verze (od verze 2003 do 2010) a s každým service packem MS Exchange změny a přidává další možnosti správy zařízení. Zařízení spravovaná tímto protokolem mohou být na platformě nejen Windows Mobile, ale také iOS a Android. Správa zařízení pomocí EAS je také závislá na samotném zařízení, tedy klientovi. EAS umožňuje administrátorům několik operací nad samotnými zařízeními. Lze získat Device Status, informaci o zařízení, lze rušit partnerství se zařízením bez kompletního smazání zařízení a lze například celé zařízení na dálku smazat – takzvaný WIPE zařízení. Administrátor také může obnovovat heslo k zařízení, případně používat retrieve log. EAS také umožňuje vynutit šifrování, manual sync při roamingu.

Správci mobilních zařízení mohou používat pro správu Exchange Management konzoli nebo přímo Exchange Management Shell – Power Shell. [20]

Jde o koncept umožňující hromadně vynutit bezpečnostní politiku pro všechna zařízení připojující se k firemnímu emailu. Nespornou výhodou je licenční pokrytí vzhledem k WS CAL a Exchange Server CAL. [21]

3.1.8 EMM – Enterprise Mobility Management (MDM, MAM a MCM)

EMM je kompletní řešení pro správu mobilních zařízení, správu aplikací a přístupu k firemním datům pro mobilní zařízení. EMM integruje mobilní zařízení do firemní infrastruktury a z části ho lze chápat také jako IT strategii, kterou je nutné správně analyzovat a poté implementovat pomocí vhodného nástroje. [22]

EMM se skládá z:

- MDM - Mobile Device Management
- MAM - Mobile Application Management
- MCM - Mobile Content Management

MDM je nástroj správy mobilních zařízení pro zajištění plné kontroly nad mobilními zařízeními s různými OS ve firemním prostředí. Tento pojem se uvádí nejčastěji ve vazbě ke správě mobilních zařízení, z části může zaujmout i pozici MAM a MCM. MDM je platforma pro pokročilou správu mobilních zařízení. Řešení umožňuje kroky nutné

k zabezpečení, monitorování, správě aplikací (doplněné o MAM) a zajištění přístupů k firemním prostředkům (email, dokumenty). MDM slouží jako jeden z hlavních pilířů bezpečnostní politiky mobilních zařízení. Centralizovaná správa, hromadné rozesílání konfiguračních profilů a správa aplikací je přínosem pro správce systému i koncové klienty. MDM umí prosazovat bezpečnostní politiky podle typů platforem zařízení, umí instalovat aplikace z vlastních firemních aplikačních portálů a spravovat podnikový obsah (email, dokumenty). [21] [22] [23]

Významnou problematikou MDM řešení a převážně doručovaných konfigurací je omezenost ze strany platformy zařízení. Ačkoliv jsou v dnešní době MDM řešení velmi vyspělá a dokáží do zařízení doručit různé restrikce, omezení či bezpečnostní pravidla, stále je tu nutná závislost na tom, jaké restrikce vydavatel platformy umožní spravovat. Jako vhodný příklad poslouží platforma Apple. Ačkoliv, v dnešní době je iOS restrikcí pro konfigurační profil mnoho, chybí zde například omezení automatického update systému, který v první verzi může mít až katastrofální dopad na koncové klienty (například nefunkční NTML v Safari). Tuto restrikci Apple nepovoluje nastavit a MDM řešení nemá způsob jak tuto situaci obejít, než pouhým informováním zaměstnanců, o nepovolení aktualizace.

MAM slouží pro správu aplikací, spravuje životní cyklus aplikace od vytvoření po její publikaci přes firemní aplikační portál. Aplikace firemního charakteru lze uzavřít do zabezpečeného kontejneru a v případě porušení bezpečnostních pravidel lze tento kontejner bezpečně odebrat.[22]

MCM slouží pro správu dokumentů přenášených přes email, uložených na síťových discích nebo Sharepointu, případně jiných uložištích.[22]

Všechny části EMM jsou propojeny a nejčastěji řešeny jediným nástrojem, a tak se některé části správy prolínají.

3.1.9 PIM

PIM je označení pro software, který organizuje a řídí informace pro rychlé vyhledávání na každodenní úrovni. Poskytuje kombinaci funkcí, včetně telefonního seznamu, kalendáře a plánovače.[24]

Standardní PIM software zahrnuje plánovač pro události, adresář kontaktů a seznam úkolů. Dále mohou být součástí také e-maily, textové poznámky (i hlasové poznámky)

a upomínky. Některé mobilní zařízení umožňují synchronizaci PIM dat s PC nebo přes webové služby.[25]

PIM spravuje, organizuje, ukládá a načítá podniková data tak, aby zaměstnanci plnili své povinnosti efektivně. Pracovníci tak využívají svůj čas na zpracování informace, nikoliv na její zdlouhavé hledání. Jedním z příkladů správce osobních informací (PIM) je Microsoft Outlook, dostupný jak pro PC, tak dnes již také na mobilní platformy.[26]

Označení PIM nesou také mobilní aplikace, které poskytují firemní e-mail, kalendář a kontakty, ale typicky poskytují zabezpečení a možnosti správy funkcí, které samotné nativní aplikace, typu e-mailový klient, mohou postrádat. Přestože klesá míra používání PIM aplikace organizacemi než v minulých letech, jsou tyto PIM aplikace častým požadavkem u společností s vysokým požadavkem na zabezpečení, jako jsou společnosti z oboru financí, zdravotnictví nebo veřejného sektoru.[27]

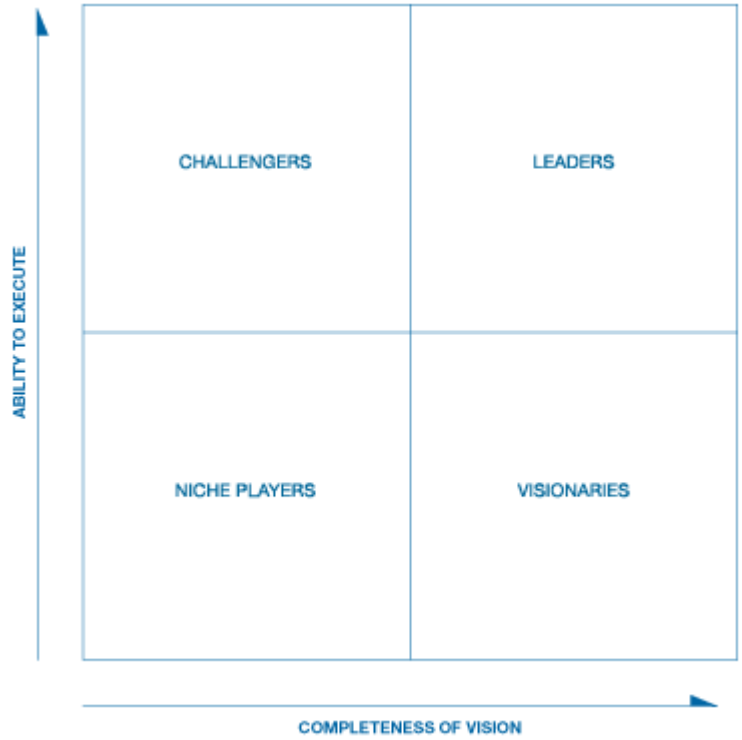
3.1.10 Gartner magický kvadrat

Magický kvadrant společnosti Gartner často zaznívá při výběru informačních technologií jako jeden z důležitých zdrojů informací.

Společnost Gartner, která magické kvadranty vytváří, se zabývá výzkumem a poradenskou činností v oblasti informačních technologií. Je přední společností v tomto oboru, poskytující náhled na informační technologie, který je důležitým zdrojem pro správná rozhodnutí klientů.[28]

Magický kvadrant je grafickým výsledkem výzkumu určitého trhu, provedený na základě jednotného souboru hodnotících kritérií, které se mohou s vývojem trhu měnit. Magický kvadrant zobrazuje postavení soutěžících dodavatelů, a pomáhá klientům určit, jak dobře tito poskytovatelé určité informační technologie realizují vytyčené vize, a jak dobře si vedou oproti výhledu společnosti Gartner na daném trhu. [29]

Magický kvadrant dělí dodavatele, kteří mezi s sebou soutěží, do čtyř oblastí, takzvaných kvadrantů.



Obrázek 1 - Magický kvadrant Gartner [29]

Lídři (Leaders) – dodavatelé, jejichž současné vize jsou ve výhodné pozici pro budoucí požadavky trhu. [30], [31]

Visionáři (Visionaries) - mají správný pohled na vývoj trhu (stejný jako má výzkum společnosti Gartner), ale není u těchto dodavatelů zřejmé, zda budou schopni dodávat na trh řešení shodné s jejich vizí. [30], [31]

Specializovaní hráči (Niche Players) – dodavatelé, kteří se soustředí na určitý segment, určitou funkcionalitu řešení, z důvodu omezených schopností nebo jsou nově příchozí na trhu. Tito dodavatelé mají potenciál růst, ale také může nastat problém, kdy nebudou stíhat rozvoj daného trhu. [30], [31]

Vyzyvatelé (Challengers) – dodavatelé, kteří dnes prosperují a mohou dominovat velkým oblastem, ale neprokazují pochopení vize trhu. [30], [31]

Magický kvadrant by měl klient použít při rozmýšlení investic v daném segmentu a výběru správného řešení informační technologie v daném zaměření. Není však pravidlem, že pro všechny klienty jsou vhodnou volbou pouze lídři trhu. Jsou dobré důvody i pro oslovení dodavatelů z jiných částí kvadrantu, vyzyvatelé mohou být vhodní

i specializování hráči mohou být lepší volbou než lídři. Vždy záleží na tom, jak se dodavatel bude vyrovnávat s obchodními cíli klienta. [30], [31]

3.1.11 Visual privacy

Visual privacy je v pojetí této práce pojem z oblasti správy mobilních zařízení. Visual privacy zajišťuje transparentnost směrem k uživatelům, kteří používají spravované mobilní zařízení. Visual privacy zobrazuje uživatelům, jaká data zařízení může společnost vidět a jaké akce může společnost se zařízením vzdáleně provádět. Zavedení této komponenty do EMM řešení vede ke zlepšení důvěry uživatelů ke správě jejich zařízení, snižuje se propast v ohledu důvěry mezi uživatelem a IT oddělením, a celkově Visual Privacy urychluje zavádění nových služeb a programů podnikové mobility, například BYOD. Komponenta Visual Privacy se zpravidla uživatelům zobrazuje při registraci zařízení do EMM řešení, dále pak kdykoliv přes aplikaci klienta, včetně notifikací v případě aktualizace pravidel, které mají vliv na soukromí a vzdálené ovládání mobilního zařízení. [32], [33]

3.1.12 SDK

Software development kit (SDK) si lze představit jako programový balík poskytující sadu nástrojů určených pro vývoj software, pro nejrůznější mobilní aplikace na tablety nebo smartphony. To pomáhá vývojářům těžit ze zavedených funkcí v robustním SDK bez nutnosti vlastního kódování potřebných funkcionalit. Znamená to, že SDK je nutné použít při tvorbě aplikace a v podstatě zasahuje do vlastního kódu aplikace. Příkladem použití SDK je převedení stávající mobilní aplikace na zabezpečenou v rámci některého z EMM řešení. V souvislosti s SDK se často také objevuje pojem App Wrapping. Pro příklad u platformy iOS nelze App Wrapping použít u aplikací, které mají být distribuovány přes Apple AppStore, pro tento případ je nutné vždy použít SDK dané platformy EMM. App Wrapping tak získává význam u in-house, vlastních aplikací klienta nedistribuované přes Apple AppStore, kde lze App Wrapping použít. [34], [35]

Použití SDK může přinést, z pohledu správy mobilních zařízení, zajímavé funkce [34], [35]:

- doručování konfigurace aplikace přes EMM, se zablokováním změn uživatelem,
- automatické vytvoření VPN tunelu,
- ověření uživatele aplikace s potřebnými službami firemní infrastruktury,
- zapnutí DLP, šifrování,
- logování aplikace do EMM,
- zahrnutí aplikace do bezpečnostního kontejneru firemních aplikací.

3.1.13 App wrapping

V podkapitole SDK bylo v souvislosti s tímto pojmem také zmíněn App Wrapping mobilních aplikací. App Wrapping je prováděn také za účelem přidání dalších funkcionalit, zajištění vylepšeného zabezpečení mobilní aplikace, přidání ověřování nebo případně omezování funkcí aplikace. App Wrapping je možné přiblížit jako obalení původní aplikace dalším kódem, který zajišťuje potřebné funkce, které nejsou součástí této mobilní aplikace samostatně. App Wrapping je možné provádět jak ve vývojové fázi aplikaci, tak po dokončení vývoje a po vydání aplikace, a to je nespornou výhodou. Převážně pro společnosti, používající aplikace třetích stran, je App Wrapping možností, jak aplikaci doplnit potřebným kódem, bez nutnosti zásahu do zdroje. Vzniká tak další vrstva nad aplikací pro její řízení, bez ovlivnění vlastního kódu aplikace. Při použití App Wrappingu je nutné dbát na licenční ujednání výrobce mobilní aplikace, pro kterou se bude App Wrapping provádět a u iOS nesmí chybět certifikát, kterým se aplikace opatřená App Wrappingem znovu podepíše. Pro iOS je omezení provádět App Wrapping pouze pro in-house aplikace. [36], [37]

Použití App Wrappingu může přinést funkce [36], [37]:

- doručování konfigurace aplikace přes EMM, se zablokováním změn uživatelem,
- automatické vytvoření VPN tunelu,
- ověření uživatele aplikace s potřebnými službami firemní infrastruktury,
- zapnutí DLP, šifrování,
- zahrnutí aplikace do bezpečnostního kontejneru firemních aplikací.

3.1.14 Appconfig

Standard vzniklý jako AppConfig Community, je spojením významných subjektů na trhu EMM a mobility obecně, tedy spojením výrobců EMM s vývojáři a dodavateli aplikací pro mobilní zařízení. Cílem této komunity je zjednodušit vývojářům a zákazníkům řídit mobilitu v podnikání. Posláním komunity je zefektivnit nasazení mobilních firemních aplikací tím, že bude působit jako standard v přístupu ke konfiguraci a správě aplikací. Členové Appconfig společně pracují na zjednodušení implementace sady ovládacích prvků aplikací pro snadnou správu a konfiguraci v zájmu obchodních politik a požadavků. Dříve vývojáři aplikací používali proprietární software development kit (SDK) pro umožnění konfigurace a správy vyvíjené aplikace prostřednictvím EMM. Pro každou EMM platformu tak vývojáři vytvářeli novou verzi vlastní aplikace. Appconfig komunita přináší nástroje a postupy, s kterými není potřebné vytvářet různé verze, jedné aplikace, pro různé EMM řešení.[38]

Obrázek 2 - EMM členové AppConfig [39]

Obrázek 3 - Část seznamu ISV členů AppConfig [39]

3.1.15 Pojmy z oblasti letectví a mobilních zařízení

Vzhledem k zaměření vlastní práce na leteckou společnost jsou v práci definovány také pojmy průniku oblasti letectví a mobilních zařízení.

3.1.15.1 EFB

EFB, pojem z letectví, vychází z Flight Bag, těžké a rozměrné pilotní tašky obsahující dokumentaci, příručky a další publikace. Flight bag je zátěží nejen pro letadlo, ale také pro samotné piloty, kteří musí s papírovou formou pracovat. EFB, Electronic Flight Bag, je elektronické zařízení, které supluje funkci této pilotní tašky a pomáhá členům letových posádek v procesu rozhodování a získání informací. [40], [41]

V tomto ohledu napomáhá rozvoji EFB trend přenosných elektronických zařízení, takzvaných Portable Electronic Devices (PED). V posledních letech se tato zařízení stávají čím dál častěji součástí kabiny letadla. [40], [41]

Tablety nebo přenosné počítače v kokpitu slouží nejen k nahrazení papírové formy dokumentace, ale také usnadňují další činnosti, jako například výpočty hmotnosti a vyvážení, potřebné délky pro vzlet a přistání nebo dokonce i zobrazení polohy letadla na pohyblivé mapě, pro zlepšení situačního povědomí. V minulosti řada z těchto činností byla prováděna pomocí papírových zdrojů, nebo na základě podpory dispečinku dané letové společnosti.[40], [41]

EFB hardware

Portable EFB – přenositelné zařízení, které není součástí certifikované konfigurace letadla. Například tímto typem může být tablet, který bude použit k zobrazování map a dokumentace. Aby tento typ EFB mohl být použit ve všech fázích letu, musí být vhodně zajištěn proti samovolnému pohybu.[40]

Installed resources – Portable EFB, které je součástí nějakého dalšího systému instalovaného v letadle. Tímto typem může být například tablet, který se přichytí do držáku, který je certifikovanou částí letadla. Součástí držáku může být napájení tabletu nebo jiná konektivita k letadlu.[40]

Installed EFB – tento typ EFB je instalován napevno v letadle, je jeho součástí a musí být zajištěno schválení letové způsobilosti.[40]

EFB software

Aplikace na EFB se dělí na několik skupin:

Typ A – jsou aplikace, jejichž nefunkčnost nebo nesprávné použití nemá vliv na bezpečnost letu. U těchto aplikací není vyžadováno žádné schválení, ale na jejich posouzení by se měl použít HMI (Human Machine Interface Assesment). Jedná se o aplikace pro zobrazení méně důležitých manuálu a dokumentace, případně interaktivní formuláře pro hlášení z letu.[40]

Typ B – jsou aplikace, jejichž porucha či nesprávné použití může představovat pouze nevýznamný poruchový stav. U těchto aplikací není vyžadováno schválení letové způsobilosti, ale je vyžadováno provozní posouzení. Jedná se o aplikace pro zobrazení elektronických letových map, aplikace zobrazující důležité dokumenty a manuály potřebné k provedení letu a aplikace pro výpočty letových výkonů, hmotnosti a vyvážení.[40]

Různé (Non-EFB) – jsou aplikace, které nutně nesouvisí s letovým provozem a je možné je na EFB zařízení instalovat. Jedná se například o webový prohlížeč, mailový klient a další. Instalace a správa těchto aplikací musí být řízena EFB administrátorem.[40]

Obrázek 4 - iPad jako EFB s mapovými podklady Jeppesen [42]

3.1.15.2 Paper Less Cockpit

Paper less cockpit vyjadřuje redukci papírové dokumentace v kabině letadla a nahrazení pomocí elektronických prostředků (EFB). Dokumentace, která se na palubě letadla vyskytuje, zahrnuje dokumentaci k letadlu, operační manuály, dokumentaci vydanou organizací provozující letadlo a také mapové podklady (en-route, terminal charts), případně letové záznamy.[43]

Paper less cockpit a v důsledku EFB vede k optimalizaci v několika bodech [43]:

- úspora místa v kabině,
- úspora hmotnosti,
- rychlý přístup k informacím,
- rychlá dostupnost aktualizací,
- vzdálený přístup k aktualizacím,
- minimalizace zdrojů pro aktualizace,
- kontrola obsahu dokumentů,
- obsah dokumentů řízený správcem EFB.

Není ani výjimkou výrobce, který předplatné na elektronickou dokumentaci cenově zvýhodňuje.[43]

3.2 Platformy

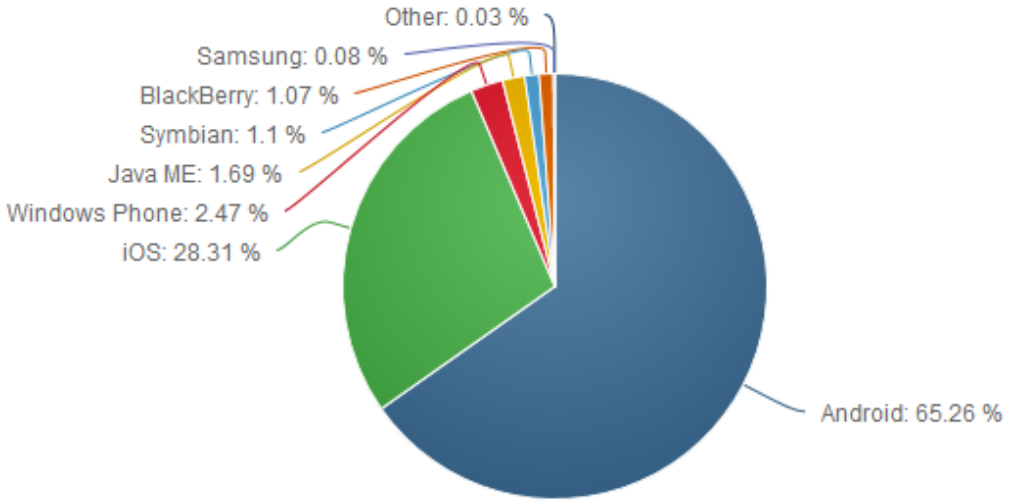
Pro mobilní zařízení je vždy charakteristické, jakou platformu/operační systém používá. Vzhledem k zaměření práce na iOS zařízení bude tento operační systém zařazen jako první. Další platformy jsou Android, BlackBerry a Windows Phone (RT). Při výběru mobilního zařízení je jedním z hlavních kroků rozhodnutí, na jaké platformě je požadováno pracovat. Pro uživatele je často určující oblíbenost nebo předchozí zkušenost z té či jiné platformy. Pro firemní účely se tento výběr řídí spíše požadavky na provozované aplikace tak, aby platforma umožňovala plynulý běh aplikace. Mezi základní požadavky lze zařadit snadnost správy zařízení a dostatečné množství restrikcí, které na zařízení mohou být konfiguračním profilem nastaveny.

Podíl jednotlivých operačních systému mobilních zařízení (telefon, tablet) získaný z dat za období od 01/2016 do 01/2017 dokazuje následující tabulka.

Tabulka 1 - Podíl operačních systému mobilních zařízení na trhu

Operační systém	Celkový podíl na trhu
Android	65,26%
iOS	28,31%
Windows Phone	2,47%
Java ME	1,69%
Symbian	1,10%
BlackBerry	1,07%
Samsung	0,08%
HUAWEI	0,01%
Kindle	0,01%
Bada	0,01%
LG	0,00%
Windows Mobile	0,00%

Zdroj: [44]



Obrázek 5 - Grafické znázornění podílu operačních systému mobilních zařízení na trhu [44]

Pro jednotlivé platformy iOS, Android a Windows jsou vybrány zastupující zařízení z rodiny tabletů, které budou v závěru kapitoly mezi sebou porovnány. Vstupními parametry výběru bylo zařízení s minimální kapacitou úložiště 64 GB, LTE modulem, a dostatečným výkonem. Cena nebyla zvolena mezi klíčové parametry, pokud však existovala možnost volby levnějšího zařízení, bylo zvoleno to.

3.2.1 iOS

Operační systém vyvinutý společností Apple. První iOS měl ještě název iPhone OS, pro jeho využití pouze na zařízení iPhone. iOS je operační systém použitý pro dotykové ovládání. Je velmi jednoduchý a intuitivní. S každou verzí přichází nové funkce, vyniká svou rychlostí a množstvím gest, kterými lze zařízení ovládat. S postupem času iOS obdržely také tablety od Apple, takzvané iPady a také další zařízení, jako například iPody. Celý systém je velmi uzavřený. Nelze provozovat iOS na jiném zařízení než na zařízení od společnosti Apple. Uzavřenost systému vyniká také v obchodu s aplikacemi, který je velmi striktní, a aplikace jsou zde před publikováním podrobovány přísným kontrolám. Uzavřenost systému také vede k případům neřešitelné absence funkcí a je možné pouze doufat v uvědomění společnosti Apple a dodání funkcionality. Apple byl postupným vývojem trhu nucen také zařazovat funkce pro firemní použití zařízení tak, aby iOS nabízel dostatečné množství nastavitelných restrikcí, konfigurace firemních poštovních účtů a jejich rozšíření například při použití MS Exchange.

Mezi výhody lze zařadit jednotné ovládání napříč všemi výrobky v oblasti mobilních zařízení, gesta ovládání, rychlost systému a jednotné aktualizace systému.

Mezi nevýhody lze započítat převážně uzavřenost systému a problematickou synchronizaci mezi zařízením a soubory v jiném zařízení. [45]

Poslední verze je iOS 10.2.1. Na podzim roku 2017 je chystána nová verze iOS 11.

Zástupce platformy

Pro platformu iOS byly vybrány zařízení iPad Air 2 a iPad Pro 9,7“. Obě zařízení disponují úhlopříčkou 9,7“, kapacitou úložiště 128GB bez podpory doplňkové microSD karty, pracují na stejném operačním systému iOS 10 aktuální verze a na první pohled jsou si velmi podobná. Avšak model iPad Pro 9,7“ nabízí novější, rychlejší a modernější A9X chip, podporu Apple pencil, modernizovaný fotoaparát, Smart Connector, vylepšený displej technologií True Tone a další drobná vylepšení. iPad Pro 9,7“ přinesl stejné parametry iPadu Pro (12,9“) ve stejné velikosti jako je nabízen iPad Air 2. Avšak pro další porovnání byl vybrán levnější model – Apple iPad Air 2 128 GB WiFi Cellular.[46]

Obrázek 6 - Apple iPad Air 2 Wi-Fi Cellular [47]

3.2.2 Android

Android je operační systém poskytovaný společností Google zdarma. Zdrojový kód lze bezplatně získat, a to umožňuje masové rozšíření této platformy. Je přesným opakem iOS. Systém je velmi otevřený, ale tato vlastnost s sebou nese možné ohrožení. Převážně na počátku do obchodu s aplikacemi pronikaly škodlivé a podvodné aplikace. Možnost upravovat systém dle vlastního modelu využívají všichni výrobci mobilních zařízení, kteří do svých zařízení aplikují tento systém. Tyto nadstavby a úpravy často systém zpomalují a snižují výdrž baterie oproti základnímu systému. Aktualizace systému jsou bolestí celé

platformy, což je zapříčiněno převážně rychlostí reakce výrobců na vydanou aktualizaci Googlem.

Mezi výhody systému patří otevřenost systému, velká podpora zařízení a dynamičnost skrze společnost Google. Nevýhodami jsou špatná optimalizace vzhledem k velkému počtu variant HW, zpožděné aktualizace a větší potenciál pro napadnutí systému. [45]

Poslední verze je Android Nougat 7.0.

Zástupce platformy

Z nabídky zařízení, které jsou dodávány s operačním systémem Android, byl vybrán tablet Samsung Galaxy Tab S2 9.7 LTE. Výběr byl zvolen tak, aby bylo možné porovnat parametry s konkurenčním iPadem společnosti Apple, platformy iOS. Vybraný model obsahuje LTE modul, má obstojný výkon, displej o rozměru 9,7“ a rozlišení obrazovky na stejné úrovni jako Apple iPad Air 2.[46]

Obrázek 7 - Samsung Galaxy Tab S2 9.7 LTE [48]

3.2.3 BlackBerry

Mobilní zařízení a platforma, pojem BlackBerry, dnes velmi známý v mobilních technologiích s business zařazením, vznikal jako zařízení s cílem jednoduchého, zabezpečeného a efektivního zařízení, které bude schopno zasílat a přijímat e-maily odkudkoliv mimo kancelář. BlackBerry a jeho platforma bylo nepostradatelnou součástí a příslušenstvím manažerů nebo představitelů států do doby příchodu iPhone a Android zařízení.[49]

BlackBerry vznikalo se společností RIM (Research In Motion) na pozadí. Dnes se akcie společnosti dostaly velmi nízko a společnost velmi redukovala své portfolio přístrojů. Platforma stejně jako ostatní nabízí vlastní portál pro stahování aplikací s názvem BlackBerry World. Každé BlackBerry zařízení je jednoznačně identifikovatelné pomocí BlackBerry PIN zařízení.

Pojem BlackBerry v podnikovém nasazení doprovází pojem BES a BIS služby. BES znamená BlackBerry Enterprise Service a BIS je BlackBerry Internet Service. Obě služby je nutné aktivovat u operátora SIM karty. BIS není určeno přímo pro podnikové použití, ale lze jej použít pro sekundární schránku také ve firemní řešení, kdy primární schránka je nastavena přes BES. BIS je definován pro soukromé použití, primárně pouze synchronizuje emaily, nikoliv kontakty, kalendář a další.[50], [51]

BES je velmi zajímavé podnikové řešení, mnohými známý BlackBerry Enterprise server ve své starší verzi 5, poskytovaného také v edici express, umožňuje správu BlackBerry zařízení a jejich napojení na Microsoft Exchange, Lotus Domino nebo Novell GroupWise, a tak plnou synchronizaci emailů do zařízení z těchto poštovních serverů. Dnes je již dostupná verze BES12, umožňující nejen správu BlackBerry zařízení, ale také zařízení s operačním systémem iOS nebo Android. BlackBerry novou správu zařízení již prodává také jako kompletní EMM (Enterprise Mobility Management) řešení.[50], [51]

Výhodou platformy BlackBerry je přímé zaměření na podnikové použití, bohužel do určité míry ovlivněné snahou dohnat konkurenční platformy iOS a Android.

Nevýhodou je dnes velmi malá nabídka přístrojů. Nevýhodou může být také z určité části přechod na „chytrý OS“, tedy opuštění staré koncepce a přechod na BlackBerry 10. Zákaznici tak přišli o velmi zajímavé, zabezpečené, podnikově orientované zařízení spravované na původním BES serveru s velmi malou datovou náročností.

BlackBerry se také může pochlubit operačním systémem pro své tablety - BlackBerry PlayBook. Zařízení dnes již nejsou zařazeny k prodeji.

BlackBerry nabízí vlastní systém přijímaní a odesílání textových zpráv založených BlackBerry PIN zařízení.

3.2.4 Windows Phone

WP je mobilní operační systém od společnosti Microsoft. Předchůdcem byl Windows Mobile, tato platforma do příchodu iPhone OS kralovala trhu. Na první pohled funkční a jednoduchý systém je také uzavřeným operačním systémem. Někteří uživatelé mohou pociťovat absenci některých důležitých aplikací, které nejsou doposud v obchodu s aplikacemi pro Windows Phone dostupné. Systém je rychlý a přehledný, a měl by zapadat do modelu SW od společnosti Microsoft (např. Office 365). Windows Phone není příliš rozšířený, vzhledem k opožděnému zavedení na trh a menšímu počtu podporujícího HW.

Mezi výhody se řadí jednotné grafické rozhraní, optimalizace a rychlost a společné aktualizace. Nevýhodou je uzavřenost systému, menší nabídka aplikací a radikální změny mezi aktualizacemi OS, které nutní k nákupu nového zařízení.[45]

Poslední verzí Windows Phone je verze 8.1.

Windows 10 Mobile

Poslední verzí mobilního operačního systému od společnosti Microsoft je nový Windows 10 Mobile. Nová platforma Windows 10 Mobile je pokračovatelem Windows Phone 8.1 a u některých mobilních zařízení s Windows Phone 8.1 je možné bezplatně aktualizovat na Windows 10 Mobile. Nový Windows 10 Mobile přinesl několik změn ve vzhledu a ovládání systému, nové zajímavé funkce včetně adaptivního prostředí Continuum. Je znatelná snaha sblížení mobilní platformy s operačním systémem pro počítače a tablety Windows 10, a to zejména v prosazování univerzálních aplikací. Mezi nevýhody patří zvýšená chybovost a zasekávání systému a nedostatek univerzálních aplikací. [52]

3.2.5 Windows a Windows RT

Tento velmi známý operační systém je nutné také zmínit, z důvodu zařazení na HW tabletů. Systém disponuje obrovskou škálou možných aplikací a použitím v profesionální sféře. Nevýhodou systému starších verzí, například Windows 8 je snaha naroubovat dotykové funkce nepříliš šťastným způsobem a za nepříznivou lze také považovat cenu licencí.[45]

V červnu roku 2016 byla vydána nová verze Windows 10, přišla s přepracováním systému a je zajímavá také tím, že Microsoft o Windows 10 tvrdí, že jde o poslední stvořený Windows. Přepracovaný systém se vyznačuje novým vzhledem, přepracovanou nabídkou start, novým centrem notifikací a sadou dalších nových funkcí. Microsoft u řady zařízení umožnil bezplatnou aktualizaci ze starších verzí Windows. Má jít o jeden konvergovaný systém pro všechny platformy zařízení. Přináší nové univerzální aplikace napříč celým ekosystémem Windows 10. Mezi nevýhody systému může spadat zhoršené ovládání na tabletech a občasné chyby.[53]

Zástupce platformy

Počet zařízení na platformě Windows, mající parametry pro porovnání se zařízení Apple iPad Air 2 bylo v dané situaci příliš málo. Klíčovým parametr, modul LTE zjednodušil výběr pouze na jedinou nabídku a to Lenovo ThinkPad 10 - 64GB, LTE. Tablet od společnosti Lenovo se nepříliš blíží k parametrům zařízení vybraných na platformě Apple a Android, ale výkonově pro většinu operací bohatě dostačuje. Za zmínku určitě stojí zařízení od společnosti Microsoft – tablet Surface Pro 4. Bohužel toto zařízení v dané situaci nebylo na náš trh dodáváno s modulem LTE.

Níže je uvedena tabulka s technickými specifikacemi tabletu Lenovo ThinkPad 10 - 64GB.[54]

Obrázek 8 - Lenovo ThinkPad 10 LTE [55]

3.2.6 Srovnání zařízení

Pojednání o platformách zahrnuje také srovnání konkrétních typů zařízení vybraných platforem Android, Apple a Windows. Srovnání je zaměřeno pouze na zařízení typu tablet současné nabídky trhu, pro vybrané platformy Apple iOS, Google Android a Microsoft Windows. Z dostupných zdrojů je možné získat kompletní přehled všech parametrů vybraných zařízení. Pro tuto práci byly vybrány pouze některé klíčové parametry vybraných tabletů, které jsou uvedeny v tabulce č. 2 níže. Samsung Galaxy Tab a Apple iPad Air 2 jsou si v některých parametrech velmi podobné. Mají podobné rozměry, váhu a rozlišení displeje. Podobná je také výbava. Samsung Galaxy Tab je lepším ve výdrži baterie a poměru displeje k tělu zařízení. Výkon obou zařízení by měl být na vyšší úrovni. Vzhledem k odlišné platformě, nelze na základě hardware výbavy soudit o rozdílech ve výkonu, pro vhodnější porovnání by bylo nutné sáhnout po dalších testech výkonu. Lenovo ThinkPad 10 je v mírném stínu ostatních dvou zařízení. Disponuje horším rozlišením a větším displejem než soupeři. Je také řádově větší a nabízí horší poměr displeje k tělu zařízení. Oproti soupeřům má instalované Window 10 Pro, a tím se stává plnohodnotným firemním nástrojem. Jako pozitivní na Lenovo ThinkPad 10 je hodnoceno jeho zpracování,

hmotnost, dokovací klávesnice a tužka na ovládání ThinkPad Pen. Bohužel, v několika recenzích je upozorňováno na jeho výkonové problémy.[56]

Cílem bylo porovnání zařízení s kapacitou disku 64 GB. Apple iPad Air 2 se již v této verzi neprodává a je nahrazen 128 GB verzí, která je uvedena v porovnání. Lenovo ThinkPad 10 je nabízen ve verzi 64 GB, a také ve verzi s kapacitou disku 128 GB, cena se pak pohybuje okolo 26 000 Kč. Ve snaze o udržení podobné cenové relace byl do porovnání vybrán 64 GB model. Samsung Galaxy Tab S2 je v současné nabídce dostupný v 32 GB verzi. Výhodou Samsung a Lenovo zařízení je možnost rozšíření kapacity úložiště pomocí micro SD karty. Kapacitu úložiště nelze u Apple iPad Air 2 standardně rozšířit.[57]

Nejlevnějším porovnávaným zařízením je Samsung Galaxy Tab S2. Pořizovací cena je vyšší u Lenovo ThikPad 10 a Apple iPad Air 2, u kterých je cenový rozdíl zanedbatelný.

Tabulka 2 - Srovnání vybraných zástupců platforem mobilních zařízení iOS, Android a Windows

		Apple iPad Air 2 128 GB Wi-Fi Cellular	**Lenovo ThinkPad 10 - 64GB, LTE**	**Samsung Galaxy Tab S2 9.7 LTE**
Sítě	Technologie	GSM / CDMA / HSPA / EVDO / LTE	GSM / HSPA / LTE	GSM / HSPA / LTE
Představení	Uvedení	2014, Říjen		2015, Červenec
Body	Rozměry	240 x 169,5 x 6,1 mm	256,5 × 177 × 9,1 mm	237,3 x 169 x 5,6 mm
	Váha	444 g (3G/LTE)	618 g (LTE)	392g (LTE)
	SIM	Nano-SIM	micro SIM	Nano-SIM
Displej	Typ	LED-backlit IPS LCD, kapacitní dotykový, 16M barev	IPS LCD (WUXGA)	Super AMOLED kapacitní dotykový, 16M barev
	Velikost	9.7 palců (~71.6% poměr obrazovky a těla zařízení)	10,1 palců (~64% poměr obrazovky a těla zařízení)	9.7 palců (~72.7% poměr obrazovky a těla zařízení)
	Rozlišení	1536 x 2048 pixelů (~264 ppi jemnost dipleje)	1920 x 1200 pixelů	1536 x 2048 pixels (~264 ppi jemnost dipleje)
Platforma	OS	iOS 8.1, možný upgrade na iOS 10.2.1	Windows 10 Pro	Android OS, v6.0.1 (Marshmallow)
	Chipset	Apple A8X	Intel Atom X7	Qualcomm MSM8976 Snapdragon 652
	CPU	Triple-core 1.5 GHz Typhoon	Intel Atom Processor X7-Z8700 (4x 1.6 GHz)	Octa-core (4x1.8 GHz Cortex-A72 & 4x1.4 GHz Cortex-A53)
	GPU	PowerVR GXA6850	Intel HD Graphics	Adreno 510
Paměť	Card slot	Ne	microSD, max. 128 GB	microSD, max. 256 GB (vyhrazený slot)
	Interní	128 GB, 2 GB RAM	64GB eMMC, 4 GB RAM	32 GB, 3 GB RAM
Funkce	WLAN	Wi-Fi 802.11 a/b/g/n/ac, dual-band, hotspot	Wi-Fi 802.11 a/b/g/n/ac	Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot
	Bluetooth	v4.0, A2DP, EDR	v4.0	v4.1, A2DP, LE
	GPS	Ano	Ano	Ano
	NFC		Ano	
	Infraport	Ne	Ne	Ne
	Radio	Ne	Ne	Ne
	USB	v2.0, reversible connector	v3.0 (3.1 Gen 1)	microUSB v2.0 (MHL TV-out)
Baterie		Nevýměnná Li-Po 7340 mAh baterie (27.62 Wh)	Nevýměnná Li-Po 32 Wh	Nevýměnná Li-Ion 5870 mAh battery
	Doba hovoru	Až 10h (multimedia)	Až 10h (multimedia)	Až 12h (multimedia)
Další	Barvy	Space Gray, Silver, Gold	Black	White, black, gold
Cena		18 500 Kč	19 000 Kč	16 000Kč

Zdroj: [46] [58]

3.3 Zabezpečení

V této kapitole bude přiblíženo zabezpečení mobilních zařízení. Budou definovány hrozby, bezpečnostní politiky, či antivirová řešení na koncovém zařízení.

3.3.1 Hrozby

Mezi základní hrozby spadají [59]:

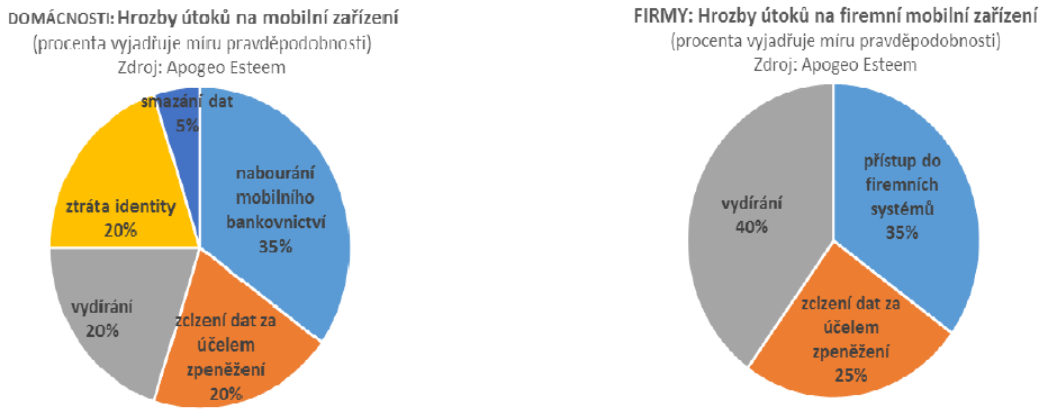
- neoprávněný přístup k zařízení,
- odcizení zařízení,
- únik citlivých informací ze zařízení,
- nedůvěryhodné zařízení připojené do firemní sítě,
- nedůvěryhodné aplikace (škodlivý kód, malware),
- zařízení připojení do nedůvěryhodné sítě,
- ukládání dat do nedůvěryhodných úložišť,
- zpracovávání nedůvěryhodného či nebezpečného obsahu na firemním zařízení.

Mobilní zařízení jsou menších rozměrů, lze je snadno ztratit a také se stávají často cílem zlodějů. Pokud se zařízení dostane do cizích rukou, hrozí únik citlivých informací ze zařízení a samozřejmě finanční škoda v rozsahu ceny daného zařízení. Škoda na zcizených informacích, ať již soukromých (fotek, zpráv) je vysoká, ale škoda převážně na datech firemního charakteru (emaily, kontakty, dokumenty) je daleko širší a přesahuje významně škodu samotného zařízení.

Aplikace stahované na zařízení je jeden z nejsnazších způsobů, jak do zařízení dostat škodlivý kód. Jednotlivé platformy mají své vlastní obchody aplikací. Striktní pravidla pro publikaci aplikace, v případě obchodu Apple AppStore v tomto případě fungují velmi dobře. Do zařízení je tak menší šance stáhnout aplikaci, která obsahuje podvodný obsah nebo škodlivý kód. Opačná je situace na Google Play, kde pravidla pro publikaci aplikací byla méně striktní a možnost stáhnout škodlivou aplikace je vyšší. Doporučení jsou taková, aby uživatel vždy stahoval pouze aplikace z ověřených zdrojů a případně povoloval pro Android pouze nejnutnější oprávnění v OS.

V tomto případě, ale mohou být útočníci také napřed. Pro platformu Android byl nalezen problém s aplikací. Ta prošla kontrolou této platformy a byla podsunuta uživateli. Aplikace nevyžadovala žádná riziková oprávnění, to znamená, že nevzbudí podezření. Tato oprávnění dostane, při následném upgrade operačního systému Android. Stane se tak

bez vědomí uživatele, bez možnosti zabránění této situaci. Původně neškodná aplikace se tak mění v nástroj, na šmírování pohybu uživatele, nebo na odposlouchávání hesel.[60]



Obrázek 9 - Podíl hrozeb pro domácnosti a firmy na mobilní zařízení [61]

Speciální pozornost je nutno věnovat při ukládání dat mimo firemní úložiště. Cloudová úložiště s sebou nesou velkou míru rizik a nejasnost ohledně správy dat, zálohování, země uložení, neposkytování dat 3 osobám a další aspekty nutné k prostudování a ověření.

Za hrozby lze také považovat jakékoliv úpravy zařízení typu Jailbreak pro iOS a Root pro Android.

3.3.2 Bezpečnostní politiky

Většina podniků má nastavenu formální bezpečnostní politiku definovanou jejich celkovou strategií pro bezpečnost a rizika. Bezpečností politika představuje první krok před začleněním mobilních zařízení do podnikového IT, a je to obecně směrnice upravující možnost využívat mobilní zařízení, pro práci s podnikovými aplikacemi a daty. Tato směrnice musí brát v úvahu jak podnikové, tak soukromé zařízení (ať pro práci nebo pouze soukromě například na Wi-Fi).

Jde o velmi důležitý článek celého řetězce zabezpečení. Bezpečnostní politika musí být čitelná a jasná. Měla by obsahovat procesy pro zařazení BYOD zařízení do firemního

prostředí a náležitosti nutné pro bezpečnostní pravidla používání mobilních zařízení ve firemním prostředí. [62]

Bezpečnostní politika vzniká na základě analýzy rizik. Přibližné body lze shrnout takto:

- počet připojených zařízení,
- definice a vynucení bezpečnostních opatření (kódový zámek určité složitosti, šifrování),
- pravidla pro používání zařízení,
- pravidla přístupu k firemnímu obsahu,
- definice procesů,
- definice povolených platforem a přístrojů,
- Black list/White list aplikací,
- definice bezdrátových sítí,
- definice chování při ztrátě zařízení,
- procesy pro správu zařízení,
- právní ošetření (BYOD, polohové služby, soukromá data na zařízení),
- další dle analýzy rizik.

Velmi častým jevem je rozpor mezi deklarovanou firemní politikou a samotnou realitou. Přibližně 95 % organizací má zavedeny politiky vztahující se k používání mobilních zařízení, ale pouze třetina zaměstnanců je s nimi podrobněji seznámena. Problém také spočívá v tom, že firmy mají problém svoji politiku vynutit. Nicméně mnohdy je i samotná firemní politika velmi volná. Například 4 z 10 organizací nijak neomezují počet zařízení, která uživatelé mohou připojovat (respektive synchronizovat). Stejně tak 4 z 10 firem nijak neomezuje přístup k webu z mobilních zařízení, stahování obsahu ani instalaci nových aplikací.

Nesporným bodem, který všeobecně platí, že dodržování musí být pasivně i aktivně průběžně kontrolováno.[63]

Nespornou součástí připravenosti na zavedení mobilních zařízení do společnosti, je identifikace hlavních právních rizik a jejich ošetření. Právní rizika vznikají ve spojitosti licencí, cloudu, bezpečnosti dat a jejich umístění a zpracování osobních údajů.

3.3.3 Antivirová řešení

Na trhu je mnoho produktů nabízející služby antivirového řešení pro mobilní zařízení. Zástupci iOS platformy se ve většině shodují na tom, že uzavřenost systému pomáhá k zabezpečení a antivirové řešení zde není potřebné.

Na platformě Android se názory už velmi mísí, vzhledem k otevřenosti platformy, starším verzím OS, které mohou mít „díry“ v systému a převážně kvůli větší míře nedůvěryhodných aplikací.

Je nutné si uvědomit, že každá kontrola v podobě antiviru povede ke snížení výdrže baterie a v některých případech i ke snížení výkonu zařízení (v případě nedostatku RAM). Z těchto důvodů je vhodné najít vhodný kompromis a rozhodnout se, zda je antivirové řešení nutností.

Každá platforma má své standardní systémové prostředky na ochranu. Antivirové řešení je doporučováno právě v případě používání starších verzí OS. Pokud, ale uživatel instaluje aplikace z neověřených zdrojů, nemá smysl takové řešení používat.

Antivirové řešení lze nahradit několika kroky při používání zařízení:

- neinstalovat aplikace z neověřených zdrojů a zakázat toto v systémovém nastavení,
- věnovat pozornost stahovaných souborům,
- ověřovat aplikace,
- vyhnout se aplikacím požadující přístup k SMS a hovorům,
- obezřetnost v internetovém prohlížeči,
- obezřetnost na bezplatných Wi-Fi – pamatovat na to, že provoz může být odposloucháván nebo přesměrován.

Na závěr lze říci, že nejlepšími bezpečnostními aplikacemi jsou pozornost a používání zdravého rozumu.[64]

3.4 Aplikace

Aplikace jsou nedílnou součástí mobilních zařízení. Tato část práce se věnuje aplikacím, které uživatelé často používají ve firemním segmentu. Shrnutí obsahuje převážně obecné aplikace, jako emailový klient, kalendář, poznámky, aplikace pro práci s dokumenty, webový prohlížeč a případně další specializované aplikace používané pro konkrétní přístup k firemním zdrojům. Aplikace lze odlišovat dle platformy, na které jsou

používány. Řada aplikací bývá na zařízeních instalována, již ve výchozím stavu od výrobce. Typicky se jedná o sadu aplikací pro email, kalendář, kontakty, webový prohlížeč a další. Dále je na uživateli, správci a nabídce v obchodě dané platformy, zda budou použity výchozí aplikace či jiné stažené. V obchodech s aplikacemi je nepřeberné množství aplikací. Lze zkoušet aplikace různých vývojářů, ale většina uživatelů vsadí na ověřené aplikace většinou od známých tvůrců. Kromě kladného ohlasu je u známých aplikací také výhodou, že se vývojář snaží o pokrytí většiny dostupných platforem mobilních zařízení, ale není to pravidlem. Cílem práce ovšem není vyjmenovat všechny aplikace, dostupné na platformách mobilních zařízení. Níže jsou uvedeny obecné údaje k jednotlivým základním aplikacím, včetně konkrétních doplnění informací k platformě iOS.

3.4.1 Emailový klient

Základní aplikace, která je na většině platforem instalována ve výchozím stavu zařízení. Emailový klient má za úkol synchronizovat emaily do zařízení, s možností nastavení řady typů emailových účtů. Pro firemní využití mezi stěžejní typy účtů spadají:

- Microsoft Exchange, Exchange Online (Office 365)
- Google
- IMAP, POP3

Profily IMAP a POP3 již postupně ustupují, převahu získávají profily typu MS Exchange, ale je rozhodující, jaký poštovní server společnost provozuje. Mezi základní funkce emailového klienta spadá kromě synchronizace elektronické pošty také možnost správy samotné schránky, jako je nastavení podpisu, přesouvání emailů v rámci složek schránky, nebo označování položek ke zpracování. Problémem by nemělo být ani šifrování emailů a elektronický podpis. Cílem je uživateli umožnit provádět na zařízení podobnou agendu, jako je schopný vykonávat v klasickém poštovním klientovi na počítači. Většina aplikací dovoluje na zařízení nastavit i více emailových účtů zároveň. V takovém případě je vhodné například firemní účet nastavit jako výchozí.

Platforma iOS obsahuje nativní aplikaci Mail, umožňující výše definované nastavení profilu, včetně jednoduchého nastavení. Pro případy synchronizace schránek s větším objemem pošty nabízí aplikace možnost nesynchronizovat celý objem schránky bez omezení, ale vybrat kratší variantu, například pouze jeden měsíc do minulosti. Je důležité

zmínit, že aplikace Mail připojuje v současné verzi iOS 10 přílohy pouze ze zdrojů fotoaparát, galerie obrázků a Apple úložiště dokumentu iCloud Drive. Pro přílohy dokumentů či jiných typů souborů je nutné odesílat email pomocí sdílení souboru z aplikace, ve které je zobrazován. Není tak umožněno, bez použití iCloud Drive, připojovat přílohu k odpovědi emailu například typu PDF.

V případě použití EMM je pravděpodobné, že vybrané EMM bude mít vlastní aplikaci emailového klienta, která bude zapadat do konceptu zvoleného řešení a zvyšovat bezpečnost. Není ale nutné vždy takovou aplikaci uživatelům nutit, zvláště pokud nejsou kladeny příliš vysoké nároky na bezpečnost, EMM umožňuje vzdáleně konfigurovat i nativní emailové klienty.

3.4.2 Kalendář, kontakty a poznámky

Velmi úzce s emailovým klientem souvisí další aplikace – kalendář, kontakty a poznámky. Při konfiguraci emailového účtu je často součástí synchronizace emailu, také synchronizace kalendáře, kontaktů a poznámek spravované pomocí jednotlivých aplikací, často výchozí aplikace již na zařízení instalované. Aplikace kalendář často umožňuje výběr mezi kalendáři, které bude zobrazovat tak, aby byla aplikace čitelnější, v případě že na zařízení je povolena synchronizace více profilů. Aplikace pro kontakty také umožňuje výběr mezi skupinami kontaktů. Poznámky jsou pro uživatele cenným pomocníkem, zvláště pokud nezůstávají pouze na zařízení, ale jsou dále dostupné i odjinud (notebook, PC). Výchozí aplikace pro poznámky nemusí být vždy vyhovující, uživatelé mohou dávat přednost aplikacím staženým z příslušného obchodu. Častým případem je například aplikace Evernote či aplikace Microsoft OneNote.

EMM řešení i v případě těchto aplikací mohou nabízet vlastní řešení, ale převážně u aplikace pro kontakty musí jít o jistý kompromis mezi bezpečností a použitelností. [65]

3.4.3 Webový prohlížeč

Každá platforma ve výchozím nastavení přichází s různými webovými prohlížeči. Pro iOS je typické Safari, pro Windows Phone je to Internet Explorer, pro Android to může být Chrome. Prohlížeče jsou dostupné také v obchodě s aplikacemi, odkud je možné si například na iOS instalovat prohlížeč Chrome. Prohlížeč Safari, ale na jinou platformu,

než iOS, nelze instalovat. U platformy iOS je možné se také setkat s problémem přehrávání flash aplikací v prohlížeči. Řešením je stažení aplikace prohlížeče, která zahrnuje podporu pro flash, například Puffin Browser, se vzdáleně spouštěným flash obsahem.

Pro iOS 10 je Safari přehledný a jednoduchý prohlížeč s možností tvorby záložek, odkazů na plochu (webclip) a také s možností zobrazení většiny známých typů souboru, již v rámci Safari a podporou HTML 5. Safari podporuje Split View, funkci iOS rozdělení obrazovky pro práci se dvěma aplikacemi najednou.[65]

3.4.4 Specializované aplikace

Příkladem specializovaných aplikací může být klient pro vzdálenou plochu nebo aplikace pro konfiguraci a provoz VPN tunelu. Často jsou používány také aplikace pro čtení dokumentů nebo jejich editaci. Pro platformu stojí za zmínku některé aplikace od společnosti Microsoft. Pro vzdálenou plochu jde o velmi spolehlivou aplikaci Microsoft Remote Desktop, pro práci s dokumenty a tabulkami Microsoft Word a Excel. Zmíněné aplikace jsou dostupné na App Store zdarma. Pro používání aplikací Word a Excel se musí vytvořit účet u společnosti Microsoft, pomocí kterého se uživatel do aplikace přihlásí. Pokud pak uživatel bude chtít editovat nebo vytvářet nové dokumenty a tabulky, musí mít předplacený účet Office 365. Apple na vytváření a editaci dokumentu a tabulek přináší vlastní řešení, aplikace Pages a Numbers. Ve starších zařízeních tyto aplikace nejsou dostupné ve výchozím stavu a je nutné je zakoupit na App Store. Pro prohlížení nejenom PDF dokumentů je velmi dobrým pomocníkem aplikace Adobe Reader, který je pro iOS zdarma. Na PDF soubory lze použít i nativní aplikaci v iOS, takzvané iBooks. Pro aplikaci na VPN záleží jaký typ připojení má být konfigurován. Řadu typů VPN připojení má iOS již integrované v sobě a lze je nastavit přes nastavení. Pro typy připojení, které nejsou integrované, existují aplikace, kterými se VPN tunel vytvoří. Příkladem může být aplikace od společnosti Cisco Systems, Cisco AnyConnect.[65]

3.5 Správa

Správa mobilních zařízení je neopomenutelnou částí nasazení mobilních zařízení do firemního segmentu. Nejčastějšími požadavky jsou jednotná správa, přívětivé prostředí a pokrytí většiny dostupných platforem.

Dalšími požadavky jsou:

- zjednodušení správy, zrychlení procesu zařazení mobilního zařízení pod správu,
- odhalení nevhodného chování:
    - jailbreak/root zařízení,
    - instalace nevhodných aplikací,
    - porušení bezpečnostních pravidel,
- zajištění přehledu instalovaných aplikací pro auditní a kontrolní účely,
- správa BYOD zařízení – firemní a soukromý obsah na jednom zařízení,
- jednotné prostřední správy pro všechny platformy a způsoby užití zařízení – BYOD, firemní zařízení, zařízení využívající pouze služeb EAS,
- zajištění přístupu uživatelů k firemním prostředkům (email, dokumenty, aplikace),
- vhodná integrace do firemní infrastruktury – např. propojení s Active Directory, Microsoft Sharepoint, Microsoft Exchange, VPN,
- dostatečné možnosti reportingu a BI nástroje (Bussiness Intelligence).

3.5.1 Možnosti správy

Možnosti správy jsou závislé na vybudované IT infrastruktuře společnosti. Pokud je implementován Microsoft Exchange od verze 2007, nabízí se pro zjednodušenou správu zařízení EAS a jeho dostupné funkce pro synchronizaci emailu, vynucení zabezpečení kódovým zámkem/PINem s dostatečnou délkou a komplexností, administrátoři mohou provést vzdálené smazání zařízení a mají kompletní přehled o připojených zařízeních. Více je o protokolu EAS popsáno v kapitole o pojmech.

Přibývající počet zařízení a požadavků od uživatelů, na přístup k firemním prostředkům nutí IT správce společnosti implementovat nové nástroje pro správu mobilních zařízení, nejčastěji označované jako MDM, případně integrovat do infrastruktury společnosti kompletní strategii EMM. V další části kapitoly bude hlouběji rozebráno řešení MDM, včetně doplňujících komponent EMM, jako MAM a MCM.

3.5.2 Řešení EMM/MDM

Obecný model MDM je klient/server. Na mobilním zařízení je instalován agent (aplikace), která komunikuje se serverovou částí, instalovanou ve vlastní infrastruktuře společnosti nebo v prostředí cloudu. Serverovou část ovládají a udržují administrátoři,

pomocí webového přístupu nebo pomocí aplikace. Agent na zařízení poskytuje serveru potřebné informace a vykonává zaslané instrukce, komunikuje na zabezpečeném komunikačním kanále a kromě příjmu instrukcí také odesílá data o zařízení, případně může reagovat na definované situace a podle nastavených pravidel vykonávat určené operace. Škálu možných nastavení, které lze na zařízení omezit, povolit nebo nastavit určují vývojáři operačních systému.

Limitujícím prvkem každého MDM řešení jsou operační systémy samotných mobilních zařízení. Každý operační systém lze vzdáleně nastavit a konfigurovat pouze do míry, kterou určuje vývojář daného operačního systému, což v důsledku znamená, že není vždy zaručena stejná úroveň správy všech platforem.[23]

Základní parametry MDM řešení jsou [64]:

- správa a zabezpečení mobilních zařízení různých platforem,
- jednoduchá konzole pro správu,
- škálovatelné a flexibilní řešení, s možností integrace do podnikové IT infrastruktury (AD),
- nasazení on-premise nebo v cloudu,
- vlastní certifikační autorita pro snazší nasazení, případně možnost použít jinou certifikační autoritu,
- podpora programu BYOD,
- zabezpečená brána, pro správu, šifrování a zajištění komunikace mezi zařízeními a podnikovými systémy. Blokování nepovolené komunikace nebo komunikace zařízeních, která nesplňují pravidla zabezpečení,
- zajištění ochrany příloh emailů,
- integrace reportovacích nástrojů,
- možnost smazat ze zařízení podnikový obsah bez nutnosti smazat soukromá data uživatele (fotky, osobní soukromý emailový profil apod.),
- detekce nevhodného chování (zrušení zabezpečení zařízení, nevhodné aplikace, jailbreak apod.) a následná aktivace událostí dle definovaného scénáře – odpojení od firemního obsahu, smazání zařízení apod.,
- zjednodušení procesu zařazení mobilního zařízení do správy.

3.5.3 Porovnání vybraných produktů EMM

Nástroje, které mohou firmy využít pro správu mobilních zařízení, v posledních letech zaplavily trh. EMM nabízí velká část zvučných jmen v oblasti software a informačních technologií. Z jejich zástupců lze jmenovat společnosti jako VMware, IBM, Cisco, Citrix, CA, SAP nebo například Microsoft. Není cílem práce provést kompletní srovnání všech dostupných produktů, je ale na místě provést přiblížení několika EMM řešení, které se v době psaní práce přetahují o vedení trhu. Do srovnání bylo vybráno řešení Airwatch společnosti VMware, MobileIron od stejnojmenné společnosti a MaaS360 od společnosti IBM. Vybrané platformy EMM jsou uvedeny jejich silnými a slabými stránkami, dle Gartneru, a dále jsou definovány některé zajímavé komponenty každého řešení. Detailní srovnání vybraných EMM řešení včetně několika dalších přináší článek v Computerworld (autor Bob Violino) a vybraná část je obsahem přílohy č. 1.

Obrázek 10 - Gartner magický kvadrant EMM platforem [27]

3.5.3.1 Airwatch

Mobilní řešení AirWatch patří mezi lídry v odvětví. Jde o produkt společnosti AirWacht se sídlem v USA, Atlantě. Únoru roku 2014 byl AirWatch získán společností VMware, kdy došlo k přejmenování na AirWatch by VWware a k zapojení mobilního řešení mezi produkty VMware a integraci do WMware technologií. Za zmínku stojí VMware IAM a produkty softwaredefined networking (SDN) od VMware.

Airwatch představuje komplexní správu podnikové mobility, dokáže spravovat zařízení napříč všemi mobilními platformami, včetně robustních přístrojů, do prostředí

skladů a logistických center, včetně periferií. Nabízí širokou podporu pro mobilní aplikace třetí strany nezávislých dodavatelů (ISV) a je jedním ze zakládajících členů standardu AppConfig.[27]

Silné stránky [27]:

- výborné postavení na trhu,
- silné zázemí společnosti VMware,
- mnoho úspěšných a rozsáhlých implementací napříč trhem,
- konzole pro správu patří mezi nejpoužitelnější a jednoduché, pro snadné naučení AirWatch disponuje v konzoli vloženými tréninkovými videi, různými průvodci a odkazy do nápovědy,
- neustále inovace na poli zero-day podpory nových operačních systémů a zaměřování se také na správu zařízení IoT a zaměřování se na jednotné pracovní prostředí,
- člen standardu AppConfig.

Slabé stránky [27]:

- emailová aplikace Boxer nedostupná pro všechny platformy, to nutí uživatele používat emailové aplikace nativní v zařízení nebo třetích stran,
- zatím nepotvrzené odladění problému se stabilitou emailové aplikace – vyřešení novou aplikací Boxer,
- plánovaná akvizice mateřské společnosti VMware, EMC, Dellem vyvolává potenciální obavy, že produkt VMware AirWatch již nebude dostávat takové pozornosti, jakou má v současném stavu, pod samostatným VMware,
- stížnosti týkající se podpory VMware AirWatch od klientů, kteří nemají přímého technického správce účtu (TAM).

Detail řešení

Airwatch podporuje všechny modely vlastnictví zařízení, pomocí kontejnerizace AirWatch Workspace Management odděluje firemní a osobní údaje na zařízení, zabezpečuje korporátní zdroje a zachovává soukromí zaměstnanců. Řešení zahrnuje flexibilní kontejnerizace pro firemní e-mail, aplikace, obsah a prohlížení. Emailový kontejner je řešen pomocí AirWatch Inboxu, který zajišťuje přístup k firemním emailům, kalendáři a kontaktům. Tato aplikace je v současné době nahrazena aplikací Airwatch Boxer, která by měla řešit chyby Inboxu. Aplikace Boxer je ale zatím dostupná pouze pro iOS a zatím není potvrzeno, zda potíže se stabilitou Inboxu byly novou aplikací vyřešeny.[66]

Pro případy, kdy uživatel opouští firmu nebo zařízení odhlašuje od programu BYOD, řešení nabízí odstraňování korporátních zdrojů ze zařízení. Nezbytnou součástí je také vzdálené vymazání pro případy ztráty nebo odcizení zařízení. [67]

Pro vývoj bezpečných aplikací AirWatch nabízí Airwatch Software Development Kit (SDK), aplikace pak budou součástí bezpečného kontejneru. Takto lze zabalit jak vlastní aplikace, tak již aplikace vyvinuté. [68]

Další komponenta AirWatch Secure Content Locker slouží k distribuci firemního obsahu, synchronizaci souborů, včetně toho poskytuje flexibilní možnosti ukládání dat. Pro případy maximální ochrany dat lze vyžadovat otevírání e-mailových příloh a obsahu v Secure Content Lockeru. [68]

Content Locker lze integrovat s místními uložišti typu Sharepoint nebo WebDav, lze použít AirWatch Cloud (integrace s Office 365, Box, Google Drive apod.), případně využívat kombinaci, tedy hybridní režim. Content locker umožňuje mimo jiné správu verzí dokumentů, lze jej provozovat jako mobilní aplikaci, webového portálu nebo desktopové aplikace. Zajímavou integrací Content Lockeru je možnost propojení s firemní sociální síti SocialCast by VMware s výhodou zlepšení spolupráce nad dokumenty.[69]

AirWatch Browser je určený pro bezpečné internetové prohlížení s funkcemi. Zahrnuje vlastní konfigurace Whitelistů a Blacklistů a tunelování aplikací pro intranetové stránky bez VPN připojení. Pro případy maximální ochrany dat lze vyžadovat otevírání hypertextových odkazů a obsahu v e-mailu v AirWatch Browseru. Browser využívá tunel aplikace přes AirWatch Mobile Access Gateway pro bezpečný přístup k interním zdrojům.[70]

Administrační konzole patří mezi přehledné, integrace s adresářovými službami a správa pomocí rolí a skupin přispívá k efektivní správě zařízení. Registrace zařízení probíhá přes agenta, na zařízení se doručí profily s podnikovými zásadami a nastavením. Na zařízení je možné doručit podmínky použití, upravitelné a s možností vedení verzí, dále také doručovat zprávy pro koncové uživatele. [71]

AirWatch Mobile Application Management slouží pro získávání, distribuci, zabezpečení a sledování mobilních aplikací. Airwatch se integruje s dostupnými obchody aplikací jednotlivých platforem Apple, Microsoft, Google, lze tak získat přístup k veřejným aplikacím. AirWatch umí pracovat s Apple Volume Purchase Programem. Pro uživatele slouží App Catalog, mimo to lze aplikace doručovat do zařízení přímo při registraci. Kontrola a sledování instalovaných aplikací může vyústit až v konfiguraci Whitelistů a Blacklistů aplikací. Zajímavou částí aplikačního managementu je zpětná vazba, kdy uživatelé mohou hodnotit a revidovat veřejné a interní aplikace. V katalogu aplikací pak mohou komentáře vidět nejen administrátoři, ale také ostatní uživatelé. V případě selhání některé aplikace AirWatch zachytí protokol chyb a odešle jej vývojářům pro prozkoumání.[71]

Ve spojení s application managementem se také skloňuje pojem AirWatch AppShield, které zaštiťuje integraci aplikací s platformou AirWatch. AirWatch umožňuje vývojářům stát se jejich partnery, rozšířit jejich aplikace pomocí AirWatch SDK, App Wrappingu pro rozšíření zabezpečení aplikace a přidání možnosti správy. To zahrnuje Data Loss Prevention (DLP), integrovaná autentizace Single Sign-On (SSO), analýzy, Jailbreak detekce, Geofencing nebo zabezpečené VPN. V AirWatch Market Place je pak zobrazen aktuální seznam partnerů.[71]

3.5.3.2 MobileIron

MobileIron je produkt stejnojmenné společnosti MobileIron se sídlem v USA v San Jose. Jako jedna z mála společností se soustředí pouze na EMM řešení, snaží se tak obstát v konkurenci ostatních, kteří své produkty EMM nabízejí jako součást balíčku svých dalších technologií. Společnost MobileIron roste co do počtu svých zákazníků, tak i svého patentového portfolia a vylepšuje propracovanost svého EMM produktu.

MobileIron jako první poskytovatel EMM zavedl do své aplikační sady komponentu Visual Privacy. Je jedním ze zakládajících členů standardu AppConfig a nabízí širokou

podporu pro třetí strany mobilních aplikací ISV. MobileIron je oceňován za schopnost držet krok v nejnovějších a pokročilých funkcích pro tři hlavní mobilní platformy a pro pokrok v zajišťování bezpečnosti U. S. certifikací. [27]

Silné stránky [27]:

- management konzole, která v posledních letech prošla inovacemi, byla doplněna zlepšeními, včetně možnosti vytvářet vlastní sestavy, dále bylo provedeno rozšíření integrace MobileIronu se SIEM řešeními třetích stran, jako Splunk a ArcSight,
- dostupnost management konzole i pro mobilní zařízení,
- škálovatelnost produktu,
- stabilita produktu i společnosti,
- rozsáhlý AppConnect ekosystém,
- podpora nejnovějších technologií napříč platformami Android, iOS a Windows (poslední verze platoforem včetně Windows 10),
- člen standardu AppConfig.

Slabé stránky [27]:

- reportované potíže s eskalací potíží k odpovědné podpoře
- Apps@Work je označován za nedostatečně inovovaný aplikační katalog
- Obavy z výměny výkonného vedení společnosti.

Detail řešení

Architektura platformy MobileIron se skládá ze tří integrovaných a distribuovaných softwarových komponent.

MobileIron Core

MobileIron Core se integruje s back-end podnikovými IT systémy a umožňuje správcům definovat IT zásady zabezpečení a správy mobilních zařízení, aplikací a obsahu. Core je možné rozšířit pomocí API rozhraní pro další integraci s technologickými partnery MobileIronu.[72]

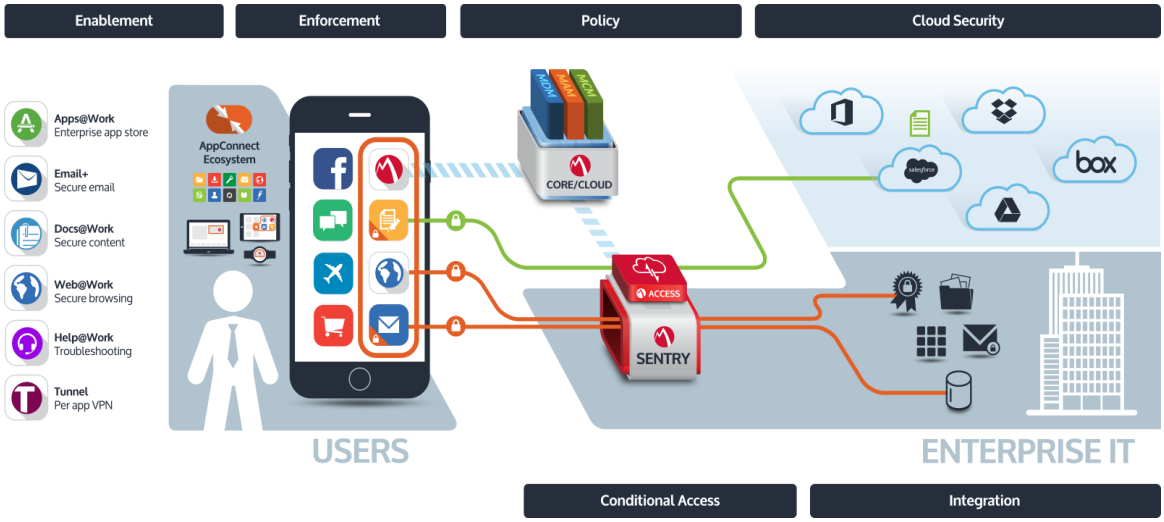
MobileIron Sentry

Sentry je in-line gateway, která spravuje, šifruje a zajišťuje komunikaci mezi mobilním zařízením a back-end podnikovými systémy.[72]

MobileIron Klient

Tato součást nese název Mobile@Work a koncoví uživatelé si ji v podobě aplikace stahují na svá zařízení. Klient automaticky nakonfiguruje zařízení dle nastavených pravidel, vynutí přiřazené politiky do zařízení tak, aby byly splněny všechny stanovené podmínky pro přijetí zařízení do firemního prostředí. Klient vytvoří zabezpečený kontejner, ve kterém jsou firemní data chráněna.[73]

Obrázkové schéma názorně představuje architekturu platformy MobileIron včetně možností nasazení v podobě MobileIron Cloud, nebo v podobě on-premise.



Obrázek 11 - Architektura MobileIron [74]

Kromě Mobile@Work mezi další komponenty koncového uživatele patří AppConnect, Apps@Work, Docs@Work, Web@Work, Help@Work, a Tunnel.

AppConnect

MobileIron AppConnect kontejnerizuje aplikace pro ochranu podnikových dat a jejich oddělení od soukromého obsahu uživatele na zařízení. Jakmile je aplikace zabalena MobileIron AppConnect, stává se integrovanou do bezpečnostního kontejneru na zařízení.

Data v tomto kontejneru jsou pak šifrována a chráněna před neoprávněným přístupem včetně možnosti odebrání těchto dat v případě narušení bezpečnostních podmínek. [75]

Docs@Work

MobileIron Docs@Work je součást určená pro Mobile Content Management. Docs@Work poskytuje přístup k dokumentům přijatých emailem, sdílených on-premise nebo v cloudu a umožňuje takové dokumenty prohlížet, upravovat a sdílet. Docs@Work chrání dokumenty před neautorizovaným přístupem, poskytuje zabezpečení včetně DLP, kdy konfigurace této komponenty je prováděna pomocí MobileIron Core. Konfigurace zahrnuje napojení na Sharepoint, Dropbox, Box, OneDrive, Office 365 aj. Docs@Work zahrnuje také kontrolu a skenování emailů na přílohy, kde lze vynutit otevření přílohy pouze v této komponentě a je tak zajištěn pracovní prostor obsahu. Zajímavostí jsou published sites a content synchronization, kde published sites jsou umístění konfigurované vzdáleně administrátory a jejich obsah je zabezpečeně uložen a synchronizován do zařízení a následně dostupný offline.[76]

Web@Work

Zabezpečený mobilní webový prohlížeč Web@Work zajišťuje uživatelům snadný přístup k interním webovým aplikacím a zdrojům. Provoz probíhá skrze MobileIron Sentry pro bezpečný přenos dat a řízení přístupů včetně možnosti split tunelu. V případě nedodržení shody zařízení s bezpečnostními pravidly, může být přístup k webovým aplikacím odebrán a tunel zablokován. Cache, cookies, historie procházení a další data webových stránek Web@Work šifruje a i tento obsah podléhá správě MobileIron, a tak při odpojení zařízení dojde ke smazání, případně pokud zařízení nebude ve shodě. Aplikace podporuje DLP metody restrikcemi na volby otevírání obsahu v jiných aplikacích, případně restrikce na kopírování a vkládání. Administrátoři mohou také uživateli přímo definovat záložky na webové aplikace tak, aby firemní zdroje byly dostupné bez zatížení uživatele nadbytečným ručním nastavením.[77]

Apps@Work

Apps@Work lze označit jako firemní aplikační portál, který řídí jak in-house, tak aplikace třetích stran, doručované k uživatelům. Apps@Work zajišťuje knihovnu aplikací a jejich distribuci, zabezpečení a řízení přístupu a také seznam použitých aplikací. Řídit lze automaticky instalované aplikace, lze určovat povolené nebo zakázané aplikace, administrátoři mohou také svázat s managementem aplikací bezpečnostní politiky.[78]

Help@Work

Help@Work usnadňuje život uživatelům v momentě potíží se zařízením. Uživatel může přes Help@Work požádat správce o pomoc, nemusí složitě vysvětlovat a popisovat problém na Helpdesk a ušetří tak svůj čas. Uživatel klikne na tlačítko a může sdílet plochu svého zařízení. Jde o nástroj pro jednoduchou a efektivní podporu, umožňující dálkovou diagnostiku zařízení, prohlížení vzdálené obrazovky zařízení, v případě Androidu i vzdálené ovládání.[79]

Tunnel

MobileIron poskytuje Multi-OS App VPN, neboli nazvaný Tunnel, který řeší problematiku VPN na zařízení tak, aby VPN připojení bylo dostupné jen pro konkrétní autorizované aplikace, zařízení a uživatele. Ověřování probíhá na základě certifikátů. MobileIron Tunnel vytváří bezpečný a šifrovaný tunel, poskytující bezpečný přístup uživatele k firemním datům a zdrojům, s podporou pro iOS a Windows Phone. Šifrovaný tunel per app VPN pak lze využít pro jakoukoliv aplikaci jak in-house, tak veřejnou. Nastavení vytváří a má pod podhledem administrátor. Ostatní aplikace na zařízení, například soukromé v programu BYOD přístup k šifrovanému tunelu nemají.[80]

Email+

Aplikace Email+ je kompletní řešení pro bezpečný přístup uživatelů k firemnímu osobnímu emailu, kalendáři, kontaktům a úkolům. Email+ lze označit jako PIM komponentu od MobileIronu. Aplikace poskytuje šifrování, ověření na základě certifikátů, S/MIME podepisování a šifrování zpráv, umožňuje integraci s Web@Work tak, aby se odkazy z emailu otevřely pouze v zabezpečeném prohlížeči, nebo integraci s Docs@Work tak, aby přílohy emailů byly uchovány v bezpečném úložišti firemního obsahu, integraci

s dalšími prvky AppConnect případně omezení funkcí jako tisk, copy/paste nebo open in pro další ochranu ztráty dat. Email+ je PIM řešení pro situace, kdy společnostem nedostačují možnosti konfigurace nativních emailových klientů (nativních PIM). Email+ je dostupný pro platformu iOS a Android.[81]

Všechny komponenty na zařízení uživatele při každém spuštění kontrolují dodržení bezpečnostních zásad, a pokud nastane nesoulad s nastavenými pravidly, je uživateli znemožněn přístup k firemním aplikacím a obsahu do doby než bude zařízení splňovat všechny nutné podmínky.

3.5.3.3 IBM

IBM v oblasti EMM přichází s produktem MaaS360. Řešení mobility u IBM spadá pod IBM Security. Zde MaaS360 pracuje v synergii s ostatními IBM Security produkty, jako Trusteer či Qradar, a také s nabídkou IAM od IBM. MaaS360 podporuje základní platformy jako iOS, Android a Windows Phone. IBM je jeden ze zakládajících členů standardu AppConfig a nabízí širokou podporu pro aplikace třetích stran ISV. Produkt Maa360 od IBM se vyznačuje snadným zavedením a působí jako komplexní EMM řešení. MaaS360 vznikl, jako cloudová služba, on-premise nasazení bylo nějakou dobu dostupné, ale v současné je MaaS360 pouze ve variantě cloudové služby. Vývojová větev varianty on-premise byla ukončena.[27]

Silné stránky [27]:

- pro společnosti se zájmem o EMM jako cloudové služby, je silnou stránkou vývoj produktu MaaS360 od počátku v tomto směru a z toho vyplývající zkušenosti a odladěný systém v oblasti poskytování EMM jako služby v cloudu,
- content management s produktem BOX (IBM a BOX),
- aplikační management a distribuční schopnosti,
- silná jednotná správa koncových bodů (UEM) včetně vylepšené integrace s IBM BigFix,
- integrace s QRadar, která umožňuje správcům vytvářet automatické akce na zařízení, založené na bezpečnostních událostech nebo na nově objevených zranitelnostech.

Slabé stránky [27]:

- malá působnost u velkých společností a spíše z velké části implementace v menších a středních společnostech,
- občasné zaostávání za konkurencí s novými funkcemi a inovacemi,
- komplikované odebírání záznamů zařízení odhlášených z EMM, a jejich zabírání licencí.

Detail řešení

IBM představuje MaaS360 pomocí několika provázaných součástí.

Obrázek 12 - Komponenty IBM Maas360 [82]

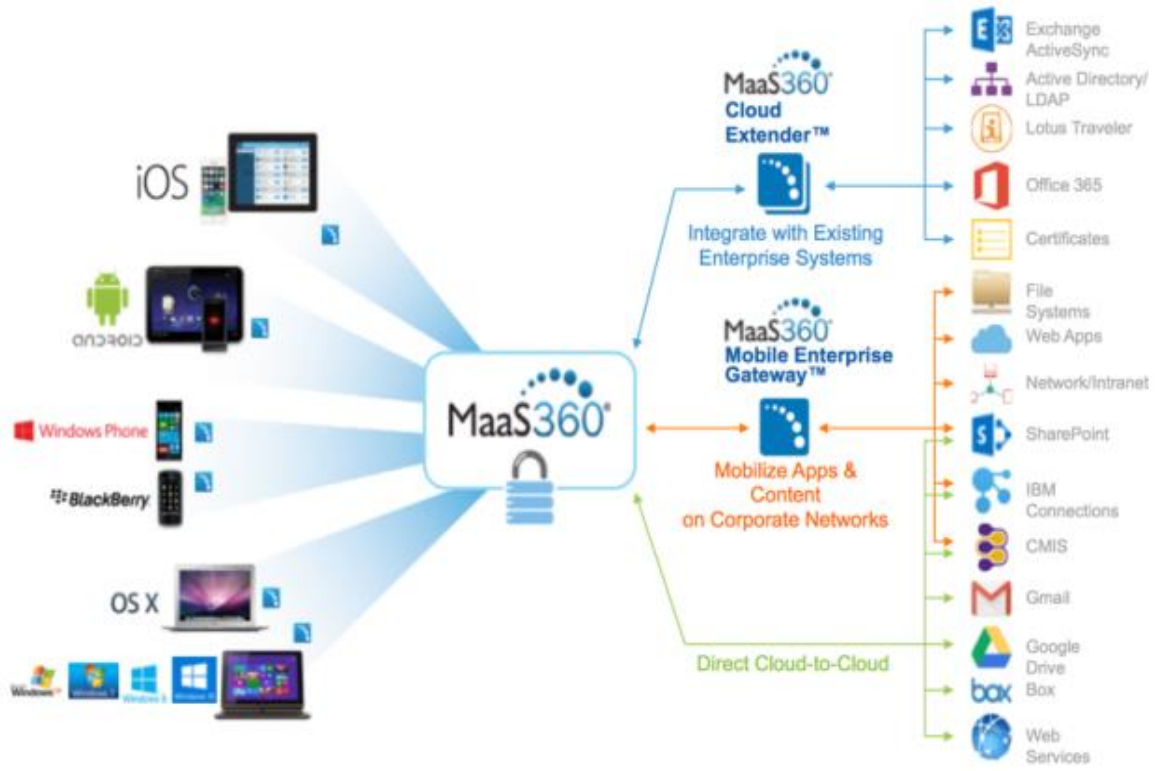
Management suite je integrace funkcí určených pro MDM a MAM. MaaS360 podporuje řadu významných platforem a známé typy zařízení. Aplikace jsou distribuovány pomocí firemního aplikačního portálu. Systém podporuje napojení na již existující infrastrukturu společnosti jako Active Directory, MS Exchange, Office 365 apod.[82]

Productivity suite obsahuje základní pracovní nástroje pro email, přílohy, aplikace a webový obsah. Zajišťuje kontejnerizací oddělení firemního a soukromého obsahu na zařízení. MaaS360 má vlastní Secure Mobile Browser, pro konfigurovatelný a bezpečný přístup k intranetovým zdrojům.[82]

Content Suite poskytuje chráněný kontejner pro distribuci, prohlížení, vytváření, editaci a sdílení dokumentů na mobilních zařízeních. Content Suite zajišťuje přístup k distribuovanému obsahu a cloudovým úložištím jako je například Microsoft SharePoint, Box, OneDrive a Google Drive. Samozřejmostí je podpora zajištění obsahu proti ztrátě citlivých dat.[82]

Gateway Suite umožňuje přístup k prostředkům firemní infrastruktury, jako Sharepoint, Intranet, z mobilních zařízení bez nutnosti vytváření VPN tunelu, což zjednodušuje připojení uživatele k firemním zdrojům při zachování požadované bezpečnosti.[82]

Threat Management nabízí, přímo z konzole EMM, řešit zabezpečení mobilních zařízení proti malware útokům a incidentům. Threat management běží na integrované technologii IBM Tresteer.[82]



Obrázek 13 - Architektura IBM MaaS360 [83]

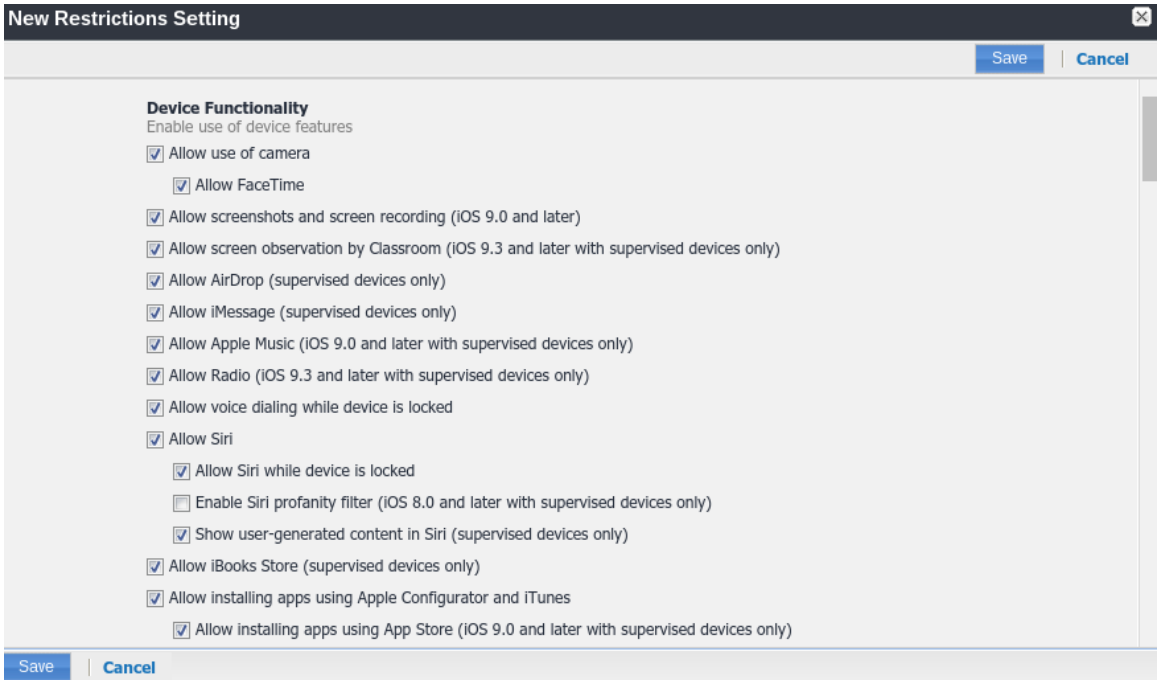
3.5.4 Apple

Apple mobilní zařízení jsou primárně cílena na spotřebitele, nikoliv pro podnikové použití. Sám Apple ale postupně rozvíjí podporu svých zařízení ve firemním nasazení a postupně doplňuje nové funkce pro správu svých mobilních zařízení. IPad, iPhone nebo

iPod touch lze převést na supervised zařízení. Společnosti mohou využít Device Enrolment Program pro rychlé nasazení iOS zařízení a Volume Purchase Program pro snadný nákup a distribuci aplikací.

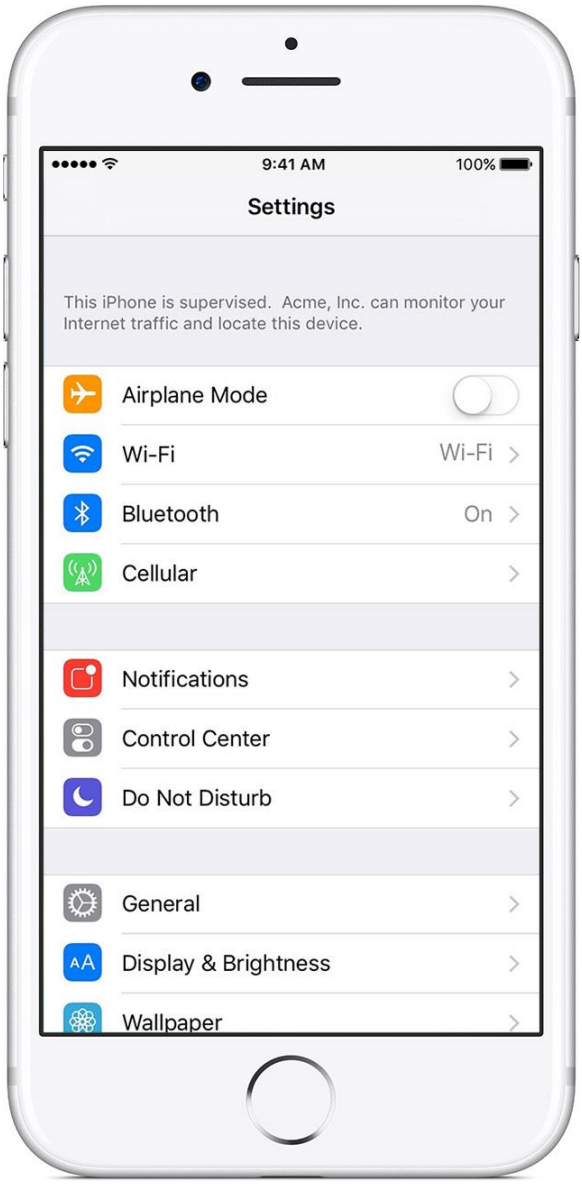
Supervised zařízení

Supervised zařízení bylo představeno jako novinka v iOS verze 5, za účelem rozšíření funkcí pro správu firemních zařízení. Apple tím pro administrátory rozšiřuje portfolio možných nastavení na zařízení iPad, iPhone a iPod Touch. S každou novou verzí iOS přichází Apple s rozšířenými management funkcemi a restrikcemi pro supervised zařízení. Příkladem může být funkce single-app mód, restrikce na zabránění automatického stahování aplikací, tichá instalace aplikace na pozadí, always-on VPN a další. Nové management funkce pak mohou využívat platformy EMM a rozšířit tak funkce pro správu. Pak je nutné rozlišovat klasická zařízení sprofilem EMM a supervised zařízení, která mohou být také spravována pomocí EMM.Například jak demonstruje níže obr. č.14, některé z restrikcí jsou dostupné pouze pro supervised zařízení.[84], [85],[86]



Obrázek 14 - Nastavené iOS restrikcí a supervised mód [87]

Supervision mód je obvykle zahájen během instalace zařízení. Ve výchozím nastavení zařízení nejsou supervised. Zařízení do tohoto módu lze převést pomocí DEP programu nebo za pomoci Apple Configuratoru.[84], [85],[86]



Obrázek 15 - Supervised mód informuje uživatele iOS v nastavení [85]

Device Enrollment Program

Device Enrollment Program (DEP) poskytuje rychlé a zjednodušené nasazení a konfiguraci iOS zařízení, která jsou nakoupená od společnosti Apple nebo od autorizovaných prodejců společnosti Apple. DEP umožňuje aktivaci supervised módu

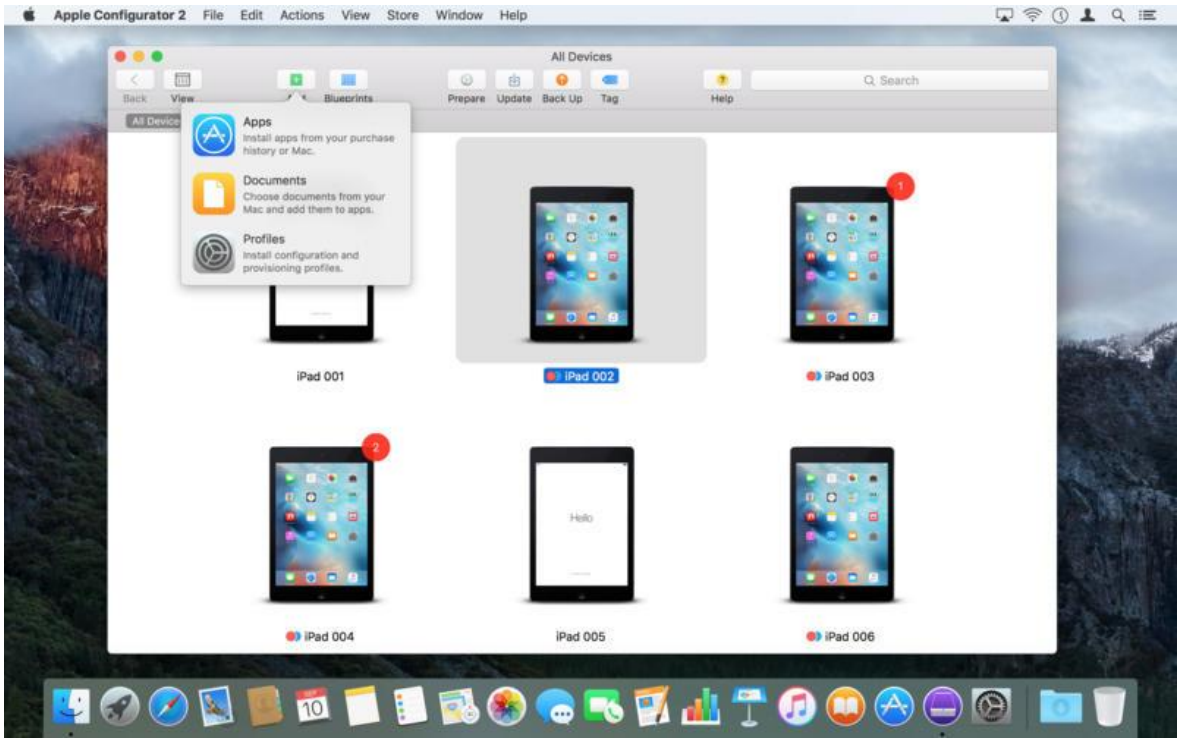
zařízení a je možné přes DEP před konfigurovat automatické zařazení do MDM systému. Zjednodušuje se tak počáteční nastavení tím, že automatizuje zařazení zařízení do MDM systému a aktivaci supervised módu nad těmito zařízeními už během instalace. To zaručuje, že všichni uživatelé obdrží potřebné konfigurace ve svých zařízeních bez dalších postupů. Uživatel může do rukou dostat zařízení, které se po aktivaci nastaví dle potřebných pravidel (nastavení účtu, aplikací, apod.) bez nutnosti přístupu administrátora ke každému zařízení zvlášť. Pro další zjednodušení procesu je možné přeskočit určité Setup Assistant obrazovky, takže uživatelé mohou začít používat svá zařízení hned po vybalení z krabice.

Co se týká limitů, tak zařízení, která lze přidat do DEP musí být zakoupena po 1. 3. 2011 a musí mít iOS verze 7 a vyšší. Navíc Device Enrollment Program není dostupný pro všechny země. Ale po dlouhém čekání je od konce roku 2016 dostupný i pro Českou republiku.[88], [89]

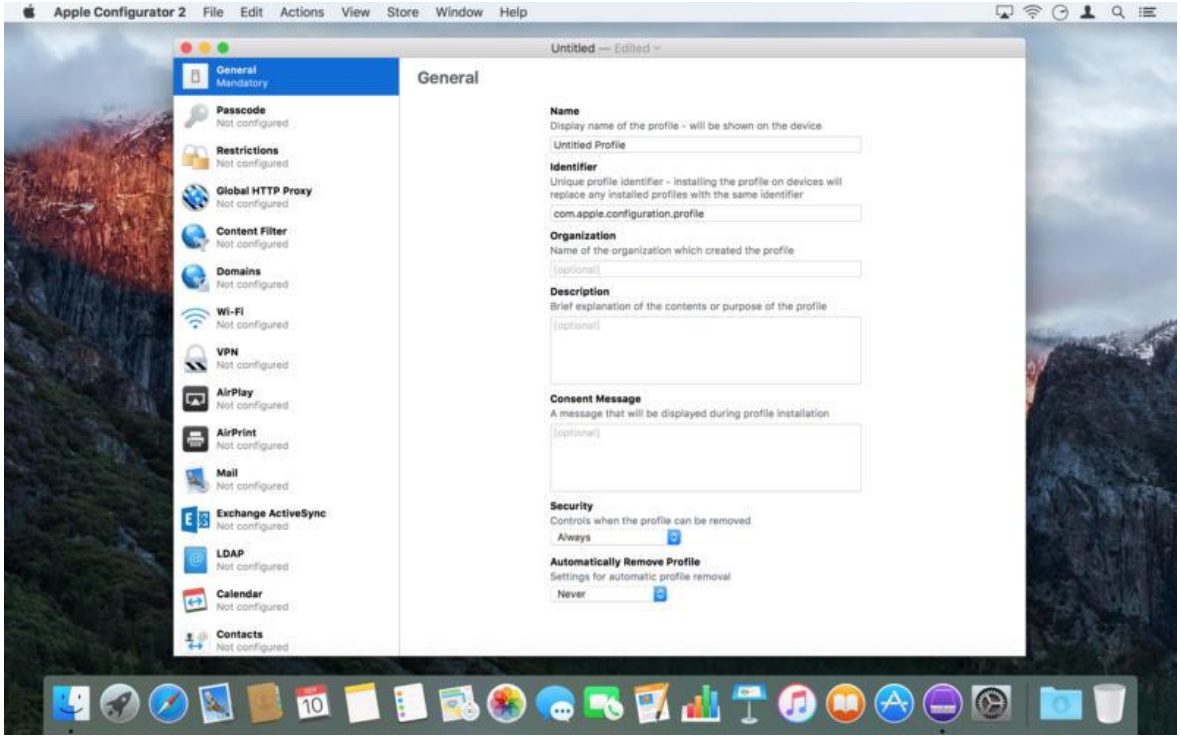
Obrázek 16 - Dostupnost DEP programu ve světě [90]

Apple Configurator

Apple Configurator je nástroj pro instalaci a konfiguraci zařízení se systémem iOS připojených přes UBS rozhraní. Jde o aplikaci, která je pro MAC OS X distribuována zdarma. Hlavním účelem aplikace je umožnit správcům IT konfigurovat nastavení na zařízení iPhone a iPad předtím než budou vydána koncovým uživatelům. Pomocí aplikace mohou správci vytvářet konfigurační profily, instalovat určité verze operačního systému a prosazovat zásady zabezpečení mobilních zařízení.[91]



Obrázek 17 - Apple Configurator - zařízení [92]



Obrázek 18 - Apple Configurator - editace profilu [92]

Volume Purchase Program

Volume Purchase Program (VPP) usnadňuje hromadný nákup a distribuci aplikací a knih pro firemní mobilní zařízení. Nákup je možný z App Store a Mac App Store, v případě knih z iBook Store. VPP umožňuje distribuci také vlastních B2B aplikací. Hlavní výhodou je distribuce směrem k uživateli. Pro správu distribuce se může použít MDM (EMM), které se napojí na VPP účet, nebo lze také použít Apple Confirugator 2. Distribuční proces aplikace je kontrolován do začátku do konce. Jakmile je aplikace na zařízení nepotřebná, lze ji vrátit zpět, případně distribuovat na jiné zařízení. Aplikace zakoupené a distribuované prostřednictvím VPP lze přiřadit uživateli nebo zařízení v jakékoliv zemi, kde je daná aplikace k dispozici. U knih není možnost opětovné distribuce na jiné zařízení. Jakmile je kniha distribuována do iBooks, zůstává majetkem příjemce. [93], [94]

4 Vlastní práce

Vlastní část práce se věnuje fiktivní společnosti, která řešila problematiku zařazení iOS zařízení do svého prostředí. Vzhledem k zajímavosti oboru a dosavadním zkušenostem autora práce byla zvolena fiktivní společnost z oboru letectví. Letectví je oblast kladoucí velký důraz na bezpečnost, a z toho mohou vyplynout zajímavé požadavky na mobilní zařízení, které jsou v ostatních společnostech řešeny okrajově, případně řešení správy mobilních zařízení nemusí být tak funkcionálně vytěžována jako právě v letecké společnosti. Vlastní práce uvede fiktivní leteckou společnost a projekt, který spustil změny v přístupu k mobilním zařízením v rámci společnosti. Ačkoliv projekt startoval v minulosti, autor práce ponechává začátek v letech minulých s postupným přechodem událostí do současného stavu tak, aby byl zřejmý postupný vývoj a bylo možné zmapovat úskalí a přístup k řešení mobilních zařízení v této konkrétní fiktivní letecké společnosti.

4.1 Letecká společnost

V praktické části se autor zabývá zavedením mobilních zařízení v letecké společnosti Letím bezpečně a.s., která na trhu působí přibližně 12 let a patří mezi lídry business aviation ve střední a východní Evropě. Společnost provozuje více než desítku business jetů, zaměstnává okolo 200 zaměstnanců, zahrnující posádky, technické oddělení, handling oddělení, operační oddělení, oddělení pro plánování a administrativu včetně vlastního IT oddělení. Společnost poskytuje široké portfolio služeb na trhu provozu, správě a managementu business jetů včetně dalších, doplňkových služeb z oblasti business aviation.

Služby poskytované společností:

- provozování letadel,
- handling a hangárování,
- opravy a údržba letadel,
- prodej letadel,
- charterování letů a brokerage,
- plánování a podpora letů,
- poradenské služby,
- travel management.

Business aviation trh je velmi rychle rostoucí a dynamický, a tak pro úspěch každé letecké společnosti je důležité být vždy o krok napřed oproti konkurenci. S tím souvisí i vlastní část této práce, která pojednává o projektu nasazení mobilních zařízení do kabin letadel, který měl pomoci společnosti v dosažení jejích cílů, což především zahrnuje udržení vedoucí tržní pozice na poli střední a východní Evropy, zlepšení efektivity práce a snížení nákladů. Projektu, který započal v roce 2013, bude věnována vlastní část. Z důvodu komplexnosti a ucelenosti se práce vrátí do minulosti a přiblíží některé z oblastí nasazení mobilních zařízení v této letecké společnosti, s vyzdvihnutím oblastí, které byly například problematické, zajímavé nebo takové, se kterými byl autor práce přímo konfrontován. Nastíněna bude většina kroků, které byly zahrnuty v daném projektu z ohledu odpovědnosti IT oddělení, v některých částech i nad rámec těchto odpovědností.

4.1.1 IT oddělení

IT oddělení společnosti v roce 2013 zahrnovalo pracovníka IT server administrátor, IT support a IT developer pod vedením manažera celého IT oddělení. Další doplňkovým zdrojem IT oddělení byl 1 MD správce sítě týdně formou outsourcingu a dále několik desítek MD pro vývoj vlastních aplikací. Společnost měla vlastní on-premise infrastrukturu, kterou spravovalo IT oddělení s pomocí outsorcing podpory.

4.1.2 Infrastruktura

Stav infrastruktury společnosti v roce 2013 byl následující.

On Premise umístění bylo rozděleno z důvodu vysoké dostupnosti v oddělených lokalitách, hlavní serverovna v jedné budově a druhá, menší serverovna v budově druhé. Serverová část byla zastoupena zařízeními IBM/Lenovo, operačním systémem Microsoft ve verzích Windows Server 2008 a vyšší. Použitá technologie virtualizace byla od Microsoft, Hyper-V. Poštovní server byl nasazen Microsoft Exchange ve verzi 2010 a databázový server Microsoft SQL Server 2008 R2. Společnost disponovala jedním terminálovým serverem Microsoft Windows Server 2003 určeným přibližně 20 uživatelům. Pro část mobilních zařízení soužil BlackBerry Enterprise Server v edici Express. Microsoft prostředí bylo podpořeno i vlastní Microsoft certifikační autoritou.

Mezi síťové prvky spadaly páteřní switche Hewlett-Packard, bezdrátová síť byla tvořena radius servery a aktivními prvky od společnosti Ruckus. Vzdálený přístup do sítě společnosti pomocí VPN byl zajištěn prvky Cisco, kde softwarovým vybavením klienta byl Cisco AnyConnect VPN client. Výhodou tohoto VPN řešení byla spolehlivost a dostupnost klienta pro většinu platforem jak klasického, tak mobilního zařízení.

Hlavní datové připojení společnosti zajišťovalo symetrické mikrovlnné spojení o kapacitě 20 Mbit download a 20 Mbit upload. Náhradní připojení pro případy výpadku hlavního spoje bylo typu ADSL, některá oddělení měla pro případy výpadku hlavního připojení připraveny USB modemy s datovými SIM kartami.

Vzhledem k povaze práce skupiny uživatelů společnosti v režimu 24 hodin, 7 dní v týdnu a 365 dní v roce bylo vždy cílem prvky infrastruktury udržovat ve vysoké dostupnosti. Ve většině případů prvků sítě a serverů byl tento cíl splněn. Například Exchange Servery byly nasazeny v clusteru s loadbalancing provozem, SQL server pro klíčové databáze měl nastavené zrcadlení. V případě virtualizace se využívalo clusteru. Bolestivým místem vysoké dostupnosti bylo datové připojení, které mělo náhradu pouze ve slabém a pomalém ADSL připojení, případně nouzovým řešení datového USB modemu na jednotlivých uživatelských stanicích.

4.1.3 Odpovědnosti IT

IT oddělení ve společnosti mělo pod správou celou svou infrastrukturu. Členové oddělení IT se starali o údržbu a zálohování serverů a údržbu sítě, také o samotné uživatele, které vybavovali technikou, přístupy do systémů a zabezpečovali podporu těchto uživatelů.

Součástí odpovědností IT oddělení bylo také zajištění bezpečnosti celé infrastruktury a nutných procesů vedoucích k omezení možných rizik.

Vzhledem k charakteru růstu IT odvětví bylo nezbytné, aby IT oddělení společnosti reagovalo a udržovalo krok s vývojem této oblasti. Odpovědnostmi IT oddělení bylo zavádění nových systémů, rozšiřování stávající infrastruktury a příprava plánů a nákladů pro další roky tak aby bylo napomáháno dosahování cílů společnosti.

Nedílnou součástí IT infrastruktury byla mobilita společnosti. IT bylo zodpovědné za řešení otázky nasazení mobilních zařízení, jejich zabezpečení a přiřazení k uživatelům, vše v souladu s tím, aby mobilní zařízení bylo podpůrným prostředkem pro práci zaměstnanců

a bylo tak dopomáháno k vyšší výkonnosti a efektivitě. Jaký zvolit model přístupu mobilních zařízení, jak provádět vzdálené ovládání a správu zařízení, jak posílit bezpečnost v mobilní sféře, to bylo na pomyslném pracovním stole v popředí s vysokou důležitostí.

4.1.4 Mobilní zařízení ve společnosti

Strukturu mobilních zařízení bylo možné dělit do skupin několika způsoby.

Podle synchronizace zařízení:

- zařízení bez synchronizace emailového účtu,
- zařízení se synchronizací emailového účtu.

Prvním a již pomalu mizícím typem bylo zařízení bez funkce synchronizace emailového účtu. Typickým zástupcem této skupiny byl klasický tlačítkový telefon, například Nokia C5. Druhý typ mobilního zařízení umožňoval synchronizaci emailového účtu. Taková zařízení bylo možné dále dělit na zařízení BlackBerry s možností registrace na BES server, a pak smartphone a tablet, které disponovali nastavením MS Exchange profilu pomocí EAS.

Podle vlastnictví zařízení:

- firemní zařízení,
- soukromá zařízení zaměstnanců.

Firemní zařízení bylo nakoupeno společností, podle pozice uživatele, pro kterého bylo zařízení určeno a dle dostupných modelů v dané době a cenové relaci. Soukromá mobilní zařízení zaměstnanců si zaměstnanci nakoupili pro sebe a pro vlastní užitek, s tím že se mobilní zařízení dále objevilo ve společnosti v režimu synchronizace firemního emailu.

Správu mobilních zařízení společnost řešila více způsoby. Firemní zařízení, která nesynchronizují firemní email, při vydání IT oddělení doplnilo o firemní kontakty a předalo uživateli. Možnosti další správy zařízení se v těchto případech neřešily. Firemní zařízení, u kterých bylo možné nastavit synchronizaci firemního emailu, byla spravovaná

pomocí BES serveru nebo pomocí MS Exchange serveru, vždy dle typu zařízení. BlackBerry zařízení s verzí sytému nižší než 7 bylo možné registrovat na BESserveru. Ostatní, smartphone zařízení nebo tablety s podporou konfigurace EAS, byla spravována pomocí MS Exchange. Soukromá zařízení byla spravována pomocí MS Exchange, uživatelé měli k dispozici návod jak nastavit firemní email ve svém zařízení.

Počet mobilních zařízení

Ve společnosti byly identifikovány počty mobilních zařízení, které se připojují k firemnímu obsahu. Přehled je k dispozici v tabulce č. 3.

Tabulka 3 - Počet mobilních zařízení ve společnosti

	iOS	Android	BlackBerry	Windows	Celkem
Telefon	15	30	10	10	65
Tablet	5	2	0	0	7
Celkem	20	32	10	10	72
Soukromé (odhad)	8	15	0	1	

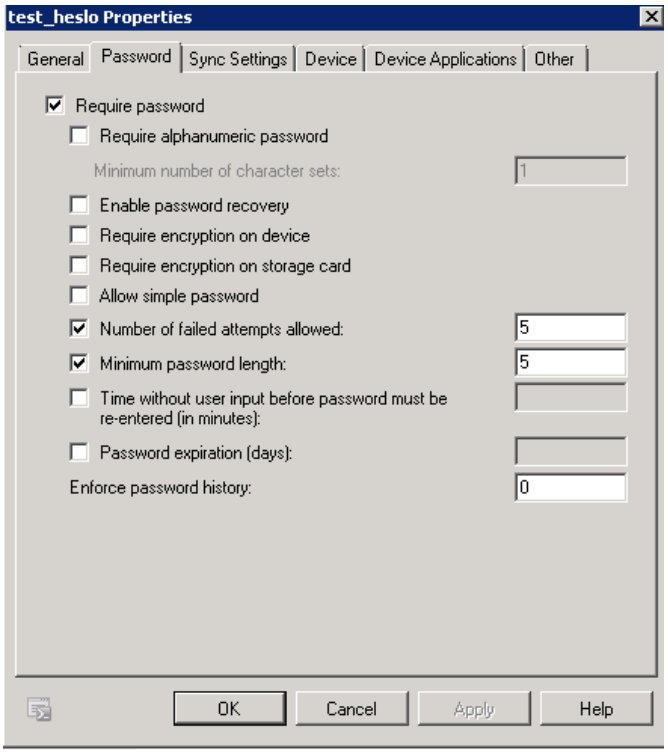
Zdroj: vlastní zpracování

Počet soukromých zařízení byl odhadován, připojení k firemnímu obsahu nebylo pod přímou kontrolou.

Zabezpečení mobilních zařízení

EAS a BES server umožňují nastavení bezpečnostní politiky. V této společnosti byla nastavena s následujícími atributy:

- minimální délku hesla nastavena na 5 znaků,
- není vyžadováno číslo nebo speciální znak v hesle,
- není specifikováno, jak dlouho mobilní telefon může být neaktivní, než je uživatel povinen znovu zadat heslo,
- po 5. špatném zadání hesla se smaže zařízení (WIPE).



Obrázek 19 - Příklad konfigurace Exchange ActiveSync Mailbox Policy [95]

Bezpečnostní politika byla doručena pouze na 40 % mobilních zařízení. Vzhledem k absenci právního ošetření BYOD, nebyla bezpečnostní politika aplikována na soukromých mobilních zařízeních s přihlášeným firemním emailem. Ihned vznikla otázka jak tuto situaci řešit.

4.2 Projekt

V roce 2013 byl ve společnosti spuštěn projekt nahrazení stávajících EFB zařízení v kokpitech letadel za mobilní zařízení iPad. Autor práce byl součástí týmu, který pracoval na části tohoto projektu týkající se odpovědnosti IT oddělení, a v současné době dále provádí administraci správy mobilních zařízení.

Projekt nasazení mobilních zařízení do kabin letadel byl rozsáhlý projekt a tato práce se věnuje části projektu, které spadaly pod povinnosti IT oddělení. Další části projektu, které nejsou v této práci obsaženy, spadají do následujících oblastí – vývoj, certifikace a instalace držáku zařízení do letadel, úpravy letových manuálů, procesů a schvalování letovými úřady, přeškolení posádek.

Cílem projektu bylo vymontování původních EFB zařízení z letadel a nahrazení stávajícího EFB zařízení iPadem. Součástí záměny byla příprava celé platformy v letadlech pro připojení iPadu, například datová sběrnice, nabíjení a další úpravy. Hlavním cílem projektu bylo snížení nákladů, převážně na licencování mapových podkladů a dále zvýšení efektivity posádek, vzhledem k obměně zařízení na modernější iPad s vyšším potenciálem provozovaných aplikací. Dalším cílem projektu bylo zřízení centrální správy iPadů pro vzdálené řízení zařízení, doručování obsahu, pro vzdálené smazání, vzdálenou instalaci čehokoliv co bude na iPadu potřeba. Požadavkem bylo také do iPadů doručovat aktuální firemní dokumentaci a manuály určené pro posádky tak, aby měli piloti na palubě, vždy po ruce správné verze dokumentů, formou paper less cockpitu.

Zajištění centrální správy iPadů, výběr zařízení, zajištění nákupem a předání posádkám bylo zařazeno pod odpovědnost IT oddělení.

Vzniklé požadavky na IT oddělení:

- zajištění centrální správy,
- výběr a nákup zařízení,
- proškolení posádek na používání iPadu,
- úprava vnitřních předpisů vzhledem k budoucím změnám.

4.3 Požadavky

Požadavky na zařízení, aplikace a správu mobilních zařízení byly výsledkem zadání projektu. Souhrn těchto požadavků je obsažen v následujících podkapitolách. Ačkoliv požadavky na mobilní zařízení a aplikace jsou definovány pouze z pohledu záměny EFB zařízení v letadlech, požadavky na centrální správu jsou dále specifikovány hlouběji tak, aby centrální správu mobilních zařízení bylo možné použít nejen pro oblast náhrady EFB, ale naopak pro celou společnost. Takové rozhodnutí mělo za cíl pokrýt celou oblast mobilních zařízení ve společnosti, včetně BYOD, a využít tak situace pro celkové zlepšení zabezpečení společnosti v oblasti mobilních zařízení. Tato analýza požadavků byla nezbytným krokem, pro to aby následná implementace projektu byla úspěšná. Přihlédlo se nejen k požadavkům managementu a IT správců, ale byly také zohledněny požadavky běžných uživatelů. Správným rozhodnutím nepochybně bylo zahrnutí klíčových uživatelů, kteří měli s mobilními zařízeními pracovat, do jednání a konzultací při určování

požadavků, neboť informace z jejich strany byly nepochybně přínosem. Skutečnost zahrnutí těchto uživatelů do procesu tvorby představovala jistotu jejich následné spolupráce, jelikož měli možnost se účastnit diskuzí a některé z jejich požadavků byly do řešení následně zapracovány.

4.3.1 Požadavky na zařízení

Mezi základní požadavky, které mělo mobilní zařízení pro posádky splňovat, patřily:

- jednoduché a intuitivní ovládání,
- stabilní platforma,
- dostupnost požadovaných aplikací pro danou platformu,
- možnost schválení Úřadem pro civilní letectví,
- dostupnost minimálně 50 ks zařízení u možného dodavatele,
- dostatečný výkon a výdrž na baterii,
- kapacita zařízení 64 GB,
- velikost okolo 10 palců,
- 3G/LTE modul,
- kladné zkušenosti z oblasti EFB zařízení.

4.3.2 Požadavky na aplikace

Přechod posádek na iPady byl podmíněn několika požadovanými aplikacemi. Jejich seznam je níže uveden s krátkým doplněním:

- Jeppesen – mapové podklady.
- Weight&Balance – aplikace, například iPreFlight od APG, pro tvorbu loadsheetu, dokumentu s vizuálním zobrazením letové obálky a výpočtem těžiště letadla pro různé fáze letu.
- RWY Analysis.
- Aplikace pro zobrazení dokumentů (různých typů, ale převážně PDF) – zobrazení dokumentů výrobce letadla a také dokumentů společnosti, včetně integrované funkce pro synchronizaci pouze aktuálních verzí dokumentů v režimu online, ale dostupné za letu, při datovém offline režimu zařízení.

- E-mail aplikace – možné použití nativní aplikace Mail.
- Aplikace pro VPN připojení.
- Webový prohlížeč – prohlížeč nejen pro internetové stránky ale také pro intranetové stránky společnosti.
- Aplikace pro vytváření dokumentů – obdoba MS Word a Excel pro mobilní zařízení.
- Webový prohlížeč s flash – pro účely školení, které jsou dostupné na webu, ale je nutné mít v prohlížeči aktivní flash.
- Aplikace pro sledování videa – pro účely školení.

4.3.3 Požadavky na centrální správu

Centrální správa mobilních zařízení měla být budoucím komplexním řešením firemní mobility. Na základě několika interních setkání zástupců IT oddělení vznikl seznam několika poznatků, problematiky a požadavků, který měl nový systém mobilní správy řešit.

- Centrální správa z jediného místa
    - Administrátoři nyní obsluhovali dvě oddělená řešení – BlackBerry server a Exchange server, kde navíc nebyla zmapována celá oblast připojených uživatelů.
- Podpora většiny mobilních platforem – iOS, Android, Windows Phone, BlackBerry
- Inventarizace mobilních zařízení
    - V dané době forma inventarizace byla prováděna tabulkami v MS Excel a bylo složité provádět inventarizaci. Nové řešení mělo v určitém měřítku napomoci při inventarizaci, nicméně se zrušením tabulek nebylo počítáno.
- On-premise instalace
    - Důraz byl kladem na instalaci mobilní správy ve vlastním prostředí. Důvodem bylo problematické datové připojení bez plnohodnotné zálohy a obava z nevýhod cloudového řešení (zálohování, právní oblast, citlivost některých dat, napojení do vlastních systémů).
- Dobrý poměr cena/výkon
    - Byl očekáván dobrý poměr ceny a výkonu řešení.

- Funkce pro oddělení firemního a soukromého obsahu na zařízení (podpora BYOD zařízení)
    - V případě soukromého obsahu na zařízení, tento obsah oddělit od firemní části zařízení tak, aby mezi nimi nebylo propojení. Uživatelé tak budou moci instalovat aplikace soukromě, ale na zařízení bude nastavena firemní politika, které budou podléhat včetně firemních aplikací.
- Vzdálená konfigurace VPN
    - Byla potřebná funkce pro vzdálenou konfiguraci Cisco AnyConnect VPN klienta.
- Firemní aplikační portál
    - Portál by měl uživatelům nabídnout aplikace potřebné pro jejich práci. Administrátorům by měl portál umožnit vzdálenou distribuci aplikací.
- Nástavba nad aplikacemi (SDK, Wrapping)
    - V této části by mělo řešení nabídnout rozšířené možnosti zabezpečení, kontroly nad daty aplikací a jejich fungování na mobilní datové síti.
- Navázání akcí uživatele na firemní politiky
    - Příkladem může být vynucená instalace aplikace tak, že pokud uživatel nebude mít na iPadu takovou aplikaci instalovanou bude podléhat nějakým způsobem restrikcím (blokování firemního obsahu, omezení některých funkcí). Stejné chování by mělo nastat v případě, pokud uživatel nebude splňovat bezpečnostní pravidla (délku vstupního hesla, maximální čas zamknutí zařízení při nečinnosti).
- Zjištění polohy přístroje
- Podpora a propojení s doménou (skupiny, ověřování uživatelů)
    - Požadováno bylo převzetí skupin a uživatelů z MS Active Directory a možnosti správy mobilních zařízení například pomocí AD skupin.
- Řídit zařízení v rámci jejich zařazení do skupiny
    - Umožnit administrátorů řídit politiky pro skupiny zařízení.
- Napojení na intranet a další interní aplikace

- Možnost vynutit vstupní heslo na zařízení
    - Požadavkem byla sada pravidel pro bezpečnostní politiku jako heslo na vstup do zařízení, délka a složitost tohoto hesla a po jaké době nečinnosti má být zařízení zamknuto.
- Možnost využití certifikátů
    - Společnost měla vlastní certifikační autoritu, a tak bylo uvažováno o jejím využití.
- Podpora MS Exchange 2010
    - Nutností byla podpora vzdáleného nastavení MS Exchange profilů do mobilních zařízení. Dále bylo počítáno s možností doručování více než jednoho EAS profilu na některá mobilní zařízení.
- DMS
    - Funkce pro synchronizaci dokumentů do zařízení
    - Funkce pro schvalování přečtení dokumentů
    - Kontrola aktuální verze dokumentů
- Zabezpečený webový prohlížeč
    - Řešení mělo nabídnout vlastní zabezpečený prohlížeč.
- Funkce pro vzdálené smazání zařízení (dále v práci zmínit odvolání příkazu na WIPE)
- Nastavení využívání 3G/WiFi nad aplikacemi
    - možnost nastavení, jak bude aplikace stahovat data. Například zakázat 3G, povolit 3G/WiFi zvlášť pro každou aplikaci.
- Spolehlivý a zkušený dodavatel
    - Mezi velmi důležité požadavky patřilo nalezení spolehlivého a zkušeného dodavatele s přidanou hodnotou tak, aby dokázal společnosti pomoci se zavedením centrální správy a dále toto řešení pomáhal udržovat v chodu.

4.4 Analýza rizik

Analýza rizik proběhla metodou interního bezpečnostního auditu. V návaznosti na audit proběhlo několik schůzek zástupců IT oddělení s auditorem. Společně bylo provedeno zhodnocení přítomnosti rizik a na základě toho byly definovány bezpečnostní politiky.

Mezi hlavní identifikovaná rizika patřil unik firemní dokumentace skrze mobilní zařízení, právně neošetřený BYOD a nekontrolovaný přístup mobilních zařízení k firemnímu obsahu. Samotná analýza rizik není předmětem zpracování této práce.

4.4.1 Bezpečnostní politiky

Na základě analýzy rizik byly obecně definovány bezpečnostní politiky.

Počet připojených zařízení

Standartní počet zařízení na uživatele jsou 2 ks, v konfiguraci jeden telefon a jeden tablet. Více zařízení je nutné schválit vedoucím oddělení a IT manažerem.

Definice a vynucení bezpečnostních opatření

Minimálním bezpečnostním opatřením je kódový zámek na zařízení o délce 5 znaků, a maximální počet neúspěšných pokusů zadání kódového zámku před smazáním zařízení je 10. Toto opatření bude vynucené pro každé připojené zařízení. Pro tablety bude tento kódový zámek mít trvanlivost 365 dní.

Pravidla pro používání zařízení

Zařízení mohou být používána v omezené míře pro soukromé účely. Je vyžadováno dodržování bezpečnostních opatření. V případě jejich porušení, nebo v případě nestandardního chování, může být ze zařízení odebrán firemní obsah, nebo dokonce může být zařízení smazáno.

Pravidla přístupu k firemnímu obsahu

Přístup k firemnímu obsahu je dostupný pomocí EMM komponent při dostatečné ochraně dat. VPN připojení v mobilním zařízení je nutné schválit vedoucím oddělení a IT

manažerem. Budou nasazena bezpečnostní opatření za účelem ochrany podnikových dat, převážně dokumentů.

Definice povolených platforem a přístrojů

Mezi povolené platformy patří Apple iOS, Microsoft Windows Phone, Google Android. Schválené přístroje bude, jako aktualizovaný seznam, vydávat každé čtvrtletí IT oddělení, včetně minimálních verzí operačních systémů.

Blacklist/Whitelist aplikací

List aplikací, které jsou schválené, včetně jejich verzí, bude vydáván IT oddělení dle potřeby. Vzhledem k obsahu verzí aplikací je počítáno s tím, že tento seznam, muže být aktualizován několikrát do měsíce.

Definice bezdrátových sítí

Jsou definovány dvě bezdrátové sítě určené pro mobilní zařízení. Jedna síť je určena pro telefony a druhá síť pro tablety. Síť pro telefony má rychlostní omezení. Registrace do obou sítí podléhá schválení vedoucího oddělení a zástupce IT.

Definice chování při ztrátě zařízení

Při ohlášené ztráty zařízení bude zařízení neprodleně na dálku smazáno. IT administrátor v momentě ohlášení ztráty odešle na zařízení příkaz na vymazání. Bylo připomenuto, že odeslání požadavku ještě neznamená skutečné vymazání, pokud zařízení po ztrátě již nebude připojeno k síti.

Procesy pro správu zařízení

Přidávání zařízení pod správu bude mít plně pod kontrolou IT oddělení. Budou eliminovány současné připojení mobilních zařízení k Exchange a budou vytvořeny nové, které budou evidovány a kontrolovány. Budou prováděny pravidelné kontroly připojených zařízení a budou pravidelně aktualizovány bezpečnostní politiky v zájmu zachování vysokého zabezpečení.

Právní ošetření (BYOD, polohové služby, soukromá data na zařízení)

BYOD zařízení zaměstnance bude ve společnosti povoleno po schválení vedoucím oddělení a IT manažera. Zaměstnanec požadující použití vlastního zařízení bude pro aktivaci firemního obsahu muset podepsat dohodu mezi jím a společností. Dohoda obsahuje potřebné právní ošetření a zaměstnanec podpisem stvrdí souhlas s nastavenými podmínkami. Na BYOD zařízení budou při povolování firemního obsahu doručeny potřebné bezpečnostní politiky.

4.5 Výběr zařízení

Vybrané mobilní zařízení bylo již určeno v úvodu projektu. Tato část práce pouze objasní důvody rozhodnutí pro výběr vhodné náhrady stávajícího EFB právě Apple iPadem. V dané situaci bylo několik známých zkušeností s instalací mobilních zařízení v cockpitu letadla, a to s mobilním zařízením Microsoft Surface a s Apple iPadem. Apple zařízení pro výběr dopomohl vybraný dodavatel mapových podkladů Jeppesen, který svou aplikací Jeppesen Mobile FD upřednostnil a rychleji vyvíjel právě pro operační systém iOS.

Nedílnou součástí výběru Apple iPadu bylo jeho potenciální možné schválení Úřadem pro civilní letectví ČR, které se mohlo inspirovat již fungujícími instalacemi ve světě.

Vybraným zařízením z nabídky trhu byl v roce 2013 aktuální model Apple iPad 4. generace, s kapacitou 64 GB, výbavou Wi-Fi a Cellular a označením A1460 černé barvy. Schválení vybraného modelu zařízení leteckým úřadem pro instalaci a použití v kokpitu letadla znamenalo nutnost udržení jednotné flotily tohoto vybraného modelu A1460. Bylo rozhodnuto nakoupit 40 ks zařízení pro piloty a dalších 10 ks do zásoby. Tvorba zásoby byla nutná, vzhledem k tomu, že byl očekáván příchod nového modelu iPadu na trh a znamenalo to, že stávající model roku 2013 nebude dále vyráběn a budou pouze doprodávány skladové zásoby a vzhledem k tomu, že bylo nutné zajistit jednotnost flotily zařízení.

4.6 Výběr správy zařízení

Společnost Letím bezpečně a.s. měla již identifikované požadavky pro budoucí centrální správu mobilních zařízení, které vycházely jak z nového projektu záměny EFB, tak z požadavků řešení centrální správy mobilních zařízení v celé společnosti. Jejich soupis je obsahem kapitoly 4.3.3. Pro hodnotící metody výběru vhodného řešení byly tyto požadavky převedeny na jednoznačná kritéria, která byla doplněna váhami. Tím bylo možné jednotlivé produkty srovnat a zdůraznit nejvhodnější platformu EMM pro následnou implementaci. Prvním krokem hodnocení bylo určení kritérií ve skupinách podle funkčního zařazení. Následoval krok, kdy byla doplněna váha ke každému z kritérií, od 1 (nejméně - nedůležité) do 5 (nejvíce - důležité). Tabulky č. 4 - 8 reprezentují jednotlivé skupiny kritérií a kritéria s váhami.[1], [96]

Tabulka 4 - Hodnotící kritéria s váhami (Mobile Device Management)

Kritérium	Váha
Mobile Device Management	
Podpora mobilních platforem	5
Vzdálené uzamčení zařízení	4
Vzdálené smazání zařízení (Wipe)	5
Lokace zařízení	3
Kodový zámek / Heslo	5
Detekce Jailbreak / Root	2
Šifrování zařízení	3
Inventarizace	3
Podpora BYOD	4
Detekce malware	3

Zdroj: vlastní zpracování, [96]

Tabulka 5 - Hodnotící kritéria s váhami (Mobile Application Management)

Kritérium	Váha
Mobile Application Management	
Blacklist/Whitelist aplikací	4
Nastavení MS Exchange	5
Řízení nákladů	3
Sandboxing/kontejnerizace	5
Vzdálená plocha	2
Konfigurace VPN do Cisco AnyConnect klienta	5
SDK a App Wrapping	2
Povinné aplikace	2
Firemní obchod aplikací	3
Integrace VPP	3

Zdroj: vlastní zpracování, [96]

Tabulka 6 - Hodnotící kritéria s váhami (Mobile Content Management)

Kritérium	Váha
Mobile Content Management	
Správa dat/dokumentů	5
Zabezpečený PIM	4
Synchronizace dokumentů (online) a dostupnost (i offline)	5
Schvalování přečtení dokumentů	2
Napojení do MS Sharepoint Foundation 2010	4
Zabezpečení dokumentů	5
Zabezpečený webový prohlížeč	5

Zdroj: vlastní zpracování, [96]

Tabulka 7 - Hodnotící kritéria s váhami (Dodavatel)

Kritérium	Váha
Dodavatel	
Edukovanost dodavatele	5
Spolehlivost dodavatele	5
Rychlost reakce dodavatele	3
Úspěšné implementace	3
Potenciální přidaná hodnota	4

Zdroj: vlastní zpracování, [96]

Tabulka 8 - Hodnotící kritéria s váhami (Kvalitativní aspekty)

Kritérium	Váha
Kvalitativní aspekty	
Pravidelné konzultace	1
Komunita produktu	3
Přímá podpora	5
Licenční poplatky	4
Appconfig	5

Zdroj: vlastní zpracování, [96]

Skupina kritérií zaměřena na dodavatele je upřesněna v kapitole 4.7 (Výběr dodavatele). Další krok spočíval v přípravě a hodnocení každého z produktů s vybraným dodavatelem, na škále mezi 1 (nesplňuje) a 5 (splňuje).

Tabulka 9 - Hodnocení EMM řešení s dodavateli (Mobile Device Management)

		AirWatch Dodavatel 1		AirWatch Dodavatel 2		MobileIron Dodavatel 3		MobiControl Dodavatel 4	
	w	p	w*p	p	w*p	p	w*p	p	w*p
Mobile Device Management									
Podpora mobilních platforem	5	5	25	5	25	4	20	4	20
Vzdálené uzamčení zařízení	4	5	20	5	20	5	20	5	20
Vzdálené smazání zařízení (Wipe)	5	5	25	5	25	5	25	5	25
Lokace zařízení	3	5	15	5	15	5	15	5	15
Kodový zámek/Heslo	5	5	25	5	25	5	25	5	25
Detekce Jailbreak/Root	2	5	10	5	10	5	10	5	10
Šifrování zařízení	3	5	15	5	15	5	15	5	15
Inventarizace	3	5	15	5	15	5	15	5	15
Podpora BYOD	4	5	20	5	20	5	20	5	20
Detekce malware	3	5	15	5	15	5	15	5	15

Zdroj: vlastní zpracování, [96]

Tabulka 10 - Hodnocení EMM řešení s dodavateli (Mobile Application Management)

		AirWatch Dodavatel 1		AirWatch Dodavatel 2		MobileIron Dodavatel 3		MobiControl Dodavatel 4	
	w	p	w*p	p	w*p	p	w*p	p	w*p
Mobile Application Management									
Blacklist/Whitelist aplikací	4	5	20	5	20	5	20	5	20
Nastavení MS Exchange	5	5	25	5	25	5	25	5	25
Řízení nákladů	3	3	9	3	9	3	9	2	6
Sandboxing/kontejnerizace	5	5	25	5	25	5	25	4	20
Vzdálená plocha	2	5	10	5	10	1	2	5	10
Konfigurace VPN do Cisco AnyConnect klienta	5	5	25	5	25	5	25	5	25
SDK a App Wrapping	2	5	10	5	10	5	10	4	8
Povinné aplikace	2	5	10	5	10	4	8	5	10
Firemní obchod aplikací	3	5	15	5	15	4	12	5	15
Integrace VPP	3	5	15	5	15	5	15	5	15

Zdroj: vlastní zpracování, [96]

Tabulka 11 - Hodnocení EMM řešení s dodavateli (Mobile Content Management)

		AirWatch Dodavatel 1		AirWatch Dodavatel 2		MobileIron Dodavatel 3		MobiControl Dodavatel 4	
	w	p	w*p	p	w*p	p	w*p	p	w*p
Mobile Content Management									
Správa dat/dokumentů	5	5	25	5	25	5	25	5	25
Zabezpečený PIM	4	4	16	4	16	5	20	4	16
Synchronizace dokumentů (online) a dostupnost (i offline)	5	4	20	4	20	4	20	3	15
Schvalování přečtení dokumentů	2	1	2	1	2	1	2	1	2
Napojení do MS Sharepoint Foundation 2010	4	5	20	5	20	5	20	5	20
Zabezpečení dokumentů	5	5	25	5	25	5	25	5	25
Zabezpečený webový prohlížeč	5	5	25	5	25	5	25	5	25

Zdroj: vlastní zpracování, [96]

Tabulka 12 - Hodnocení EMM řešení s dodavateli (EMM služby a další)

		AirWatch Dodavatel 1		AirWatch Dodavatel 2		MobileIron Dodavatel 3		MobiControl Dodavatel 4	
	w	p	w*p	p	w*p	p	w*p	p	w*p
EMM služby a další									
Reporting	3	5	15	5	15	4	12	5	15
Alerting	5	5	25	5	25	4	20	5	25
Podpora a napojení do AD	3	5	15	5	15	5	15	5	15
Přehlednost centrálního managementu	5	5	25	5	25	4	20	4	20
User-self service portál	3	5	15	5	15	5	15	5	15

Zdroj: vlastní zpracování, [96]

Tabulka 13 -Hodnocení EMM řešení s dodavateli (Dodavatel)

		AirWatch Dodavatel 1		AirWatch Dodavatel 2		MobileIron Dodavatel 3		MobiControl Dodavatel 4	
	w	p	w*p	p	w*p	p	w*p	p	w*p
Dodavatel									
Edukovanost dodavatele	5	3	15	2	10	5	25	3	15
Spolehlivost dodavatele	5	2	10	2	10	5	25	2	10
Rychlost reakce dodavatele	3	3	9	5	15	4	12	3	9
Úspěšné implementace	3	4	12	3	9	4	12	4	12
Potenciální přidaná hodnota	4	2	8	1	4	5	20	2	8

Zdroj: vlastní zpracování, [96]

Tabulka 14 - Hodnocení EMM řešení s dodavateli (Kvalitativní aspekty)

		AirWatch Dodavatel 1		AirWatch Dodavatel 2		MobileIron Dodavatel 3		MobiControl Dodavatel 4	
	w	p	w*p	p	w*p	p	w*p	p	w*p
Kvalitativní aspekty									
Pravidelné konzultace	1	3	3	3	3	2	2	3	3
Komunita produktu	3	5	15	5	15	5	15	1	3
Přímá podpora	5	3	15	3	15	2	10	3	15
Licenční poplatky	4	1	4	1	4	1	4	1	4
Appconfig	5	5	25	5	25	5	25	5	25

Zdroj: vlastní zpracování, [96]

Tabulka 15 - Hodnocení EMM řešení s dodavateli (Výsledné scóre/pozice)

		AirWatch Dodavatel 1		AirWatch Dodavatel 2		MobileIron Dodavatel 3		MobiControl Dodavatel 4	
	w	p	w*p	p	w*p	p	w*p	p	w*p
Výsledné skóre	**158**	**693**		**687**		**700**		**656**	
Výsledné skóre bez dodavatele	138	639		639		606		602	
Výsledná pozice		**2**		**3**		**1**		**4**	

Zdroj: vlastní zpracování, [96]

Rozdíly ve výsledném skóre jednotlivých řešení nebyly příliš velké. Skóre určilo na pozici 1 řešení MobileIron s Dodavatelem 3. Pozice 2 a 3 byla určena pro produkt AirWatch, pro každou pozici s jiným dodavatelem. Poslední pozici získal produkt Soti s Dodavatelem 4.

Výsledný výběr řešení MobileIron z pohledu funkcí je v pořádku. Všechny tři platformy EMM splňovaly většinu kritérií. Ačkoliv má například Airwatch podporu platforem daleko vyšší než ostatní, není mezi požadavky společnosti podpora ostatních platforem, které AirWatch nabízí navíc (Windows 10, Mac OS X, Apple TV OS, Apple Watch OS, Chrome OS, Tizen, Symbian S60).

V závěru hodnocení je důležité poznamenat, že zařazení dodavatele do hodnotících kritérií mohlo způsobit, že zcela nevhodný dodavatel znehodnotil výsledek celého produktu, který mohl být obstojný. To demonstruje rozdíl mezi řádky tabulky č. 15 „Výsledné skóre“ a „Výsledné skóre bez dodavatele“. Kritéria dodavatele byla zařazena záměrně, aby vliv jeho hodnocení promluvil do vlastního výběru EMM.

Výběr MobileIron zahrnoval také určení licencí. V prvním kroku bylo dodání 50 licencí Premium bundle (MobileIron Advanced Management Software License, AppConnect a AppTunnel, Docs@Work, Web@Work) a dodání 100 licencí MobileIron ActiveSync Management Subscription.

4.7 Výběr dodavatele

Dodavateli a jeho výběru je věnována vlastní podkapitola. Dobrý dodavatel mobilního řešení, typu EMM, může klientovi, který se chystá EMM implementovat velmi pomoci. Pomocí se rozumí přidaná hodnota dodavatele, který svou zkušeností z oboru klientovi šetří náklady, čas a kapacity IT oddělení klienta. Důvodem vlastní podkapitoly věnované dodavateli je vyzdvihnutí několika oblastí, kterou mohou hrát důležitou roli při zavádění nového řešení centrální správy mobilních zařízení.

Je zřejmé, že trh s mobilními zařízeními je trhem velmi rychle rostoucím a je vhodné hledat dodavatele, který za sebou má již několik let zkušeností, několik úspěšných instalací a spokojené zákazníky. Výhodu dobrého dodavatele autor vidí ve větším počtu nabízených řešení větší než pouze jediné. Pokud dodavatel má zkušenosti z více možných EMM řešení, dokáže tato řešení porovnat a nabídnout klientovi to, co je pro něj vhodnější

a nejlépe pasuje na jeho požadavky. Navíc takový dodavatel má přísun informací mobilní sféry z více zdrojů, které může zužitkovat právě při práci s klientem. Autor tím netvrdí, že výběr dodavatele, který instaluje pouze jediné řešení je chyba. V případech, kdy klient je rozhodnutý pro konkrétní řešení, může to být dokonce výhoda, kdy dodavatel má hluboké a detailní znalosti takového systému, protože pracuje výhradně s ním.

Jak správně vybrat dodavatele není snadné definovat. Několik dobře mířených otázek může klientovi napomoci rozlišit, zda dodavatel má reálné zkušenosti z dané oblasti. Například pokud je tématem iOS a dodavatel nemá odpověď pro otázku, jaký je stav VPP v České republice a jak Vám pomůže s nákupem aplikací, nemusí to být vhodný dodavatel pro tuto oblast, případně pokud Vám nedokáže správně interpretovat použití Wrappingu aplikací, také to není dobrým znamením.

Je nezbytné v oblasti mobilních zařízení nabyté informace od dodavatelů ověřovat, například i napříč ostatními dodavateli, případně z nezávislých zdrojů. Může se stát, že klient dohledá informace a vyhodnotí dodavatele jako nevhodného z toho důvodu, že podává špatné informace.

Často dodavatelé za cenu snížení své vlastní schopnosti nebo schopností nabízeného řešení, slibují všechny požadavky klienta, ačkoliv některé nejsou možné a nemusí být ani podporovány výrobci EMM, případně výrobci dané platformy. S tím také souvisí situace, kdy klient nemusí trvat na svém přesném znění požadavku, má určité pochopení schopností EMM řešení a je pak na dodavateli zda dokáže pomoci klientovi „jinou cestou“, tak aby došlo k částečnému splnění požadavku nebo případně řešení problematiky jiným způsobem. V takových případech se dobrý dodavatel stává velkou výhodou, kterou klient ocení.

V konkrétním případě nasazení EMM v letecké společnosti Letím bezpečně a.s. bylo poptáno několik dodavatelů, kteří poskytovali instalaci a podporu produktů MobileIron, Airwatch a Soti.

Po několika úvodních kolech jednání bylo zřejmé, že úroveň edukovanosti dodavatelů v oboru není shodná a bylo nutné z toho vyvodit důsledky. Požadavky na EMM po prvních jednáních dále krystalizovaly a s tím i otázky, které byly dodavatelům pokládány. Výsledek těchto otázek byl brán v potaz jako hodnotící kritérium pro výběr EMM produktu.

4.8 Implementace EMM

Na základě hodnotících metod a kritérií byl vybrán pro správu mobilních zařízení produkt MobileIron s nasazením on-premise v prostředí společnosti. Instalace a podpora byla zajištěna Dodavatelem 3. Na začátku implementace byly přijaty od dodavatele požadavky na implementaci. Instalaci EMM následovalo nasazení první konfigurace pro testovací skupinu zařízení. V průběhu testování a přípravy prvních konfiguračních profilu se vyskytla některá úskalí. Jakmile byla většina prvních problémů vyřešena a byla dopracována finální konfigurace a došlo k distribuci řešení na mobilní zařízení v celé společnosti.

Tabulka 16 - Období jednotlivých částí implementace EMM

Položka implementace	Období
Požadavky na implementace	12/2013
Instalace	02/2014
První konfigurace	02/2014
Testování	02-03/2014
Finální konfigurace	03/2014
Distribuce na mobilní zařízení	04-11/2014

Zdroj: vlastní zpracování

4.8.1 Požadavky na implementaci

Společnost Letím bezpečně a.s. požadovala instalaci řešení on-premise. Oproti cloudové variantě tak bylo nutné připravit na straně společnosti prostředí pro instalaci. S dodavatelem bylo domluveno několik základních atributů instalovaného řešení. MobileIron je nabízen pro on-premise instalaci ve variantách virtuální appliance nebo jako fyzické boxy. Pro implementaci ve společnosti byla vybrána virtuální appliance, vzhledem k možnosti využití stávajícího prostředí.

MobileIron je založen na Linux appliance, Red Hat Enterprise Linux distribuce (CentOS), a nepotřebuje licence Windows Serveru pro vlastní instalaci, na rozdíl od platformy AirWatch. Databáze je součástí Core (VSP) serveru, není tak nutné instalovat SQL server.

Výběr nasazení Sentry

Sentry server se instaloval v nasazení tzv. Standalone Sentry, nikoliv jako Integrated Sentry. Standalone Sentry (virtuální nebo fyzické zařízení) je umístění Sentry serveru mezi mobilním zařízením a podnikové zdroje, jako je například e-mailový server. Namísto toho Integrated Sentry není umístěn in-line, ale místo toho je přímo nainstalován na serveru ActiveSync, s podporou pouze MS Exchange 2007 a 2010.[97]

Certifikační autorita

Z pohledu certifikační autority bylo nutné zvolit integrovanou autoritu v rámci MobileIron řešení nebo vlastní Microsoft Certification Authority, kterou společnost již měla zavedenou.

Proběhlo zvážení jednotlivých kladů a záporů. Certifikační autoritu (CA) bulit-in VSP není třeba připojovat na vlastní CA, není tak nutné otevření portu 443 mezi VSP a vlastní CA a není nutné tvořit servisní účet. Další výhodou je správa certifikátů pro mobilní zařízení přímo z management konzole VSP serveru. Za nevýhodu lze považovat skutečnost, že lze použít VSP CA pouze pro služby publikované přes server Sentry. Pokud by byla použita vlastní MS CA, lze vystavené certifikáty použít i pro další případy (například VPN), nicméně správa certifikátů by probíhala mimo VSP server, bylo by nutné připravit propojení mezi MS CA a VSP serverem a také by bylo nutné mít instalovanou MS CA na Windows Enterprise serveru, aby bylo možné nainstalovat NDES komponentu.

Z důvodu snadnější implementace a menšímu riziku potenciálních problémů oproti použití certifikační autority vlastní.

Tabulka č. 17 zobrazuje základní atributy instalovaného řešení.

Tabulka 17 - Atributy instalovaného EMMřešení

Atribut	Instalováno
Typ instalace	On-premise
Virtuální/fyzické appliance	Virtuální
Typ virtuálního prostředí	MS HyperV
Typ databáze	Vlastní integrovaná
Certifikační autorita	Bulit-in VSP CA
Typ nasazení Sentry	Standalone Sentry

Zdroj: vlastní, [98]

Dodavatel připravil a zaslal dokument, který obsahoval požadavky na hardware a nastavení sítě, nastavení firewallu, nastavení podpory, servisní účty a SSL certifikáty. Předpokládané spuštění řešení pro účel testování bylo naplánováno na únor 2014.

4.8.1.1 Hardware požadavky

Vybraný hypervizor byl HyperV, ale mezi podporované hypervizory spadaly také VMware nebo KVM.

Hardware požadavky pro nasazení EMM řešení MobileIron do 200 zařízení pro jednotlivé servery bylo:

MobileIron VSP (dnes nazýváno Core)

Tabulka 18 - Požadavky na HW pro VSP server

Položka	Požadováno
Virtual CPU	1x
RAM	4GB
HDD	80GB
OS Type	RHEL5 64
NIC	E1000

Zdroj: [98]

MobileIron Sentry

Tabulka 19 - Požadavky na HW pro Sentry server

Položka	Požadováno
Virtual CPU	1x
RAM	4GB
HDD	40GB
OS Type	RHEL5 64
NIC	E1000

Zdroj: [98]

4.8.1.2 SSL certifikáty

Pro HTTPS provoz bylo nutné obstarat SSL certifikáty. První variantou bylo pořídit pro každý server vlastní certifikát. Druhá varianta zahrnovala pouze jeden wildcard certifikát. Podmínkou bylo, aby vydavatel wildcard certifikátu byl v seznamu certifikačních autorit na iOS, Android či Windows Phone zařízeních.

Vybrán byl wildcard certifikát, který bylo možné použít na další servery i mimo řešení MobileIron. Nutné certifikáty, jejich použití a síla klíče zobrazují následující tabulky.

ActiveSync certifikát

Tabulka 20 - ActiveSync certifikát

Použití	**WebServer Encryption, MobileDevice Access**
Síla klíče	2048

Zdroj: [98]

VSP certifikát

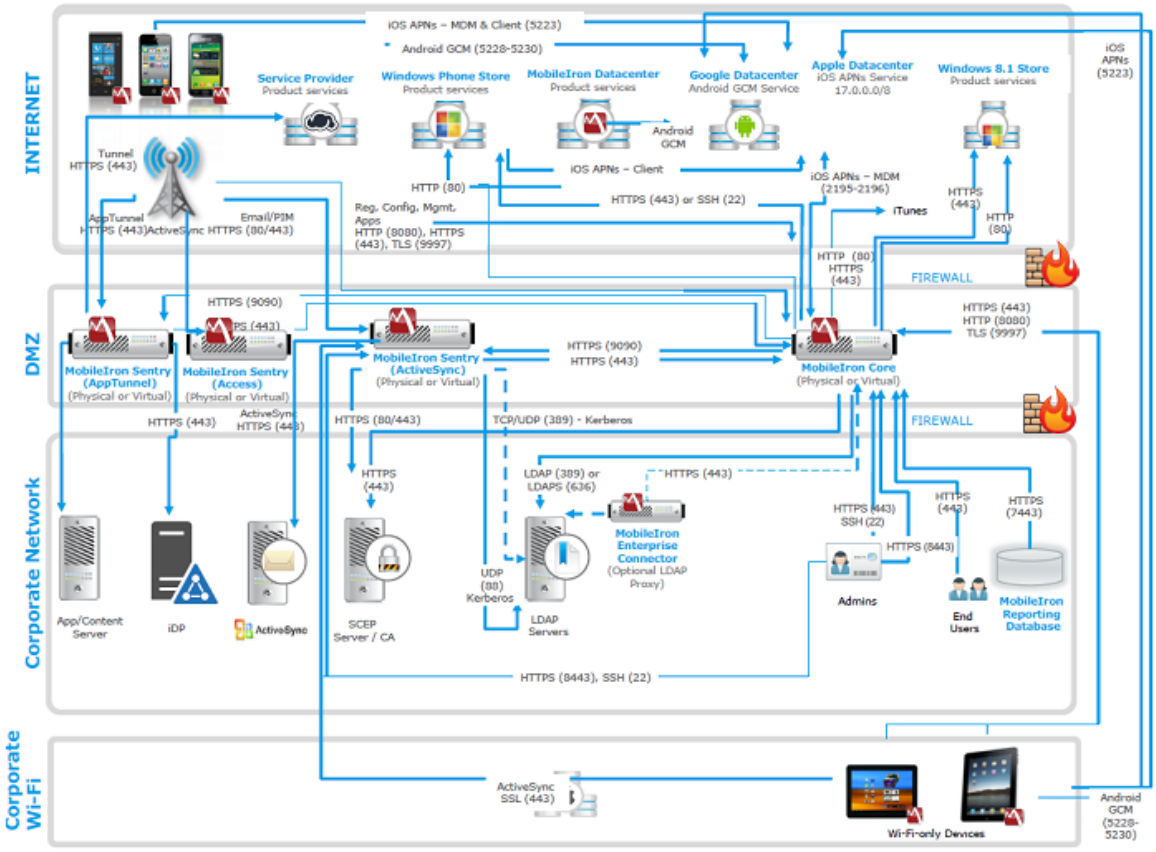
Tabulka 21 - VSP certifikát

Použití	**WebServer Encryption**
Síla klíče	2048

Zdroj: [98]

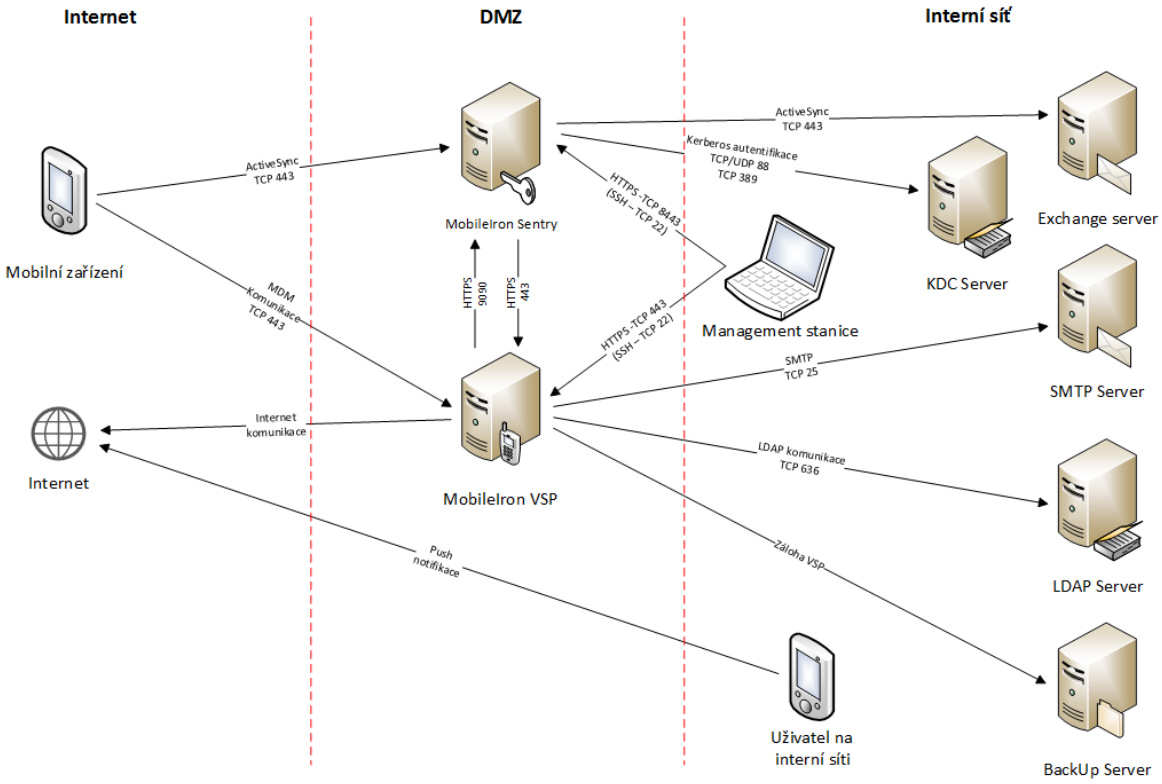
4.8.1.3 Síťové a firewall požadavky

Servery VSP (Core) i SENTRY měly být umístěny v DMZ a publikovány do internetu. Pro každý server bylo nutné zajistit vlastní veřejnou IP adresu. Níže je umístěn obrázek č. 20 znázorňující kompletní diagram architektury MobileIron.



Obrázek 20 - Diagram architektury řešení MobileIron [99]

Pro účely implementace a přípravy sítě byl pro společnost Letím bezpečně a.s. vytvořen zjednodušený diagram této architektury, zobrazený obrázkem č. 21.



Obrázek 21 - Zjednodušený diagram architektury instalovaného řešení [100]

4.8.1.4 Podpora a správa EMM řešení

Bylo nutné zvolit management stanici pro účely správy a instalace MobileIron serveru. Zvolená stanice měla mít přístup do DMZ, na VSP server (port TCP 443) a Sentry server (port TCP 8443). Pro oba servery bylo vyžádáno nastavení přístupu přes SSH na portu TCP 22.[98]

4.8.1.5 Servisní účty

Požadavkem bylo vytvoření servisních účtů pro LDAP,SMTP a případně Kerberos.

LDAP účet

Servisní účet bylo požadováno zřídit pro přístup k adresářové službě, pro účel čtení stromu adresářové služby.

SMTP účet

Servisní účet bylo požadováno vytvořit, pokud bylo nutné se na SMTP serveru ověřovat.

Kerberos účet

Servisní účet pro Kerberos bylo potřebné vytvořit pro ověřování na serveru ActiveSync, pokud měl být tento způsob ověřování použit.

4.8.2 Instalace EMM a seznámení

Instalace řešení byla provedena během jednoho pracovního dne. Ze strany společnosti Letím bezpečně a.s. bylo připraveno prostředí dle požadavků dodavatele. Instalace probíhala dodavatelem on-site ve společnosti za účasti zástupců vlastního IT oddělení. Instalovaly se servery VSP (Core) a Sentry na připravené virtuální prostředí.

Kroky instalace

Níže jsou zobecněny kroky samotné instalace obou serverů. Zpočátku jde o shodné kroky instalace serverů, následuje část odlišná, kde se kroky instalace jednotlivých serverů liší.

Kroky instalace VSP a Sentry serveru (shodné):

- výběr typu instalace,
- odsouhlasení licenčního ujednání,
- jméno společnosti,
- jméno kontaktní osoby za společnost,
- emailová adresa kontaktní osoby,
- zadání enable secret hesla,
- username lokálního administrátora (nelze použít root),
- zadání hesla administrátora,
- určení fyzického rozhraní sítě – GigabitEthernet1 nebo GigabitEthernet2,
- zadání IP adresy serveru,
- zadání síťové masky IP adresy serveru (netmask),
- zadání síťové výchozí brány,
- zadání external hostname, IP adresy,
- povolení vzdáleného přístupu přes SSH,

- povolení přístupu přes Telnet,
- povolení a konfigurace NTP serverů,
- restart serveru.

Kroky instalace VSP (Core):

- konfigurace emailové integrace,
- konfigurace LDAP serveru,
- kontrola nastavení portů,
- konfigurace routes (System manager),
- konfigurace Portal ACLs,
- konfigurace standalone Sentry.

Kroky instalace Sentry:

- nastavení Sentry ve VSP (Core) serveru (Admin portal),
- konfigurace routes,
- kontrola/konfigurace static host.

Po instalaci měli administrátoři k dispozici přístup do několika webových portálů MobileIron řešení. Management prostředí obou serverů se nepatrně liší. Zatímco VSP (Core) server obsahuje dvě management prostřední – Admin portal a System manager, Sentry server disponuje pouze management konzolí pouze System manageru.

VSP server

Admin portál VSP serveru je hlavní konzole, která poskytuje většinu funkcionality a je určena pro provádění nejběžnějších administrativních úkolů ohledně správy zařízení od vytváření konfigurací a politik, přes správu zařízení, napojení do ostatních serverů až k logům.

System manager je specifikovaný pro práci s konfigurací samotného fungování VSP serveru. Obsahuje:

- konfiguraci VSP serveru,
- správu jeho síťového nastavení,
- upgrade VSP serveru,
- řešení problémů a údržba,

- monitoring.

Sentry server

Poskytuje pouze jeden webový portál a to System manager, který obsahuje funkce:

- konfigurace Sentry serveru
- správu jeho síťového nastavení,
- upgrade Sentry serveru,
- řešení problémů a údržba,
- monitoring.

Mimo dostupné webové portály serverů lze použít pro konfiguraci rozhraní SSH na portu 22, například pomocí software Putty. Tento nástroj je vhodné použít pro úkony z příkazové řádky, které nejsou dostupné v System manageru serveru. Práce s příkazovou řádkou pak vychází z OS Linux, jde však o appliance, která je upravená, a tím jsou některé oblasti pozměněné nebo do nich není umožněn přístup. Privilegovaná práva „root“, jak jsou známa z prostředí Linux, zde nejsou pro zákazníka ani dodavatele dostupná, pouze pro přímou podporu MobileIron.

Po instalaci proběhlo skolení administrátorů společnosti pod vedením zástupce dodavatele v délce jednoho dne.

4.8.3 První konfigurace

Instalaci následovalo nasazení prvních konfiguračních profilů a bezpečnostních politik (některé již v rámci školení), které byly následně aplikovány na testovací zařízení.

První konfigurace zahrnovala:

- vytvoření skupin se zabezpečením v Active Directory,
- synchronizaci potřebných skupin LDAP do VSP serveru,
- vytvoření labelů navázaných na LDAP skupiny,
- vytvoření IT politik,
    - nastavení Default Security policy,
    - nastavení iOS Security policy,
    - nastavení iOS Security policy – Piloti,
    - nastavení iOS Security policy - FA,

    - nastavení Default AppConnect policy,
    - nastavení AppConnect policy - Posadky,
    - nastavení AppConnect policy - ABSJets,
    - nastavení Default Lockdown policy,
    - nastavení Default Privacy policy,
- vytvoření konfiguračních profilů,
    - nastavení Exchange,
    - nastavení profilu W@W,
    - Webclip - System - iOS Enterprise AppStore,
    - VPN profil,
    - iOS restrikce,
- nastavení distribuce aplikací/nahrání aplikací do Apps@Work,
    - nastavení App Control.

Seznam nutných nastavení nemusí být kompletní. Nezahrnuje všechny nutné a výchozí profily. Profily a politiky, které jsou zajímavé, budou dále rozebrány.

Nasazení politik do zařízení je pak realizováno pomocí labelů, skupin uživatelů.

Politiky, označované jako Policy je možné vytvářet více jednoho typu. Pokud pak je konkrétní label přiřazen k oběma Policy stejného typu, je na zařízení publikována ta politika, která má vyšší prioritu. Priorita se nastavuje u každé Policy, kdy se určí, zda priorita dané politiky je vyšší než nebo nižší než jiná konfigurace stejného typu politiky. Jde o rozdíl oproti konfiguračním profilům, které také umožňují nastavení více konfigurací jednoho typu konfiguračního profilu. Ale pak je nutné konkrétní label přiřadit pouze k jednomu výskytu daného typu konfiguračního profilu, nelze určovat priority.

Security policy

Bezpečnostní politika určuje, jak budou mobilní zařízení zabezpečena. Security policy umožňuje v prvním kroku nastavit heslo k zařízení. Pro heslo lze volit minimální délku, časový limit nečinnosti, počet neúspěšných pokusů, historii hesla a počet dnů do expirace a další atributy. Pro iOS zařízení je specifické zamykání zařízení od 6. špatného pokusu. První zamčení je na 1 min, dále se pak interval zamčení prodlužuje. Pokud je nastaven nižší počet pokusů než 6, pak se smaže zařízení bez zamykání okamžitě po zadání špatného hesla.

V dalším kroku se nastavuje Access control pravidla, která určují, jak bude zacházeno se zařízeními, která se například nastavený počet dní neohlásí VSP (Core) serveru, budou mít zastaralou politiku, nebo budou porušovat určené App Control pravidla. Pro iOS zařízení je tato sekce rozšířena na akce za podmínek pokud je verze iOS nižší než nastavená verze, pokud je vypnuta ochrana dat, pokud je detekováno kompromitované iOS zařízení nebo pokud typ zařízení je ve vyjmenovaném listě (např. iPhone 3, 3GS apod.) z důvodu ochrany proti připojení nepodporovaných zařízení. Stejně tak jsou Access control pravidla rozšířena o sekci pro Android a Windows zařízení.

Security policy řeší odděleně také konfiguraci pro Android a Windows ve zvláštní sekci, ale to nebylo potřebné nastavit.

Mezi další Security policy nastavení spadalo také nastavení šifrování. Politika může vynutit šifrování celého zařízení, SD karty a také logů zařízení. V dnešních možnostech lze dokonce určovat, jaké typy souborů se budou šifrovat přímo v konfiguraci politiky.
Z provozních důvodů bylo nutné rozlišit tři skupiny uživatelů pro Security policy v sekci hesla k zařízení. Piloti měli konfiguraci časového limitu nečinnosti nastaveno na 1 hodinu, stevardky a ostatní uživatelé 5 minut. Piloti a stevardky měli nastaven počet neúspěšných pokusů zadání hesla k odemčení zařízení 10, ostatní uživatelé iOS 7.

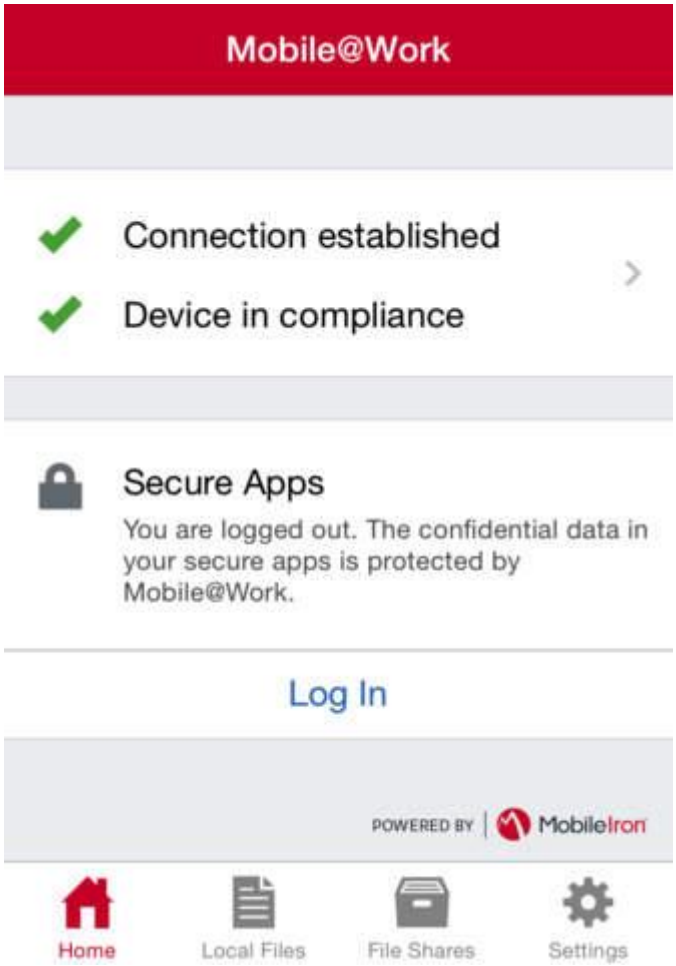
AppConnect policy

AppConnect je MobileIron komponenta, která provádí kontejnerizaci aplikací za účelem ochrany firemních dat. Politika se především stará o zabezpečení kontejneru. Je možné nastavit AppConnect heslo, které budou nuceni uživatelé zadávat v rámci používání kontejneru zabezpečených aplikací. Pro iOS lze toto heslo zadávat i pomocí otisku prstu. Politika také nastavuje, po kolika dnech nekontaktování serveru bude na zařízení smazán celý AppConnect a po kolika minutách se zařízení musí znovu ohlásit serveru.

Co se týká bezpečnostních politik v rámci AppConnect nastavuje se zvlášť DLP pro iOS a Android zařízení. Povoluje nebo zakazují se funkce kopírovat, vložit, otevřít v, tisk. Pokud bude funkce povolena, rozlišuje se, zda bude povolena pro všechny aplikace, nebo pouze v rámci autorizovaných AppConnect aplikacích, případně zda bude existovat nějaký Whitelist aplikací, pro který bude funkce povolena. Pokud takový Whitelist bude nastaven je nutno pamatovat, že pokud nejde o AppConnect aplikaci, nelze funkce povolené aplikace dále ovlivňovat. Pokud bude například povolena funkce „otevřít v“ pro aplikaci

třetí strany, dokument do takové aplikace předaný může uživatel již zaslat, uložit případně část zkopírovat kamkoliv.

V nastavení se rozlišily dvě skupiny uživatelů, které mají rozdílné nastavení. První skupinou jsou posádky, které mají rozdílně nastavené heslo pro AppConnect heslo od druhé skupiny obecných uživatelů. Heslo v první konfiguraci ale nebylo vyžadováno. Jak vypadá obrazovka zadání hesla pro AppConnect v Mobile@Work zobrazuje obr. č. 22.



Obrázek 22 - Přihlášení do AppConnect přes Mobile@Work [101]

Exchange

Pro nastavení poštovního profilu v zařízení slouží konfigurační profil Exchange. Obsahuje nastavení jména serveru, nastavení SSL a domény a uživatelských přihlašovacích údajů v zástupných symbolech. V profilu se také vybírají položky pro synchronizaci, jako pošta, kalendář, kontakty a úkoly. Dále je možné nastavit jaká část schránky do minulosti se má k uživateli synchronizovat. Lze povolit S/MIME. Pro

samotný ActiveSync je možné nastavit tzv. Peak Time a dále nastavit, jak bude probíhat synchronizace v době tzv. Peak Time. Pro samotný iOS lze dále nastavit blokování aplikacím třetích stran přístupu k tomuto emailovému účtu.

Vlastní konfigurace obsahovala:

Tabulka 22 - Konfigurace Exchange

Položka	Nastaveno
Server	Adresa Sentry serveru
SSL	Povoleno
Doména	Vlastní
Certifikát	Integrovaná CA
Přihlašovací údaje	zástupné řetězce ($USERID$, $PASSWORD$, $EMAIL$
Položky k synchronizaci	Vše
Synchronizace do minulosti	Vše
Peak time – synchronizace	jakmile položka dorazí během i mimo Peak Time
Blokování aplikací třetích stran v přístupu	Ne

Zdroj: vlastní zpracování, [102]

Web@Work

Konfigurace pro webový prohlížeč od MobileIronu je přehledná a nastavuje se pouze AppTunnel Rules, identita certifikátu a samotné záložky. V AppTunnel Rules se definují Sentry služby na specifických portech 80 a 443. Záložky je pak možné naplnit odkazy na vlastní podnikové webové aplikace, včetně určení pořadí. V tomto kroku je důležité mít na paměti pravidla na vlastním firewallu a nastavit je tak, aby Sentry server měl prostup na webové aplikace (server kde aplikace běží) na portech 443 a 80.

VPN

Nastavení konfiguračního profilu VPN se skládá z určení typu připojení a dle této volby se rozbalí příslušné nastavení odpovídající zvolenému typu. Vybraným typem spojení byl Cisco AnyConnect. Bylo tak nutné doplnit adresu serveru a zástupné řetězce za uživatelské údaje. V prvním kroku nebyl použit certifikát a bylo pouze plánováno jeho možné využití. Proto nebyly povoleny volby VPN on Demand a Per-App VPN.

Synchronization policy

Sync politika byla nastavena na VSP server, s použitím TLS s hlavními intervaly v minutách podle tabulky č. 23 níže. Byla nasazena výchozí konfigurace, vzhledem k tomu že byla uvedena jako doporučená.

Tabulka 23 - Konfigurace Synchronization policy

Hearbeat Interval	**14**
Sync Interval	240
iOS Location-Based Wakeups Interval	15

Zdroj: vlastní zpracování

iOS restrikce

Restrikce na zařízení je možné doručit pomocí konfiguračního profilu. Pro iOS jde o oddělený set funkcí, které lze povolit, zakázat nebo vynutit. Jaké funkce na iOS bude možné takto ovlivňovat, určuje společnost Apple. Platforma EMM je tak závislá na tom, jaké restrikce Apple umožní v rámci EMM ovlivňovat. Při první konfiguraci iOS restrikcí bylo možných voleb méně než dnes. Je tak viditelný progres v rostoucím počtu funkcí, které může administrátor na zařízení vzdáleně zakazovat nebo povolovat. Na začátku převládalo použití spíše povolených funkcí.

Mezi nastavené restrikce spadalo:

- zakázaná funkce Siri na zamčeném zařízení,
- zakázané odesílání diagnostických dat do společnosti Apple,
- vynucené šifrování zálohy iOS v aplikaci iTunes.

Šifrování zálohy zařízení do iTunes je vynuceno z důvodu zabezpečení komunikace mezi mobilním zařízením a servery MobileIronu.

4.8.4 První zařízení

Pro zařízení bylo rozhodnuto používání Apple ID vázaných na adresu uživatele. Uživateli bylo umožněno použít i vlastní Apple ID.

Vzhledem k absenci DEP programu pro Českou republiku v roce 2013, nebylo uvažováno použití iOS zařízení v „supervised“ módu. Použití nenahrávala ani těžkopádnost samotného procesu zařazení iPadů do supervised módu.

Postup přidání zařízení do EMM

Přidání zařízení do managementu bylo nastaveno tak, aby jej mohli provádět pouze administrátoři s pomocí registračního PINu. Administrátor nejdříve připravil uživatele v Active Directory. Vytvořil uživatele nebo použil stávajícího a nastavil mu patřičné skupiny svázané s EMM. Poté v MobileIron Admin portálu přidal zařízení dle kroků:

- vyhledání a výběr uživatele,
- volba platformy mobilního zařízení,
- výběr typu zařízení,
    - soukromé
    - firemní
- výběr zařízení se SIM nebo bez,
- volba možnosti odeslání přihlašovacích údajů na email (uživatele).

Server vygeneroval příslušné přihlašovací údaje včetně registračního PINu do pop-up okna. Na zařízení uživatele je pak nutné stáhnout z App Store aplikaci MobileIron. Po instalaci a spuštění aplikace se pro registraci zadaly vygenerované údaje a registrační PIN. Na zařízení se pak instalovaly přiřazené profily, konfigurace a doručily se potřebné certifikáty.

4.8.5 První problematika

Ačkoliv po první konfiguraci následovalo testování, práce přechází přímo na řešení první problematiky jak v rámci prvního testování, tak mimo něj.

Další Sentry server

Jak již bylo v rámci kapitoly 4.6 Výběr dodavatele zmíněno, společnost se rozhodla pro zakoupení 50 licencí Premium bundle a 100 licencí MobileIron ActiveSync Management Subscription. To znamenalo, v první řadě nasazení hlavních licencí na přibližně 50 ks iPadů a dále pak nasazení EAS profilu z MobileIronu pro další mobilní zařízení v rámci společnosti (telefony, BYOD). První konfigurace byla zaměřena právě na iPady a jejich konfiguraci. Po dokončení vznikla otázka na nasazení emailového profilu s „lehkou“ licencí pro mobilní zařízení, také z důvodu testování.

Byla nalezena nesrovnalost s použitím Sentry serveru pro konfiguraci zařízení s licencí MobileIron ActiveSync Management Subscription. Tento druh licence sloužil pouze pro zařízení, kde bude ručně konfigurován EAS profil, bez klienta MobileIron. Problémem bylo, že stávající Sentry server měl nastavenou autentizaci zařízení za pomoci certifikační identity a certifikát na zařízení byl publikován pomocí MobileIron klienta. V důsledku byla pro ActiveSync licenci požadována konfigurace Sentry serveru s autentizací zařízení pomocí hesla (Pass Through - BASIC/ntlm). Výsledkem bylo rozhodnutí pro vystavění druhého Sentry serveru, který bude zařízení ověřovat na základě hesla. Nebylo nutné platit licenci za další Sentry server, pouze se spotřebovaly další HW prostředky v rámci virtualizace. Další Sentry server již odpovídal požadavkům na konfiguraci ostatních zařízení.

Bugy

Po přidání prvních zařízení do managementu se vyskytlo několik nesrovnalostí. U zařízení byly zobrazovány všechny profily jako „pending“, tedy ve stavu kdy čekají na přijetí. Na zařízení však byly profily aplikovány. Jednalo se o chybu, kterou MobileIron opravil v jedné z příštích aktualizací.

Přidání zařízení do managementu také provázely potíže. Provedení dle základního postupu přidání zařízení neproběhlo regulérně a na zařízení nebyly doručeny všechny politiky a konfigurační profily. Bylo nutné přes aplikaci MobileIron provést ručně tzv. Re-Enroll zařízení, ruční vyžádání nové instalace profilů a politik na zařízení.

Dalším problémem bylo zasílání alertů o zařízeních s Policy out of date. Ačkoliv zařízení bylo v pořádku s aktuálními politikami, neustále byly doručovány alerty pro administrátory s opačnou informací. Z důvodu obavy, že budou zařízení dále nesprávně přesunuta do karantény, změnila se nastavení Policy z přesunutí do karantény na zasílání alertů.

Absence vyhledávání

V aplikacích MobileIron Web@Work a Mobile@Work nebylo k dispozici vyhledávání. Vzhledem k plánovanému využití Mobile@Work pro dokumenty šlo o jeden z významných problémů. Řešeno bylo v dalších verzích aplikace, přidáním funkce vyhledávání.

Exchange

Při používání testované verze Exchange profilu nastala otázka ohledně kalendáře v mobilním zařízení iOS a dostupnost místností a equipmentu při plánování schůzek. V dané verzi iOS a VSP serveru bylo možným řešení pouze instalace komponenty třetí strany na Exchange, která by uměla za běhu synchronizovat položky ze sdílených schránek (vždy nový kalendář v iOS). Nebo bylo možné přistupovat přes Web@Work do OWA portálu, kde je tato funkce dostupná. Dalším řešením bylo uživateli do zařízení připojit všechny potřebné schránky.

Dále byl interně identifikován problém s dostupností emailového archivu (na PC známé jako PST soubor). Řešení za pomoci EMM nebylo možné. Bylo tak řešeno hledáním vhodného produktu pro archivaci emailů s požadavkem na dostupnost na mobilním zařízení.

Restrikce iOS

Bylo zvažováno zakázání snímku obrazovky zařízení, ale vzhledem k možnostem nastavení bylo z požadavku ustoupeno. Apple umožňuje na iOS zařízení provést zakázání funkce snímku obrazovky pouze pro celé zařízení. Nelze zákaz aplikovat jen na některé klíčové aplikace, například na všechny AppConnect aplikace. Zákaz snímku obrazovky pro celé zařízení, minimálně v první konfiguraci, nebyl možný, vzhledem k tomu, že uživatelé často reportují problém právě tímto způsobem, převážně v momentě, kdy uživatel neumí správně předat informaci o chybě na zařízení.

Problematická byla také absence restrikcí ohledně aktualizací aplikací a aktualizací iOS. Apple toto nedovoloval ani dnes nedovoluje nastavit pomocí restrikcí. Výjimkou je takzvané „supervised device“, u kterého je dnes možné vynutit iOS aktualizaci. Tento typ zařízení nebyl v rámci společnosti používán.

Restrikce iOS přinesla také šifrované zálohy zařízení v iTunes. Jakmile je iOS zařízení poprvé připojeno k počítači s programem iTunes může být zálohováno. Ve výchozím nastavení programu iTunes je zálohování zařízení po prvním připojení nastaveno. Uživatel je vyžádán, aby zadal heslo pro přístup k šifrované záloze. Jakmile je heslo zadáno a provede se šifrovaná záloha, musí být toto heslo zapamatováno. Pokud uživatel heslo zapomene, není možné zálohu použít. Přesněji dle podpory společnosti

Apple - *Pokud ztratíte nebo zapomenete heslo, neexistuje žádný způsob obnovení vašich informací nebo vypnutí funkce Šifrovat zálohy*. [88]

Heslo je možné kdykoliv změnit v programu iTunes. Ale zároveň si toto heslo uchovává i samotné zařízení a i po připojení k jinému počítači a provedení nové zálohy, bude vždy požadováno poslední zadané heslo. Pokud tedy uživatel zadá jednou heslo, nezmění jej a po roce provede zálohu zařízení například před aktualizací iOS nebo v rámci reinstalace iOS zařízení, heslo si nebude pamatovat, nebude moci zálohu použít. Apple dnes nabízí možné řešení, a to provedení zálohy do prostředí iCloud a následně použití této zálohy bez nutnosti znát heslo.

Řízení mobilních dat (3G) nad aplikacemi

Požadavek řízení mobilních dat tak, aby byla povolena nebo zakázaná mobilní data nad konkrétní aplikací, nebyl splněn. EMM řešení takové omezení nebylo schopno řešit, také vzhledem k možnostem, které umožňuje platforma Apple iOS. Mobilní data bylo možné vypnout pouze na celém zařízení, to ale nebylo žádoucí. Požadavek nebyl kritický a byl odsunut na pozdější řešení.

Nákup aplikací

Hromadný nákup aplikací pro uživatele byl dalším klíčovým požadavkem. Bylo požadováno, aby přiřazená licence uživateli mohla být navrácena v případě, že uživatel ze společnosti odejde, nebo změní své zařízení a licenci již nebude potřebovat. Nabízelo se tento požadavek řešit pomocí VPP, který ale nebyl v České republice v roce 2014 dostupný. Hledala se cesta skrze vytvoření účtu VPP v jiné zemi, která byla na seznamu dostupných, ale nebylo povoleno v dané době distribuovat aplikace v rámci VPP do jiné země, než byla provedena registrace VPP účtu. Dočasným řešením bylo použití takzvaných GIFT kódů, které byly ručně zakoupeny a ručně distribuovány na uživatele.

Tisk

Problematika tisku z iPad zařízení byla vyřešena pomocí tiskáren s podporou funkce AirPrint a umístěním tiskáren do stejného subnetu sítě, do kterého se připojovaly iPady.

4.8.6 Finální konfigurace

Po dořešení některých prvních problémů byla připravena finální konfigurace pro nasazení na všechny iPady posádek. Souběžně mohla začít migrace uživatelů telefonů s EAS synchronizací přímo do MobileIronu. Od první konfigurace do spouštění distribuce MobileIron do zařízení byl proveden jeden upgrade VSP serveru. Ten vyřešil problém s chybně zobrazovaným pending stavem profilů na zařízení. Také proběhla aktualizace aplikace Mobile@Work pro iOS, která přinesla některá vylepšení, včetně novinky v synchronizaci dokumentů.

Konfigurace bezpečnostních a AppConnect politik se již od první konfigurace neměnila. Přibila konfigurace druhého Exchange profilu na zařízení, pro uživatele, kteří používali sdílenou schránku. Pro tyto účely byl využit druhý Sentry server s ověřováním „Pass Through“. Další změnou oproti prvotní konfiguraci byla příprava Docs@Work original profilu. MobileIron komponenta Docs@Work sloužila pro přístup k firemnímu obsahu, s možností napojení na Sharepoint, WebDav a další. Novinkou v dané verzi byla možnost přístupu ke sdílenému úložišti přes takzvané „Priority Folders“. Takto nazvané složky umožňovaly online synchronizaci dokumentů, včetně přístupu v offline režimu. Více informací o nastavení a používání o Docs@Work je obsahem kapitoly 4.9.2.

Vzhledem k vybudování nové Sentry bylo postupně připravováno také prostředí pro migraci ostatních mobilních zařízení v rámci EAS. To zahrnovalo nastavení ActiveSync policy a právní přípravu pro BYOD (více o BYOD v kapitole 4.9.6).
Tabulka č. 24 zobrazuje nastavení ActiveSync.

Tabulka 24 - Nastavení ActiveSync

Položka	Nastaveno
Zabezpečení zařízení heslem	vyžadováno
Minimální délka hesla	5 znaků
Maximální doba nečinnosti	5 min
Maximální počet neúspěšných pokusů zadání hesla	10

Zdroj: vlastní zpracování

Novinkou v nastavení EAS přes MobileIron bylo to, že jakékoliv první kontaktování serveru zařízením bylo blokováno. Všechny povolené připojení tak spravoval administrátor, a ačkoliv si uživatel mohl nastavit EAS konfiguraci v telefonu sám, bez

vědomí administrátora a patřičných schválení, se uživatel k obsahu emailové schránky na svém telefonu nedostal.

Obecně ale označení finální konfigurace není správné. Vzhledem k postupnému přetváření EMM platformy, změnám výrobců OS mobilních zařízení, jejich postoji vůči business zařazení je možné označit jakoukoliv konfiguraci jako konečnou pouze krátkodobě. Je tak nutné administrátory neustále vzdělávat v nových funkcích a provádět průběžné změny konfigurace, ať už vynucené nebo nevynucené, věnovat se s pečlivostí změnám verzí, hlídat novinky a změny. Požadavek, který byl dříve vzhledem k funkcionalitě neřešitelný, může být v budoucnu nastavitelný. Na místě je také registrace do komunity dané platformy EMM a podílet se svými nápady a sdílením vlastní problematiky na rozvoji daného řešení.

4.9 Používání EMM

Již implementované EMM řešení je nutné dále udržovat, podporovat a rozvíjet. V průběhu času probíhala údržba řešení a byly provedeny změny, v konfiguracích, nastavení a infrastruktuře. Zvláštní pozornost byla věnována klíčové synchronizaci dokumentů do EFB zařízení posádek a managementu aplikací na těchto zařízeních. MobileIron řešení bylo udržováno a používáno až do roku 2017, bez předpokládané budoucí změny na jinou platformu.

Tabulka 25 - Mapa změn a údržby

Kroky	Období nebo interval
Změny konfigurace a nasazení	
MobileIron Assemble	2016
Docs@Work new	2015
Přidání konfigurace pro Wi-Fi	2014
Publikace in-house applikace	2015
Ověřování Kerberos	2015
Údržba	
Zálohování	Každý den
Upgrade	Dle dostupnosti a doporučení dodavatele
Obnova Apple push certifikát	Každý rok
Obnova SSL certifikáty	Dle použitých certifikátů (např. každé 3 roky)

Zdroj: vlastní zpracování

4.9.1 Průběžné změny konfigurace

V průběhu používání EMM řešení vyvstalo několik nových požadavků na úpravy konfigurace vzniklé ze strany managementu, uživatelů, samotným vývojem používané platformy mobilních zařízení a samotného EMM, vlivem otevření nových možností ze strany výrobců EMM a výrobců mobilních platforem. Mezi klíčové změny konfigurace jednoznačně spadá použití ověřování pomocí Kerberos, také přechod z Docs@Work original na samostatnou aplikaci Docs@Work jak je známa dnes, zavedení striktní kontroly verzí aplikací a iOS pro posádky, úpravy AppConnect Policy, zavedení konfigurací pro Wi-fi, rozšíření katalogu aplikací včetně in-house aplikace nebo testování AppConnect partners aplikací. Některé změny byly vyvolány příchodem iPadů z jiných oddělení společnosti správu v MobileIronu. Systém se osvědčoval u posádek a ostatní vedoucí chtěli také využívat výhody EMM platformy tak, aby oni sami nebo jejich zaměstnanci mohli pro práci použít iPad. Postupem času bylo rozhodnuto, že všechna zařízení iPad budou pod správou MobileIron s plnou podporou MobileIron klienta.

Vzhledem k rozsahu práce není možné definovat a přiblížit všechny změny provedené do současné doby, proto bude zmíněno několik změn, které byly zajímavé a budou krátce rozepsány.

Přechod na Kerberos

Ověřování uživatelským jménem a heslem bylo použito v Exchange profilu a v přístupu k Sharepoint úložišti přes Priority Folders v Docs@Work. Postupem času narůstala chybovost, převážně v části Docs@Work. Problém se projevoval tak, že složky, které se měly automaticky synchronizovat, viděl uživatel ve stavu odpojeno a byl nucen zadat heslo pro přístup do složek a případnou synchronizaci. Chování chyby bylo různorodé. Někteří uživatelé nehlásili žádné problémy a ti co hlásili problém, tak v několika různých variantách. Byla ověřena funkčnost ověřování na straně MobileIron a Sharepointu.

Po několika neúspěšných pokusech o dohledání příčiny chyby, dodavatel doporučil přejít na variantu ověřování pomocí Kerberos constrained delegation, kdy se uživatelé nebudou ověřovat pomocí hesla, ale pomocí certifikátu. Uživatel se ověřuje certifikátem na Sentry serveru, dále pak pomocí Kerberos ticketu na interním serveru (Exchange, Sharepoint).

Po stránce nastavení je nutné odladit ověřování Kerberos za chodu celého systému. Prvním krokem je příprava servisního účtu pro Kerberos na straně systému společnosti, vygenerování keytab souboru, jak bylo zadáno v požadavcích na implementaci. Nastavení ověřování Kerberos bylo připraveno na straně EAS a Sharepoint. Finální konfigurace byla provedena na Sentry serverech a VSP serveru. Následovalo testování, při kterém se zkoušela dostupnost systému přes testovací zařízení. Výsledkem bylo funkční ověřování bez nutnosti zadávání hesla pro Exchange profil (hlavní) a Docs@Work. Šlo o jednoznačný přínos pro uživatele a zároveň byla zachována míra zabezpečení. Jakmile zařízení uživatele bylo odebráno z VSP serveru, byl okamžitě smazán jeho certifikát, a ačkoliv Kerberos mohl být ještě aktivní, Sentry server již přístup blokoval. Výhodou je, že uživatel nemá přístup k samotnému Kerberos ticketu, s tím pracuje Sentry server na základě požadavku ze strany certifikátem ověřeného uživatele.

Přechod na Docs@Work aplikaci

Docs@Work byl zprvu součástí aplikace MobileIron, klienta, který byl instalován na každém iPadu. MobileIron následně oddělil komponentu Docs@Work do samostatné aplikace a nadále pak udržoval obě možnosti konfigurace do doby, kdy původní Docs@Work zmizel z možností konfiguračních profilů a aplikace MobileIron přišla o tuto sekci. Více informací o konfiguraci a používání Docs@Work je obsažen ov kapitole 4.9.2.

Úpravy AppConnect

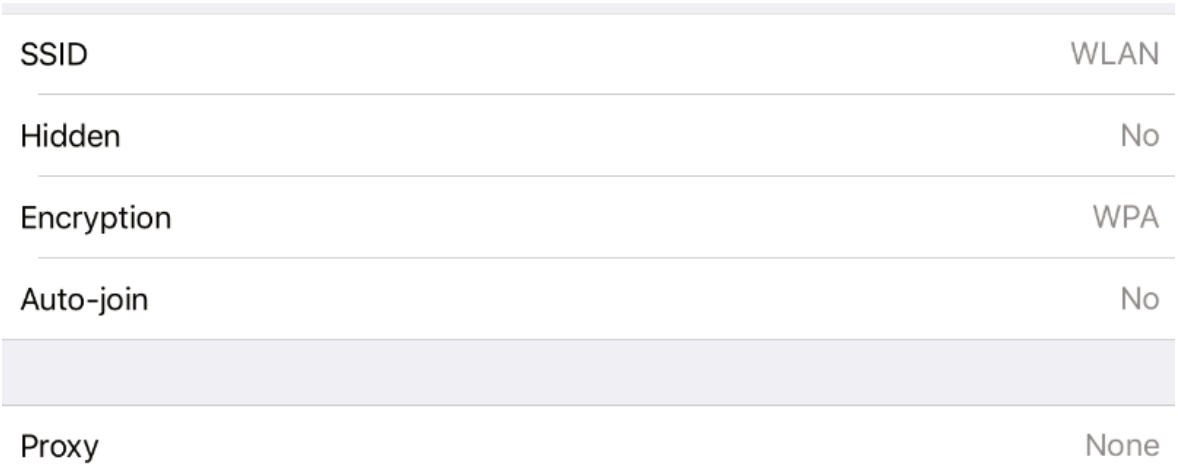
AppConnect politiky od první konfigurace neprocházely razantními změnami. Byla provedena pouze jedna změna v konfiguraci, vyvolaná právě zařazením iPadu jiného oddělení společnosti pod správu MobileIron. Přidala se navíc další AppConnect politika s povoleným tiskem pro AppConnect aplikace. Tato změna byla schválenou výjimkou pro jedno oddělení ve společnosti. Tamější zaměstnanci pracovali převážně s PDF formuláři, a museli každý formulář po vyplnění tisknout. Tato zařízení byla dokonce připojena do vnitřní sítě a byla používána pouze v rámci společnosti. Na základě těchto podmínek byla udělena výjimka.

Konfigurace Wi-Fi profilů

Budova společnosti byla pokryta Wi-Fi signálem s vyhrazenými sítěmi pro mobilní zařízení. Takto vyhrazená síť nebyla v první konfiguraci doručována jako profil do zařízení. Úvaha nad využitím Wi-Fi konfiguračních profilů se objevila až v momentě nového požadavku, která se týkal Wi-Fi sítí v samotných letadlech. Letadlo, které bylo takto vybaveno, mohlo být za letu připojeno do internetu a pasažéři mohli pomocí připojené Wi-Fi surfovat, stahovat a odesílat emaily apod. Náklady spojené s přenesenými daty za letu jsou vysoké.

Ačkoliv se posádky mohly také k síti připojit a využít síť, bylo nežádoucí, aby se opětovně připojovaly bez svého vědomí. Zařízení iPad se k Wi-Fi síti chová tak, že pokud se jednou k síti připojí, bude se k síti připojovat pokaždé, jakmile bude v dosahu. Toto chování je obvyklé na většině mobilních zařízení, a pokud lze změnit, je automatické připojování ke známým sítím výchozím nastavením.

Cílem nové konfigurace bylo, zamezit posádkám automatické připojování zařízení k těmto sítím. V prvním kroku bylo identifikováno, která letadla disponují připojením k bezdrátové síti s přístupem do internetu. Každé letadlo mělo vlastní konfiguraci, tedy vlastní SSID sítě, přístupové heslo, šifrování. Bylo nesmírně důležité připravit konfigurace s nastavením shodným, jako bylo nastavení sítě v letadle, jinak profil nebyl ve shodě a potřebný parametr nefungoval. Připravené konfigurace pak byly v jednotlivých letadlech odzkoušeny a konfigurace v některých případech opraveny. Posledním krokem byla provedena distribuce na skupiny posádek tak, aby každý měl v zařízení potřebný profil za každé letadlo, který měl deaktivovaný atribut „Auto join“.



Obrázek 23 - Příklad doručeného profilu do iOS- volba auto-join „No“ [91]

Používání Wi-Fi profilů, může zkomplikovat používání klíčenky na iOS zařízení. Klíčenka je nástroj, který mimo ostatní funkce, také synchronizuje mezi iOS zařízeními jednoho uživatele informace o připojených a konfigurovaných Wi-fi sítích. Klíčenka je součástí nastavení iCloud na iOS zařízení. Komplikace mohou nastat, pokud uživatel používá více iOS zařízení a klíčenku. Pokud k synchronizaci připojených Wi-Fi sítí dojde a uživatel nemá povoleno ze svých zařízení přístup do shodných sítí, může dojít k blokaci. K těmto případům může docházet, pokud jsou nastaveny oddělené Wi-Fi sítě pro telefony (iPhone) a tablety (iPad) a pokud je přístup na nesprávnou síť trestán blokací přístupu po určitý čas. Další komplikací je případ uživatele, který na svém iOS zařízení, kam není doručen Wi-Fi profil z EMM, upraví nastavení Wi-Fi sítě, která je profilem nastavena na druhé zařízení již s profilem EMM. Takovým úkonem se doručený Wi-Fi profil z EMM stává nefunkčním a je nutno administrátorem provést „re-push profilu“, ručně provedenou distribuci konfiguračního Wi-Fi profilu. Je vhodné pamatovat na tato úskalí při návrhu a uživatele informovat o možných problémech.

Práce s aplikačním katalogem

Aplikační katalog byl měněn dle požadavků uživatelů a vedoucích oddělení. Byly přidávány specializované aplikace, přidávány do jednotlivých kategorií tak, aby se uživateli ve firemním aplikačním portále Apps@Work zobrazovaly správně zařazené. Nevýhodou řešení Apps@Work byla situace, kdy uživatel aplikaci stáhl z veřejného App Store a nikoliv z Apps@Work. Pak bylo nutné požádat uživatele, aby takovou

„unmanaged“ aplikaci smazal a nainstaloval ji znovu, přes Apps@Work. Unmanaged aplikace se chová tak, že není přímo spjata s MDM profilem a pokud uživatel poruší bezpečnostní požadavky, smaže ručně MDM profil nebo z jiného důvodu mu bude odebrán firemní obsah, unmanaged aplikace mu na iPadu zůstane včetně dat. Na unmanaged aplikaci se nevztahují i další nastavení z aplikačního katalogu, například ochrana proti zálohování aplikace do iTunes nebo iCloud. V současné době má VSP (Core) server funkci, která takovou situaci řeší. Administrátor může na koncové zařízení zaslat požadavek na překlopení aplikace z unmanaged módu do managed módu. Dnes je funkce konvertování unmanaged aplikace rozšířena o volby, zda konvertování provést v rámci vybraného uživatele, vybraného labelu nebo pro všechny uživatele. Podobným způsobem lze uživatelům posílat také požadavky na aktualizaci nebo novou instalaci aplikace.

Další z možností, která byla ve společnosti využita, bylo publikování in-house aplikace přes MobileIron. Vlastní vytvořenou aplikaci je možné distribuovat nahráním samotného IPA souboru a doplnit některé klíčové informace, jako je verze, kategorie aplikace a další. Aplikaci lze stejným způsobem aktualizovat při ponechání stejného názvu.

Konfigurace Assemble

Verze aplikací, které byly používány na zařízeních posádek, bylo nutné začít striktně kontrolovat. Byla vyvolána diskuze s dodavatelem, který doporučil řešení pomocí MobileIron Assemble nástroje. Přiblížení k nástroji MobileIron Assemble a jeho konfiguraci přináší kapitola 4.9.3.1.

Testování AppConnect partner aplikací

MobileIorn na svých stránkách „MarketPlace“ dává k dispozici seznam AppConnect Partners aplikací. V podstatě jde o aplikace třetích stran, které využívají MobileIron SDK, AppWrapping nebo API a je možné je provozovat s využitím AppConnect technologie. Každá aplikace má svoje vlastnosti, může být zdarma, ale zároveň může mít vlastní model licencování, nezávisle na licencích zakoupených od MobileIronu. Je ve prospěch každé EMM platformy, aby měla dostatek takových partnerů, napomáhá to urychlení integrace mobility ve společnosti. Zmíněný MarketPlace je rozdělen do kategorií, které lze prohledávat.

Za zajímavé AppConnect partnery z pohledu společnosti byly označeny:

Tabulka 26 - Příklad partnerských aplikací AppConnect

Prodejce	Produkt
Adobe Systems Incorporated	Adobe Acrobat Reader
InfraWare, Inc.	Polaris Office for Mobileiron
Box	Box for EMM
Infragistics Business Solutions, Inc.	ReportPlus for MobileIron
Infragistics Business Solutions, Inc.	SharePlus for MobileIron
Druva	Druva inSync for MobileIron
Cisco Systems	AnyConnect Secure Mobility Client
Check Point Software Technologies, Ltd.	Check Point Mobile VPN
Check Point Software Technologies, Ltd.	Check Point Mobile Threat Prevention

Zdroj: [104]

Nespornou výhodou je v případě používání EMM platformy od MobileIronu to, že MobileIron je zákládajícím členem komunity AppConfig. Aplikace pro fungování v rámci AppConnect technologie pak lze hledat i mezi ISV členy AppConfig. [89]

4.9.2 Synchronizace dokumentu

Nastavení synchronizace dokumentů byl klíčový prvek fungování iPadu jako EFB zařízení. Digitální forma dokumentů měla být dostupná posádkám za letu i na zemi vždy v aktuální verzi, při zajištění základní ochrany dat. Předchozí model fungování byl problematický z pohledu verzí dokumentů, které mohli mít uživatelé mezi sebou rozdílné. Nový systém tak měl přinést mnohá zlepšení v zjednodušené administraci, automatizované synchronizaci a jednoduchém přístupu k dokumentům ze zařízení.

Při nasazování nových EFB zařízení byly definovány základní podmínky synchronizace dokumentů do EFB zařízení:

- doručit na zařízení konfiguraci synchronizace bez nutného nastavení uživatelem,
- doručovat na zařízení vždy aktuální verze dokumentu,
- mít na zařízení dokumenty dostupné online,

- mít na zařízení dokumenty dostupné offline (za letu, na letišti mimo signál),
- zajistit DLP – ochrana proti ztrátě firemních dat,
- další
    - zajistit potvrzení o přečtení dokumentů,
    - kontrola aktuální verze dokumentů.

MobileIron za těchto podmínek vyhovoval svojí komponentou Docs@Work. Nesplňoval pouze podmínky zajištění potvrzení o přečtení dokumentů a vzdálené kontroly verze dokumentů na zařízení. To byly spíše funkcionality moderního DMS systému.

Docs@Work byl již u řady společností používanou součástí, ale offline synchronizace (Priority Folders) v době implementace MobileIronu ve společnosti byla novinkou. Z nabízených možností sdíleného úložiště, ze kterého bylo možné dokumenty synchronizovat, byl vybrán Microsoft Sharepoint. Firma disponovala edicí Microsoft Sharepoint Foundation 2010, který byl také podporován.

Spuštění Docs@Work zahrnovalo přípravu struktury doručovaných dokumentů a přípravu prostředí v MS Sharepoint. Struktura dokumentů byla určena dokument administrátorem společnosti, který vydefinoval potřebné dokumenty a jejich rozdělení pro synchronizaci do koncového zařízení. Při tvorbě struktury dokumentů bylo nutné dodržet pravidla synchronizace do Docs@Work. Do zařízení bylo možné v Docs@Work synchronizovat, v režimu offline synchronizace, konečné složky, ale bez podadresářů. Tomu byla přizpůsobena také příprava prostředí Sharepointu, kde byl vystaven nový web s knihovnou, která obsahovala definované složky dokument administrátorem.

Práce dokument administrátora pak spočívala v nahrání nového dokumentu nebo nové verze dokumentu na Sharepoint a pomocí konfigurace Docs@Work v MobileIronu byl nový dokument nebo nová verze dokumentu doručena do zařízení, jakmile bylo zařízení online. Jak často a na jakém typu sítě se dokumenty synchronizovaly, určovala konkrétní Docs@Work konfigurace.

Struktura Sharepointu se v průběhu času změnila, především na základě příchodu nové aplikace Docs@Work a hlavně z důvodu začlenění iPadů dalších oddělení společnosti pod správu MobileIron včetně synchronizace dokumentů. Pro každé oddělení byl tak vytvořen nový web, kde dokument administrátor udržuje aktuální dokumenty synchronizované do zařízení.

Na straně MobileIron figurovaly potřebné konfigurace. Jak již bylo v předchozích kapitolách nastíněno, na začátku probíhala konfigurace Docs@Work Original v rámci aplikace MobileIron (Mobile@Work). Konfigurace v Docs@Work v rámci Mobile@Work byla pojmenována Docs@Work Original. Během dalšího období MobileIron ukončil podporu Docs@Work Original a přinesl zákazníkům samostatné a oddělené řešení sdílení firemního obsahu, samostatnou aplikaci MobileIron Docs@Work.

Docs@Work Original

Konfigurace Docs@Work Original probíhala na VSP (Core) serveru. Každá koncová složka ve sdíleném úložišti měla vlastní konfiguraci. Docs@Work Original profil obsahoval nastavení adresy Sentry serveru, cesty ke sdílené složce a nastavení parametrů synchronizace. Ty určovaly, v jakém časovém intervalu bude kontrolována sdílená složka na nové verze dokumentů, zda se bude kontrola a stahování provádět pouze na Wi-Fi nebo také přes mobilní data a jak velký objem dat, lze najednou přenášet.

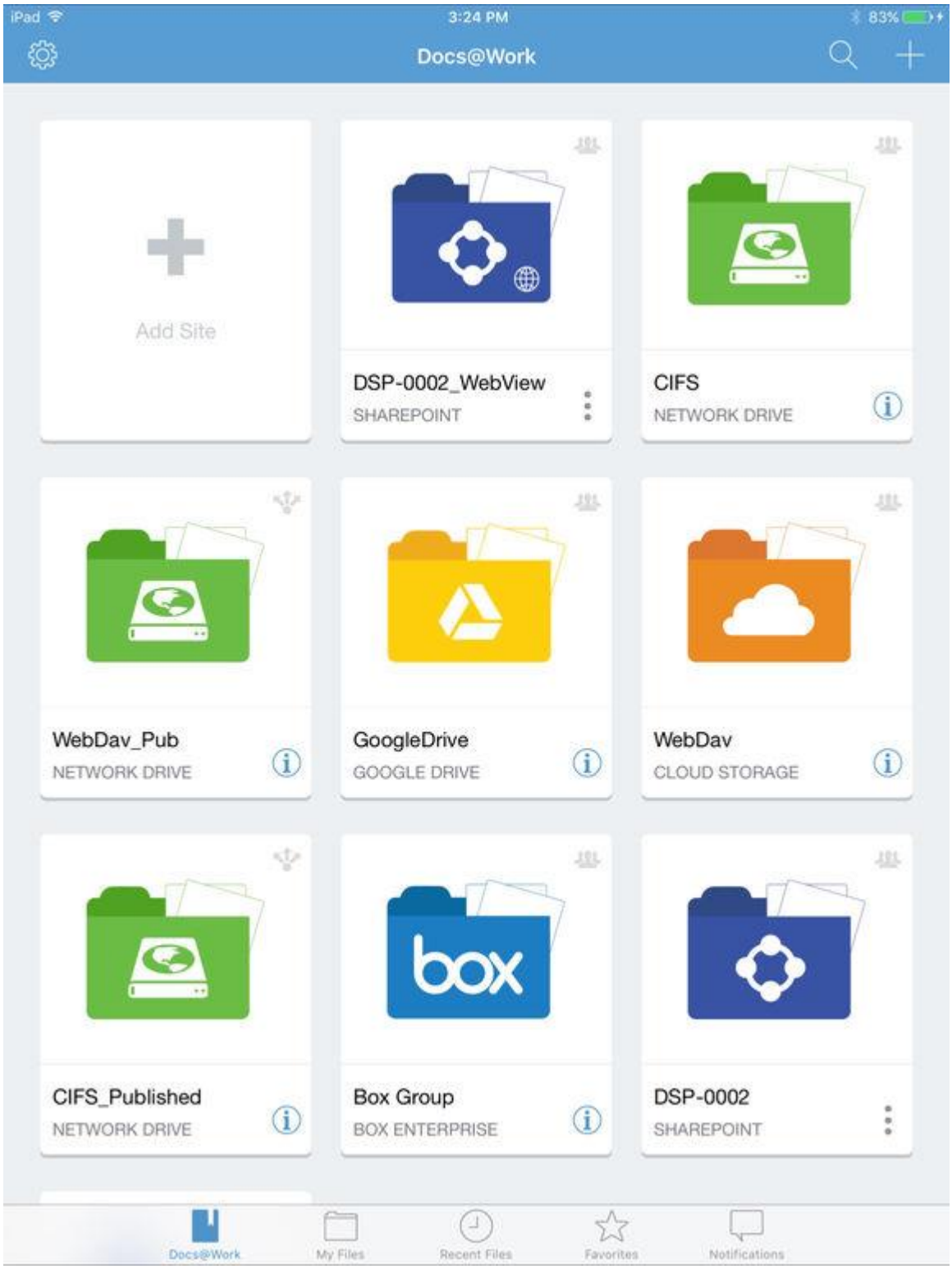
Následovala distribuce na koncová zařízení. Dokumenty měly v aplikaci Mobile@Work vlastní záložku, kde se pro uživatele zobrazovaly jemu přiřazené a synchronizované složky. Složky byly označeny zeleně, pokud byly synchronizovány v pořádku, nebo modře, pokud probíhala synchronizace, nebo červeně, pokud byly složky odpojené (chyba ověřování), nebo šedě pokud bylo zařízení offline. Stejné barevné označení nesly dokumenty ve složkách.

V rámci používání se od začátku konfigurace objevovaly první problémy s ověřováním. Ačkoliv bylo povolené uložení přihlašovacích údajů, aplikace u některých uživatelů požadovala ověření opětovně, v některých případech neověřila uživatele v offline režimu a uživatel tak nemohl přistupovat k dokumentaci. Vzhledem k povaze důležitosti dostupné dokumentace za letu, v offline režimu, bylo nutné problém odstranit. Řešením byl přechod na Kerberos ověřování. Po několika dalších verzích Mobile@Work bylo u některých uživatelů zaznamenáno zvláštní chování. Jeden ze synchronizovaných dokumentů byl označen zeleně, jako aktuální, ale na Sharepoint sdílené složce již byla nová verze dokumentu. Jediným možným řešením bylo znovu provést synchronizaci dokumentu a to dvěma způsoby. Prvním bylo na Sharepointu dokument smazat a znovu nahrát, to ale ovlivnilo všechny uživatele. Druhým možným řešením bylo uživateli odebrat dočasně Docs@Work Original profil a zpět vrátit, tím proběhlo znovu nahrání všech

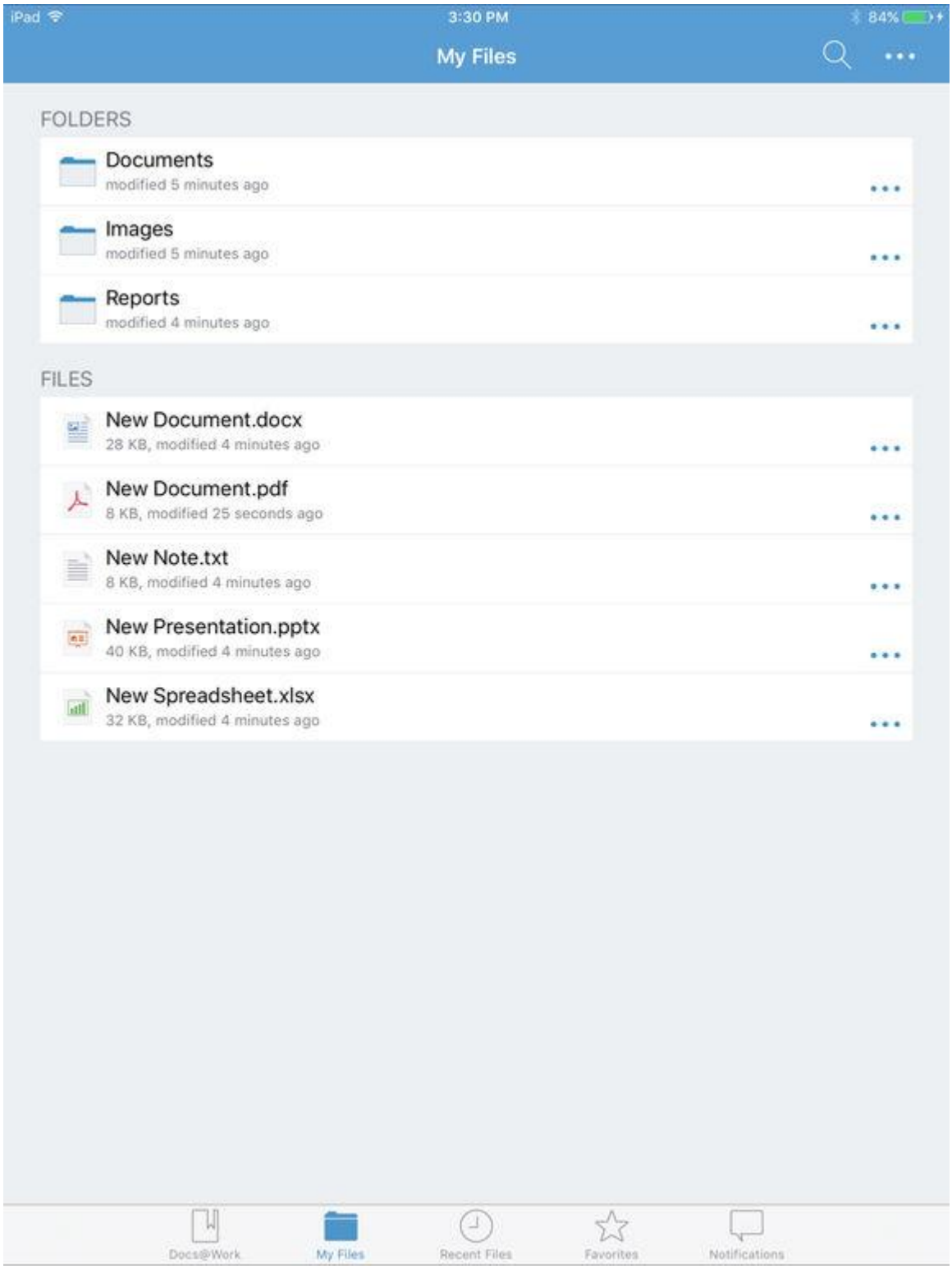
složek a všech dokumentů. V době, kdy se tento problém vyskytl, již nebyl Docs@Work Original podporovaný MobileIronem a probíhalo testování nové aplikace Docs@Work, na kterou se záhy přešlo.

Docs@Work

Samostatná aplikace Docs@Work přináší více možností oproti původní verzi Docs@Work Original. Konfigurace profilu Docs@Work nabízí více možností a samotná aplikace má k dispozici více funkcí. Aplikace se rozděluje na část Docs@Work, kde je možné nastavit sdílené složky propojené s MS Sharepoint, WebDav, případně i veřejnými úložišti jako Box, Dropbox, Drive a další. Sdílené složky lze nastavit jako online náhled nebo formou synchronizace do offline režimu. Další záložka, My Files, je lokální část aplikace, kde může uživatel ukládat své dokumenty, vytvářet nové včetně adresářové struktury. Recent Files a Favourites pracují jako náhled, pro dokumenty které byly v rámci aplikace naposledy otevřeny nebo označeny jako oblíbené. Poslední záložka Notifications upozorňuje na nové změny v Docs@Work části, jako nově nahraný dokument nebo nově aktualizovaná verze dokumentu.



Obrázek 24 - Příklad sdílených složek aplikace Docs@Work [105]



Obrázek 25 - Část "My Files" aplikace Docs@Work [105]

Konfigurace Docs@Work obsahuje nastavení Sentry serveru, nastavení sdílených složek pro synchronizaci, definici atributů synchronizace a specifické rozšiřující konfigurace. Oproti Docs@Work Original, kde bylo pro každou sdílenou složku nutno vytvořit konfigurační profil, v novém Docs@Work se v jednom konfiguračním profilu nadefinují všechny potřebné složky, například pro určitou skupinu uživatelů. Specifické konfigurační atributy pak dále doplňují konfiguraci. Přes atributy lze nastavit, aby uživatel nemohl vytvářet vlastní sdílené složky v Docs@Work, nebo pouze zakázat vytvoření sdílených veřejných složek z Dropbox , Boxu nebo Google Drive.

Konfigurace obsahovala pouze sdílené složky v MS Sharepoint bez možnosti, aby si uživatel mohl tvořit vlastní sdílené složky kamkoliv jinam. Synchronizace byla nastavena po 5 minutách, pouze na Wi-Fi síti a s maximálním přenosem 500 MB. Aplikace s konfigurací byla testována a následně distribuována k uživatelům, při spolupráci s dokumentovým administrátorem společnosti tak, aby byla zajištěna potřebná struktura a funkčnost dokumentů.

Při používání aplikace byly identifikovány některé první problémy. Obecně se jednalo o rychlost aplikace a netransparentnost stahování dokumentů.

Nebylo zřejmé, který dokument byl stažen a který ne. Aplikace na úvodní stránce v části Docs@Work informuje, co právě dělá, například stahování některé konkrétní složky, ale není k dispozici informace, jak se stahují konkrétní dokumenty. Aplikace také byla výrazně pomalejší oproti předchozí verzi Docs@Work Original při načítání dokumentů pro zobrazení. Převážně u dokumentů, které byly větší, šlo o řády minut. Postupem času MobileIron zapracovává opravy chyb, nové funkce a rychlost se také výrazně zlepšila. Od verze Core serveru 9 a verze Mobile@Work 8.5, již není k dispozici konfigurace Docs@Work Original.

Alternativa Docs@Work

Existuje řada aplikací, které umožňují připojení sdílených složek a jsou dokonce v seznamu AppConnect partners. Příkladem můžou být aplikace Box for EMM, Dropbox EMM, FileBrowser for Business, vždy dle aktuálního seznamu MarketPlace MobileIron nebo AppConfig ISV členů. Pro porovnání je ale nutné hledat alternativní řešení v rozsahu, v jakém funguje Docs@Work. Je nutné brát v potaz, že MobileIron pro svou komponentu má připravený konfigurační profil a není tak nutné na každém zařízení zvlášť konfigurovat

sdílené složky a přístup k nim. Navíc se vhodně využívá ověřování přes Kerberos v rámci Sentry serveru, uživatel tak nemusí složitě zadávat uživatelské jméno a heslo, přihlašovací údaje nejsou nikde ukládána. Dále je Docs@Work součástí AppConnect technologie, je tak zaručeno dodržování ochrany dat dle AppConnect politik. A dalším důležitým prvkem je cena. Většina aplikací třetích stran je licencována zvlášť, zatímco Docs@Work je již součástí Gold licence od MobileIronu. EMM Gold licenci, dle Obr č. 26 níže, je nutné pořídit minimálně při využití AppConnect technologie.[106]

Mobile Security:	EMM Silver	EMM Gold	EMM Platinum
Core	✓	✓	✓
Sentry	✓	✓	✓
Apps@Work	✓	✓	✓
AppConnect		✓	✓
Email+		✓	✓
Docs@Work		✓	✓
Web@Work		✓	✓
Help@Work			✓
Tunnel			✓
MobileIron Monitor			✓
ServiceConnect Integrations			✓

Obrázek 26 - Přehled balíčku MobileIron licencí [107]

4.9.3 Management aplikací

Správa aplikací zahrnuje práci s aplikačním katalogem, nákup placených aplikací a také vlastní kontrolu instalovaných aplikací. Administrátor v Admin portálu VSP (Core) serveru spravuje aplikační katalog, může přidávat, odebírat aplikace linkované z App Store nebo in-house vlastní aplikace. Aplikace mohou být přiřazovány na skupiny uživatelů a těm pak skrze server rozesílat požadavky na instalaci, aktualizaci nebo konvertování na managed aplikace. Administrátor také vidí, jaké aplikace jsou na zařízení instalované a v jakých verzích. VSP (core) server je v roli hlavního nástroje pro správu aplikací. Zpřísněním požadavků na kontrolu aplikací se ale narazilo na některé z limitů VSP (Core) serveru a jeho managementu aplikací. Jedním z příkladů může být generovaný report, který by měl obsahovat seznam zařízení a na nich instalovanou verzi určité aplikace, nebo daný report ještě rozšířit o notifikaci na uživatele, kteří používají zastaralou verzi aplikace.

Zpřísnění kontroly verzí aplikací, požadavky na rozšířený reporting a rozesílání notifikací, vedlo k rozhodnutí instalace a použití nástroje MobileIron Assemble.

Management aplikací je citlivá záležitost. Je zde velká náchylnost k chybě vzhledem k různým problémům. Základním kamenem úrazu je absence možnosti instalovat starší verzi aplikace, pokud nově stažená verze vykazuje problémy.

Příkladem může být stornování verze aplikace Cisco AnyConnect VPN klienta na Apple App Store. Uživatelům, kteří si v době dostupnosti novou verzi aplikace stáhli, po jejím stornování na App Store, přestala aplikace fungovat. Uživatelé ztratili přístup do firemního prostředí pomocí VPN, díky chybě mezi vývojáři aplikace a zástupci z App Store. Problém trval několik hodin. Nemusí ani dojít k chybě nebo stornování verze aplikace na straně Apple, ale samotný vývojář aplikace může způsobit chybu, je pak důležité nedovolit uživatelům stahovat nejnovější verze aplikací, bez předchozího testování.

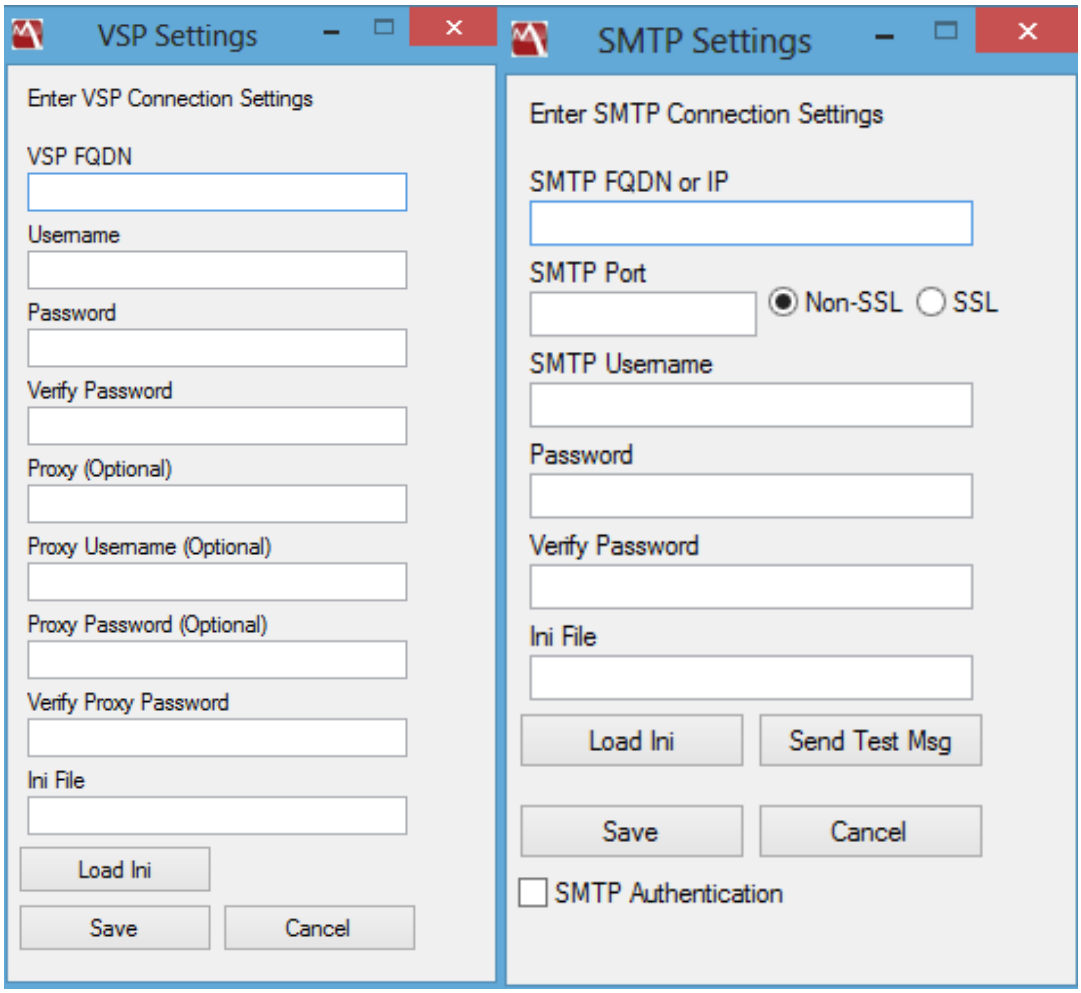
4.9.3.1 Nákup aplikací

Nákup aplikací v době nedostupnosti Apple VPP programu byl řešen formou GIFT kódů. Ty byly rozesílány na koncové uživatele ručně, pomocí aplikace iTunes. Úskalí této podoby nákupu se nachází v možné různorodosti použitých Apple ID na zařízeních. Pokud uživatelé používají různá Apple ID, mohou mít nastaveny odlišné regiony obchodu App Store. V každém případě je nutné pro uživatele nakupovat GIFT aplikace vždy v iTunes Store, který má nastavenou zemi (region) shodně jako je nastavená země App Store u Apple ID, kde GIFT aplikace bude použit. Pokud nakupujeme v rámci různých regionů, je nutné mít pro každý region zvlášť Apple ID a k němu přiřazenou platební kartu, vydanou v dané zemi (regionu). Kontrola a zjištění jaký region u jakého Apple ID je použit nelze přes EMM platformu zjistit. Výše definované úskalí by měl vyřešit Apple VPP, který umožňuje hromadný nákup a distribuci aplikací pro firemní použití, a je již dostupný pro Českou republiku.

4.9.3.2 MobileIron Assemble

Nástroj MobileIron Assemble měl za úkol pomoci administrátorům s plněním kontroly verzí aplikací, rozšířeným reportováním a rozesíláním notifikací. Jde o silný nástroj, který má široké portfolio využití. Kromě zmíněných úloh lze dynamicky provádět různé akce nad zařízeními za splnění podmínek a filtrů. MobileIron definuje atributy, které z VSP serveru je možné číst, měnit a ovládat, jaké akce lze provádět a jaká je vlastní syntaxe. MobileIron Assemble je rozšířením standardních funkcí EMM platformy MobileIron. Assemble pracuje formou skriptů, které si administrátor napíše pomocí příručky, která je k nástroji přiložena. Skripty pak lze spouštět ručně nebo pomocí plánovače úloh. Nástroj Assemble je možné instalovat na Windows Server, který má povolenou konektivitu na VSP (Core) server na portu 443.

V prvním kroku je provedeno nastavení základních konfiguračních INI souboru pro server VSP a SMTP server. Níže obr. 27 zobrazuje, jaké položky je nutné vyplnit. Na straně VSP (Core) serveru musí být připraven lokální uživatel, který bude v konfiguraci vyplněn.



Obrázek 27 - Konfigurace VSP a SMTP serveru pro použití Assemble [108]

Po úspěšné konfiguraci je možné začít vytvářet skripty. Jejich tvorba a příklady obsahuje příručka dodaná s nástrojem. Náhled do syntaxe skriptu zobrazuje obr. č. 28.

```
[RuleNum]
numberofrules=1
sleeptime=250
delimeter=,

[Rule1]
NumberofElements=1
Wakeup=yes
Action=message
ActionReason=send message to all devices
SendMessage=yes
SendMessageText="Well, Hello there! :)"
Element1_trigger=label:name
Element1_description=all company owned devices
Element1_operator=contains
Element1_source=local
Element1_value=
```

Obrázek 28 - Syntaxe Assemble skriptu [108]

Pomocí Assemble jsou skriptem řešeny tyto úlohy:

- report zařízení se zastaralou verzí aplikace (pro různé aplikace),
- týdenní report všech instalovaných aplikací na zařízení,
- notifikace
    - požadavek na aktualizaci aplikace (pro zařízení se zastaralou verzí),
    - požadavek na aktualizaci iOS (pro zařízení se zastaralou verzí, pro zařízení pro která je aktualizace dostupná),
- dočasné aplikování labelu za splnění definovaných podmínek.

4.9.4 Údržba a provoz MobileIron

Provádění záloh, aktualizací serverů a další opatření spadají do odpovědností administrátorů EMM řešení a jsou zejména kritické pro samotnou bezpečnost řešení. Nezbytnou součástí údržby řešení je pravidelná obnova certifikátů, nebo pravidelná kontrola logů jednotlivých serverů. Je doporučeno nastavení notifikací do sběrné schránky, kterou administrátoři kontrolují, v případě různých alertů nebo oznámení ohledně spravovaných zařízení a celé EMM infrastruktury.

Zálohování

Zálohovat MobileIron řešení je možné po jednotlivých serverech. Vzhledem k instalaci serverů do virtuálního prostředí probíhalo zálohování každé VM zvlášť, v pravidelných intervalech. VSP (Core) server může být zálohován také vlastní integrovanou funkcí, která se nazývá System backup. Pro System backup lze nastavit, kam se má záloha ukládat a v jakých pravidelných intervalech se bude záloha provádět. Umístění pro zálohu může být lokální na VSP (Core) serveru nebo do sdílené složky v síti. Sentry servery byly zálohovány jako virtuální stroje, ale vzhledem k tomu, že neobsahují žádnou databázi, není záloha příliš kritická. Postačí do zálohovaného umístění uložit nebo přepsat poslední aktuální konfiguraci.

Upgrade

Od zavedení EMM MobileIron ve společnosti probíhalo pravidelné provádění aktualizací serverů. Důvodem je podpora nových funkcí, vylepšení řešení, opravy chyb a zejména podpora nových verzí OS mobilních zařízení. Od verze 8 VSP (Core) serveru nastal zlom, kdy MobileIron integroval do svého řešení modul pro aktualizace podpory nových verzí a typu mobilních operačních systému. Pokud tedy Apple vydal novou verzi iOS, nebylo nutné provádět upgrade celého VSP (Core) serveru, ale pouze proběhl platform update v rámci serveru, který zajistil podporu nového OS. Tyto samostatné aktualizační balíčky pro podporu nových verzi OS, bylo možné stahovat automaticky nebo manuálně.

Co se týká provádění upgrade MobileIron řešení, dodržovala se tato pravidla:

- provádění upgrade včas, aby celé řešení bylo podporováno od MobileIronu,
- provádění upgrade tak, aby VSP a Sentry servery byly vzájemně kompatibilní,
- provádění upgrade ve spolupráci s podporou.

Co se týká samotného provedení upgrade, byl postup rozdělen na část před provedením upgrade, provedení upgrade a část po provedení upgrade. Na začátku většinou ze strany dodavatele byla oznámena nová verze. Administrátor konzultoval změny, novinky a známé chyby s dodavatelem a následně rozhodl, zda provést upgrade nebo setrvat na stávající verzi. V případě rozhodnutí pro provedení upgrade bylo nutné projít procesem přípravy, kdy se stávající řešení zálohuje, otestují se základní funkce a stáhnou

se potřebné balíčky. Provedení upgrade může provést administrátor nebo dodavatel. Po úspěšném provedení upgrade se provádí základní testovací proces. Jakmile je vše v pořádku, po několika dnech se smažou vytvořené zálohy. Pokud nastane problém v průběhu upgrade nebo po něm, je možné ze záloh navrátit původní funkční stav.

Kroky před provedením:

- konzultace s podporou ohledně již provedených instalací u jiných zákazníků,
- provedení kontroly novinek nové verze a známých chyb.

Příprava a provedení:

- zálohování všech serverů ve vypnutém stavu (konzistence dat) – na Hyper-V provedením snapshotu,
- kontrola funkcí EMM,
- provedení upgrade.

Kroky po provedení upgradu:

- testovací proces,
- smazání záloh nebo obnova ze zálohy.

Výjimkou nebyly ani samotné reinstalace serverů MobileIron. Například v momentě, kdy bylo doporučeno navýšení boot partition, bylo nutné VSP (Core) server instalovat jako nový. Ve zkráceném znění byl postup takový, že byl proveden System backup VSP (Core) serveru, na firewallu zakázány patřičné porty a byla provedena čistá instalace serveru. Poté následovala obnova z provedeného System backupu.

Nutnost zákazu portů na firewallu vychází z toho, že pokud by byl nově instalovaný VSP server s prázdnou databází dostupný pro mobilní zařízení, na těchto zařízeních by byl proveden „retire“. Pokud zařízení nemá dostupný VSP (Core) server, může i nadále fungovat. Je to zajištěno díky tomu, že Sentry server si uchovává poslední známou konfiguraci VSP (Core) serveru a poskytuje tak zařízením potřebné přístupy. Jediné co nelze v danou chvíli provádět je například vzdálené mazání zařízení, retire nebo přidání nového zařízení.

Certifikáty

V rámci EMM řešení je nutné každý rok obnovovat Apple push certifikát a dle data expirace také obnovovat SSL certifikáty.

5 Zhodnocení výsledků a doporučení

Fiktivní společnost bojovala s několika zásadními problémy v oblasti mobility. Projekt zavedení mobilní platformy do kokpitů letadel spustil v organizaci řadu procesů, jednání včetně bezpečnostního auditu. To mělo za následek odhalení několika rizikových oblastí. Lze vyjmenovat klíčové položky rizikových oblastí, mezi které lze zařadit nedostatečné zabezpečení mobilních zařízení, jejich nekontrolovaný přístupu k firemnímu obsahu, riziko úniku firemních dat a nepříliš dobře řízenou správu mobilních zařízení. Ovládání správy mobilních zařízení z více míst, evidence v tabulkách a určitá benevolence směrem k uživatelům, to vše generovalo čím dál tím silnější zátěž na vlastní IT oddělení. Příchod požadavku centrální správy mobilních zařízení tak byl brán jako velký krok směrem k lepším zítřkům v řešení mobilní platformy uvnitř organizace. Klíčovým faktorem byla správa iOS zařízení pro letové oddělení společnosti, ale v rámci samotného projektu byla rozšířena působnost změn na kompletní mobilní infrastrukturu společnosti, a to včetně BYOD zařízení. Byl to velmi náročný krok, který lze ovšem s odstupem času zhodnotit kladně.

Tíženému výsledku předcházelo určení důležitých požadavků na centrální správu, pro projekt také určení požadavků na zařízení a provozované aplikace. Vhodným krokem při sběru a kladení požadavků bylo zahrnutí klíčových uživatelů do společných jednání a diskuzí. Naslouchání těmto klíčovým uživatelům a zařazení řady jejich požadavků do celkového souhrnu řešení bylo nepochybně dobrým tahem. Důsledkem této úzké spolupráce bylo velmi hladké přijetí nových procesů a opatření mezi uživateli mobilních zařízení.

Výběr správy zařízení se přímo vázal na vymezené požadavky. Do posledních kol výběru nové platformy správy zařízení (EMM) tak propadla pouze řešení, která měla pro společnost smysl. Nutno podotknout, že všechna EMM řešení, která byla porovnávána, z velké části splňovala určené požadavky. Z řady jednání však vyplynulo, že ani tak EMM řešení, jako samotný dodavatel a budoucí podpora, bude hrát velkou roli v úspěšné implementaci a ve snadném nasazení nové platformy firemní mobility. Dodavatel je pro společnost, která nemá mnohé zkušenosti z oblasti mobilních zařízení, velmi důležitý partner, který by měl přinést přidanou hodnotu a předat část svého „know-how“. Zařazení hodnotících kritérií dodavatele do celkového hodnocení EMM platforem se vyplatilo. Ačkoliv byla vybrána bodově „horší“ platforma MobileIron, dobře hodnocený dodavatel

vyrovnal bodovou ztrátu. Bodový propad byl zaznamenán v rámci kritérií, která nebyla příliš důležitá, a v důsledku také nešlo o nějak výrazný propad.

Samotná implementace se také neobešla bez komplikací. Problémy které nastaly, byly ale vyřešeny buď opravou v nových verzích, nebo byly nalezeny jiné cesty k tíženému výsledku za pomoci dodavatele a jeho zkušeností. Při implementaci nedošlo k výraznému zpoždění, první zařízení byla registrovaná několik dní po instalaci MobileIron platformy. Několik týdnů poté byla sestavena finální konfigurace a distribuována do iPadů. Tímto krokem byla zahájena restrukturalizace mobilní infrastruktury společnosti. V dalších krocích byly identifikovány doposud připojené mobilní zařízení a byla provedena jejich migrace do nového prostředí. BYOD byl právně zajištěn a je nyní pod plnou kontrolou. V průběhu používání EMM byl také zrušen BES server, proběhla výměna BlackBerry zařízení za smartphony spravované pomocí EMM.

Výsledkem implementace je ucelená správa mobilních zařízení. Administrátor pracuje z jedné management konzole. Jsou jasně identifikována připojená zařízení, na kterých jsou vynucována bezpečnostní opatření. Je možné zařízení na dálku smazat, odemknout, vynutit přísnější politiky, provádět inventuru a další.

V porovnání s prvotním stavem se zásadně změnil výsledný počet zařízení připojených k firemním zdrojům. Všechna taková zařízení jsou pod správou EMM a jejich nové počty zobrazuje tabulka č. 27.

Tabulka 27 - Vysledný počet zařízení ve společnosti

	iOS	Android	BlackBerry	Windows	Celkem
Telefon	30	25	0	33	88
Tablet	100	0	0	1	101
Soukromé	8	30	0	0	38
Celkem	138	55	0	34	227

Zdroj: vlastní zpracování

Nelze jednoznačně hovořit o idealistickém nasazení EMM platformy. Řada zařízení se připojuje pomocí EAS, který je sice kontrolovaný a spravovaný přes MobileIron, ale neposkytuje tak širokou paletu funkcí, politik a konfigurací. Konečné řešení je kompromisem mezi požadavky na bezpečnost, funkčností a také cenovými náklady. Je zde prostor na postupné zlepšování, utahování bezpečnostních pravidel a prosazování firemních politik. Nezbytnými budoucími kroky nepochybně bude využití nově

povolených programů Apple pro Českou republiku, VPP a DEP, a přesun některých typů zařízení pod plnou kontrolu MobileIron.

Rozhodnutí pro implementaci EMM ve společnosti je vždy na zvážení, ale řada aspektů hovoří pro zavedení alespoň nějaké centrální správy. Pole mobilních zařízení se rozrůstá, zaměstnanci s nimi přichází do styku v soukromých životech a snaží se protlačit své požadavky do organizací, kde pracují. Ve společnostech, kde nebude řešena mobilita, nebude kontrolována a zabezpečena, hrozí velká rizika úniku firemních dat. Je doporučeno zvážit, zda je tato oblast dostatečně zabezpečena a provést klíčové rozhodnutí.
Naproti tomu, zakoupení licencí, implementace a používání EMM jsou nákladnou činností pro celou společnost, ať se to týká finančních nebo časových zdrojů. Je tak nezbytné vytěžit z daného řešení maximum, hledat jeho limity a snažit se neustále posouvat dopředu. Nejhorším scénářem je zamrznutí na bodu, kdy jsou zařízení zavedená ve správě, mají nahrané profily a nic dalšího není očekáváno. Pro takové účely dostačují daleko levnější řešení, některá zdarma nebo za minimální cenu licence.

V případě rozhodnutí pro EMM je dobré pamatovat na to, že řešení mobility by mělo přinášet komfortní a jednoduchý přístup k firemním zdrojům při zachování potřebné míry bezpečnosti a ochrany dat společnosti.

V rozhodování nesmí být ani opomenut přístup k pořizování nových zařízení, případně povolení BYOD zařízení svých zaměstnanců. Velmi zajímavým a vhodným řešením je spojení modelů CYOD a COPE, tedy nechat uživatele vybrat si jaké firemní zařízení bude používat a povolit využití zařízení pro soukromé účely.

Je doporučeno neustále sledovat novinky v oblasti EMM platforem, novinky v mobilních operačních systémech a být vždy o krok napřed před uživateli, aby se případná změna, chyba nebo nutná konfigurace vyřešila dříve, než se uživatel dostane do problému. V oblasti iOS světa se neustále odehrávají změny v operačním systému, které mohou přinést zajímavé novinky nebo také těžko řešitelné potíže. Je nutné pamatovat na to, že iOS byl stvořen pro spotřebitele a někdy je na firemní využívání zapomínáno. Některé nové funkce tak mohou zablokovat funkce správy nebo přístupu k firemnímu obsahu. Doporučením je hlídat každou verzi, podrobovat nové verze testování a mít zavedené správné postupy nejen v administrátorském světě, ale také na straně uživatelů. Je důležitá změna procesů, definice toho co uživatel může a nemůže na zařízení měnit, převážně být důrazní tam, kde jsou funkce EMM krátké a neumožňují vynucovat nebo omezovat to, co

potřebujeme. Ale zároveň se nelze nespoléhat na dodržování všech procesů a tam, kde nelze něco omezovat nebo vynutit nastavením, tam provádět alespoň predikci a kroky pro prevenci potíží.

Při hledání vhodné EMM platformy se nelze spoléhat na 100% pokrytí všech požadavků, které budou na centrální správu definovány, vždy jde o určitý kompromis mezi požadavky a reálnými možnostmi. Každý výrobce má snahu své řešení rozvíjet. Tak mohou být v dalších verzích některé nesplněné požadavky vyřešeny.

Pro správu iOS zařízení je doporučeno využít módu supervised zařízeních, ve spojení s Apple DEP programem a za využití Apple VPP pro licencování a distribuci aplikací, a naplno tak využít nabízených možností. Dalším zajímavým krokem může být pořízení zařízení s MAC OS, registrace a zaplacení vývojářského účtu a začít některé tíživé problémy řešit vlastním vývojem. V distribuci vlastních in-house aplikací je EMM velmi dobrým nástrojem. Nehledě na to, že MAC OS je ideální zařízení pro stahování logů a práci s iOS zařízeními a bez použití pro vývojové činnosti tak nalezne také uplatnění.

6 Závěr

Hlavním cílem práce bylo představit nasazení mobilních zařízení do firemního prostředí se zaměřením na iOS zařízení. Dílčími cíli práce bylo provést analýzu trhu sledované problematiky, definovat důležité pojmy z oblasti mobilních zařízení a jejich business zařazení a dále také uvést možnosti správy a nutné zabezpečení pro využívání mobilních zařízení ve firemním segmentu. Hlavní cíl práce a dílčí cíle byly splněny.

Práce se v teoretické části věnuje několika základním pojmům, které jsou v zadané oblasti častým tématem a přibližuje tak probíranou tématiku. Prostor je také věnován mobilním platformám, jejich určení a základnímu definování. Za platformy Apple iOS, Google Android a Microsoft Windows jsou vybrána zařízení a je provedeno jejich základní porovnání. Část zabezpečení mobilních zařízení uvádí hrozby, bezpečnostní politiky a antivirová řešení. Nedílnou součástí nasazení mobilních zařízení do organizací je jejich správa. Byly definovány možnosti správy se zaměřením na Enterprise Mobility Management. Správa zařízení byla podrobně rozebrána v rámci vybraných EMM platformách. Těmi byla řešení od společností MobileIron, VMware a IBM. Každá platforma EMM má svojí logiku a přístup ke správě zařízení. Pozornost byla také věnována společnosti Apple a cílení na podnikovou sféru. Správa zařízení může být rozšířena formou módu supervised zařízení, VPP a DEP programy.

Vlastní práce se věnuje tématu zařazení iOS zařízení do fiktivní společnosti od počátečních kroků až po konečnou implementaci a používání EMM platformy. Za fiktivní společnost byla vybrána letecká organizace, která řešila zavedení iOS zařízeních pro své posádky letadel. Kromě iOS zařízení měla společnost potíže se současným řešením mobility. Byla tak navržena implementace centrální správy mobilních zařízení v rámci celé společnosti. Následovaly kroky určení požadavků, výběru zařízení a jejich správy. Vybranou platformou správy zařízení se stal MobileIron. Práce seznamuje s implementací a používáním tohoto produktu. Zahrnuje úskalí a problematiku, které se v průběhu doby vyskytly. Výsledek zhodnocení je kladný, centrální správa přinesla tížené výsledky. Všechna mobilní zařízení se dostala pod kontrolu, na všechny zařízení byla doručena bezpečnostní politika a minimalizovalo se riziko úniku firemních dat. Posádky byly schopny pracovat s iPady jako EFB zařízením a bylo tak naplněno požadavku modernizace EFB zařízení. Nejde o konečný stav, který lze zlepšit supervised módem pro zařízení a zahrnutím Apple DEP a VPP programů. Takové nástroje lze efektivně používat

ve spojení s Enterprise Mobility Managementem a povýšit tak IT strategii firemní mobility. Mezi doporučení spadá vhodný výběr centrální správy v kombinaci s dodavatelem a podporou s přidanou hodnotou. Základním doporučením je stav mobility ve společnosti začít řešit, identifikovat rizika a vybrat vhodné řešení, které splní požadované potřeby.

7 Seznam použité literatury

1. PIERER, Markus. Mobile Device Management: Mobility Evaluation in Small and Medium-Sized Enterprises. Springer Fachmedien Wiesbaden, 2016. ISBN 978-3-658-15045-7.
2. První mobil jste mohli koupit před 30 lety. Od té doby se změnil k nepoznání. *Česká Televize - Media* [online]. 2013. [cit. 2015-08-20]. Dostupné z: http://www.ceskatelevize.cz/ct24/media/1074286-prvni-mobil-jste-mohli-koupit-pred-30-lety-od-te-doby-se-zmenil-k-nepoznani
3. JANEČEK, Vladislav. Cesta do pravěku: jak se zrodil tablet. *Tablety - historie* [online]. 2010. [cit. 2015-08-20]. Dostupné z:http://www.zive.cz/clanky/cesta-do-praveku-jak-se-zrodil-tablet/sc-3-a 153583/#utm_medium=selfpromo&utm_source=zive&utm_campaign=copylink
4. What is a Mobile Device? *Mobile Devices* [online]. 2015. [cit. 2015-08-20]. Dostupné z: http://mobiledevices.about.com/od/glossary/g/What-Is-A-Mobile-Device.htm
5. What is a Mobile Device? *Mobile Devices* [online]. 2015. [cit. 2015-08-20]. Dostupné z: http://www.gcflearnfree.org/computerbasics/9
6. BYOD. *Network security* [online]. 2015. [cit. 2015-05-20]. Dostupné z: http://www.compunet.cz/bezpecnost-siti-byod.php
7. SCHOALLERT, Tomas. Na jaká právní rizika si dát pozor při zavádění mobilních technologií v organizaci. IDC Enterprise Mobility. 2014. Prezentace
8. ROUBÍK, Tomáš. Na co si dát pozor při používání BYOD zařízení ve firmách? *Mobilní zařízení - BYOD* [online]. 2014. [cit. 2015-08-20]. Dostupné z: http://www.lupa.cz/clanky/na-co-si-dat-pozor-pri-pouzivani-byod-zarizeni-ve-firmach/
9. ČERMÁK, Miroslav. *BYOD: bezpečnostní politika. BYOD* [online]. 2012. [cit. 2015-08-20]. Dostupné z: http://www.cleverandsmart.cz/byod-bezpecnostni-politika/
10. KOUTNÁ, Eva. O přijetí BYOD často rozhoduje jednoduchost a bezpečnost. *Analýzy a studie* [online]. 2013. [cit. 2015-08-20]. Dostupné z:

http://computerworld.cz/analyzy-a-studie/o-prijeti-byod-casto-rozhoduje-jednoduchost-a-bezpecnost-49372

11. LIPPERT, Thomas. Jak zabezpečit mobilní zařízení ve firmách. *Hardware* [online]. 2012. [cit. 2015-08-20]. Dostupné z: http://channelworld.cz/clanky/jak-zabezpecit-mobilni-zarizeni-ve-firmach-7676
12. MobileDevice Ownership - How to Choose the Right Mix. Mobile [online]. 2014. [cit. 2016-12-13]. Dostupné z: Device Ownership - How to Choose the Right Mix.pdf
13. GOPALARATNAM, Mani. BYOD versus COPE: A look at the future of enterprise mobility. *Venturebeat* [online]. 2013. [cit. 2016-12-13]. Dostupné z: http://venturebeat.com/2013/05/01/byod-versus-cope-a-look-at-the-future-of-enterprise-mobility/
14. BlackBerry. Beyond BYOD BlackBerry Ovum. *Blackberry* [online]. 2014. [cit. 2016-12-13]. Dostupné z http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/Beyond-BYOD-BlackBerry-Ovum.pdf
15. STÝBLO, Karel. Cloud - historie, definice, modely a praktické využití. *Cloud* [online]. 2014. [cit. 2015-08-20]. Dostupné z: http://www.cs.vsb.cz/Files/osobni_stranky/michal-radecky/IT/2013/pr8-cloud.pdf
16. MARTINŮ, Ondřej. Který webový disk vám nabídne zdarma nejvíc? Prozkoumejte ty největší. *Web* [online]. 2014. [cit. 2015-08-20]. Dostupné z: http://technet.idnes.cz/cloud-uloziste-test0qh/sw_internet.aspx?c=A140922_124129_sw_internet_oma
17. LAŠ, Jan. Téma – Cloudová úložiště. *Web* [online]. 2015. [cit. 2015-08-20]. Dostupné z: http://android.chaputo.cz/tema-cloudova-uloziste/
18. LIPPERT, Thomas. Jak zabezpečit mobilní zařízení ve firmách. *Hardware* [online]. 2012. [cit. 2016-12-13]. Dostupné z: http://channelworld.cz/clanky/jak-zabezpecit-mobilni-zarizeni-ve-firmach-7676
19. Řešení Office pro firmu. *Officedoprace* [online]. 2015. [cit. 2015-08-20]. Dostupné z: http://www.officedoprace.cz

20. Exchange 2007 a správa mobilních zařízení. *Administrativa* [online]. 2011. [cit. 2015-05-20]. Dostupné z: http://www.samuraj-cz.com/clanek/exchange-2007-a-sprava-mobilnich-zarizeni/
21. ŘEHOŘ, Petr. Sekce bezpečnost. *ICZ* [online]. 2013. [cit. 2015-05-20]. Dostupné z: https://www.icz/files/2013_09_17_Z%C3%A1kaznick%C3%BD%20den/OVS_08_Bezpecnost.pdf
22. Co je to EMM řešení. *Produkty* [online]. 2015. [cit. 2015-08-20]. Dostupné z: http://www.system4u.cz/produkty/mobilni-reseni-emm-mdm/enterprise-mobility-management-emm/
23. Bezpečnost a správa mobilních zařízení. *Mobilní technologie* [online]. 2011. [cit. 2015-08-20]. Dostupné z: http://www.businessit.cz/cz/bezpecnost-sprava-mobilnich-zarizeni-android-apple-mdm.php
24. PIM. Personal information manager. *Gartner* [online]. 2017. [cit. 2017-01-03]. Dostupné z: http://www.gartner.com/it-glossary/pim-personal-information-manager/
25. PIM (Personal Information Manager/Management). *Gsmarena* [online]. 2017. [cit. 2017-01-03]. Dostupné z:http://www.gsmarena.com/glossary.php3?term=pim
26. NEWTON., L. Personal Information Management (PIM). *Business* [online]. 2017. [cit. 2017-02-22]. Dostupné z: http://www.business.com/software/personal-information-management-pim-software-basics/
27. SMITH, Rob., TAYLOR, Bryan., SILVA Chris., BHAT, Manjunath., COSGROVE Terrence., GIRARD, John. Magic Quadrant for Enterprise Mobility Management Suites. *Gartner* [online]. 2016. [cit. 2017-01-03]. Dostupné z: http://www.gartner.com/
28. About Gartner. *Gartner* [online]. 2017. [cit. 2017-01-03]. Dostupné z: http://www.gartner.com/technology/about.jsp
29. Gartner. *Gartner* [online]. 2017. [cit. 2017-01-03]. Dostupné z: http://www.gartner.com/technology/home.jsp
30. Gartner Magic Quadrant. *Gartner* [online]. 2017. [cit. 2017-01-03]. Dostupné z: http://www.gartner.com/technology/research/methodologies/research_mq.jsp#

31. ŽÁK, Čestmír. KREUZIGER, Pavel. Jak fungují magické kvadranty. *Inside* [online]. 2013. [cit. 2015-08-20]. Dostupné z: http://kpc-group.cz/wp-content/uploads/2013/07/magicke-kvadranty.pdf
32. MobileIron Core. *Mobileiron* [online]. 2017. [cit. 2017-01-09]. Dostupné z: https://www.mobileiron.com/en/products/platform-architecture/mobileiron-core
33. Visual Privacy. *Mobileiron* [online]. 2017. [cit. 2017-01-09]. Dostupné z: https://www.mobileiron.com/en/video/visual-privacy
34. What Is A Mobile SDK? *Redfoundry* [online]. 2016. [cit. 2017-01-09]. Dostupné z: http://www.redfoundry.com/what-is-a-mobile-sdk/
35. AppConnect and AppTunnel Datasheet. *Mobileiron* [online]. 2017. [cit. 2017-01-09]. Dostupné z: https://www.mobileiron.com/en/datasheet/appconnect-and-apptunnel-datasheet
36. MORIARTY, Joe. What is App Wrapping? *Contentraven* [online]. 2013. [cit. 2017-01-09]. Dostupné z: http://blog.contentraven.com/security/bid/297554/what-is-app-wrapping
37. MobileIron AppConnect 2.9.6 for iOS App Wrapping Developers Guide [online]. 2013-2017. [cit. 2017-02-06]. Dostupné z: MobileIron AppConnect 2.9.6 for iOS App Wrapping Developers Guide.pdf
38. What is the AppConfig Community? *Appconfig* [online]. [cit. 2017-01-16]. Dostupné z: https://www.appconfig.org/about/
39. AppConfig EMM/ISV Members. *Appconfig* [online]. [cit. 2017-01-16]. Dostupné z: https://appconfig.org/members/
40. Úřad pro civilní letectví. Použití EFB - Směrnice, CAA-SLP-042-n-14. *Caa* [online]. 2016. [cit. 2017-01-16]. Dostupné z: http://www.caa.cz/file/7766
41. U.S. Department of Transportation. Advisory Circular. *Faa* [online]. 2012. [cit. 2017-01-16]. Dostupné z: https://www.faa.gov/documentlibrary/media/advisory_circular/ac%20120-76b.pdf
42. Jeppesen Mobile FliteDeck. *Jeppesen* [online]. 2017. [cit. 2017-01-16]. Dostupné z: http://ww1.jeppesen.com/aviation/products/mobile-flitedeck/index.jsp
43. Operational Approvals - Less Paper Cockpit. *Adcs-aviation* [online]. 2017. [cit. 2015-01-16]. Dostupné z: http://www.adcs-aviation.com/en/operational-approval-detail/operational-approval/11-less-paper-cockpit.cfm

44. Mobile/Tablet Operating System Market Share.Realtime Web Analytics. *Netmarketshare* [online]. 2015 [cit. 2015-08-20]. Dostupné z: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1&qpsp=198&qpnp=1&qptimeframe=M
45. DOLEŽAL, Jakub. Mobilní platformy: historie a současnost. *Operační systémy - Android, iOS*. [online]. 2014 [cit. 2015-05-20]. Dostupné z: http://www.svetmobilne.cz/mobilni-platformy-historie-a-soucasnost/1926-24
46. GSMArena. *Gsmarena* [online]. 2017. [cit. 2017-01-16]. Dostupné z: http://www.gsmarena.com
47. Refurbished iPad Air 2 Wi-Fi + Cellular 64GB - Space Gray. *Apple* [online]. 2017. [cit. 2017-01-16]. Dostupné z: http://www.apple.com/shop/product/FH2M2LL/A/refurbished-ipad-air-2-wi-fi-cellular-64gb-space-gray
48. Galaxy Tab S2 (9.7 LTE). *Samsung* [online]. 2017. [cit. 2017-01-16]. Dostupné z: http://www.samsung.com/cz/tablets/galaxy-tab-s2-9-7-t819/
49. GILLETTE, Felix, BRADY Diane a WINTER Caroline. The Rise and Fall of BlackBerry: An Oral History. Businessweek. *Bloomberg* [online]. 2013. [cit. 2015-05-20]. Dostupné z: http://www.bloomberg.com/bw/articles/2013-12-05/the-rise-and-fall-of-blackberry-an-oral-history
50. HAVRYLUK, Michal.Mobilní OS pro experty: workoholikova pevnost BlackBerry OS. *Telefony* [online]. 2010. [cit. 2015-05-20]. Dostupné z: http://mobil.idnes.cz/mobilni-os-pro-experty-workoholikova-pevnost-blackberry-os-prf-/telefony.aspx?c=A100628_223333_chytre-telefony_ham
51. BOTSYURKO, Ruslan.Quo vadis, BlackBerry? Analytický pohled na vývoj společnosti. BlackBerry a Android. *Smartmania* [online]. 2013. [cit. 2015-05-20]. Dostupné z: http://smartmania.cz/clanky/quo-vadis-blackberry-analyticky-pohled-na-vyvoj-spolecnosti-5762
52. KARÁSEK, Jakub. Recenze Windows 10 Mobile: Budoucnost je univerzální. *Smartmania* [online]. 2016. [cit. 2017-01-16]. Dostupné z: https://smartmania.cz/recenze-windows-10-mobile-microsoft-test-12777/

53. KARÁSEK, Jakub. Velká recenze Windows 10: Lepší než předchůdci? *Smartmania* [online]. 2015. [cit. 2017-01-25]. Dostupné z: https://smartmania.cz/recenze-windows-10-microsoft-test-11679/
54. Lenovo ThinkPad 10 10 64GB 3G 4G Black tablet. *Icecat* [online]. 2015. [cit. 2017-01-25]. Dostupné z: http://icecat.cz/en/p/lenovo/20e30012mc/tablet-ThinkPad+10-30407565.html
55. Tablety - ThinkPad. *Lenovo* [online]. 2015. [cit. 2017-01-25]. Dostupné z: http://shop.lenovo.com/cz/cs/tablets/thinkpad/thinkpad-10/
56. ČAMBALA, Lukáš. ThinkPad Tablet 10 s přídavnou klávesnicí: Ještě to chce pilovat. *Lenovoblog* [online]. 2015. [cit. 2017-01-25]. Dostupné z: http://www.lenovoblog.cz/2015/01/thinkpad-tablet-10-s-pridavnou-klavesnici-jeste-to-chce-pilovat.html
57. Lenovo ThinkPad Tablet 10 / Z3795 / 4 GB / 128 GB / 10.1" FHD IPS / DigitizerPen / 4G / MicroHDMI / USB / Win8.1 PRO. *Lenovoshop* [online]. [cit. 2017-01-25]. Dostupné z: http://www.lenovoshop.cz/lenovo-thinkpad-tablet-10-z3795-4-gb-128-gb-10-1-fhd-ips-digitizerpen-4g-microhdmi-usb-win8-1-pro_d570744.html
58. Alza. *Alza.cz* [online]. 1994 - 2017. [cit. 2016-12-17]. Dostupné z: http://www.alza.cz
59. Mobilní bezpečnost. *ICT Bezpečnost* [online]. 2015. [cit. 2015-05-20]. Dostupné z: http://www.sefira.cz/mobilni-bezpecnost
60. Nové hrozby pro Android. *Mobily* [online]. 2013 [cit. 2015-05-20]. Dostupné z: http://www.mobilmania.cz/nove-hrozby-pro-android/a-1326764/default.aspx#utm_medium=selfpromo&utm_source=mobilmania&utm_campaign=copylink
61. PALYZA, Jiří. Aktuální informace o elektronické bezpečnosti. IDC Enterprise Mobility. 2014. Prezentace.
62. ŘEHÁČEK, David. Zabezpečení mobilních zařízení. *IT Security* [online]. 2009. [cit. 2015-05-20]. Dostupné z: http://www.systemonline.cz/it-security/mobilni-zarizeni-celi-novym-bezpecnostnim-hrozbam.htm

63. LIPPERT, Thomas. Jak zabezpečit mobilní zařízení ve firmách. *Hardware* [online]. 2012. [cit. 2015-05-20]. Dostupné z: http://channelworld.cz/hardware/jak-zabezpecit-mobilni-zarizeni-ve-firmach-7676
64. KILIÁN, Karel. Je na Androidu potřeba antivirový program?. *Svět androida* [online]. 2014. [cit. 2015-05-20]. Dostupné z: http://www.svetandroida.cz/android-antivir-201408
65. iTunes Preview. *Apple* [online]. 2014. [cit. 2017-02-06]. Dostupné z: https://itunes.apple.com/us/genre/ios/id36?mt=8
66. Správa mobilních zařízení od AirWatch. *Airwatch* [online]. 2017. [cit. 2017-02-06]. Dostupné z: http://www.air-watch.com/cz/reseni/sprava-mobilnich-zarizeni
67. Přineste si vlastní zařízení BYOD. *Airwatch* [online]. 2017. [cit. 2017-02-06]. Dostupné z: http://www.air-watch.com/cz/reseni/prineste-si-vlastni-zarizeni-byod
68. Správa pracovního prostředí od AirWatch. *Airwatch* [online]. 2017. [cit. 2017-02-06]. Dostupné z: http://www.air-watch.com/cz/reseni/kontejnerizace-pracovni-prostredi
69. Správa mobilního obsahu. *Airwatch* [online]. 2017. [cit. 2017-02-06]. Dostupné z: http://www.air-watch.com/cz/reseni/sprava-mobilniho-obsahu
70. Správa prohlížení od AirWatch. *Airwatch* [online]. 2017. [cit. 2017-02-06]. Dostupné z: http://www.air-watch.com/cz/reseni/sprava-prohlizeni
71. Správa mobilních aplikací. *Airwatch* [online]. 2017. [cit. 2017-02-06]. Dostupné z: http://www.air-watch.com/cz/reseni/sprava-mobilnich-aplikaci
72. Enterprise Mobility Management Platform. *Mobileiron* [online]. 2017. [cit. 2017-02-06]. Dostupné z: ttps://www.mobileiron.com/en/emm-platform
73. MobileIron Client - MDM Application for Enterprise Environments. *Mobileiron* [online]. 2017. [cit. 2017-02-06]. Dostupné z: https://www.mobileiron.com/en/products/platform-architecture/mobileiron-client
74. Mobileiron platform architecture. *Mobileiron* [online]. 2016. [cit. 2015-05-20]. Dostupné z: https://www.mobileiron.com/sites/default/files/products/mobileiron-platform-architecture-2016.png
75. App Wrapping and Containerization by AppConnect. *Mobileiron* [online]. 2017. [cit. 2017-02-06]. Dostupné z: https://www.mobileiron.com/en/products/appconnect

76. Mobile Document Management with Docs@Work. *Mobileiron* [online]. 2017. [cit. 2017-02-06]. Dostupné z: https://www.mobileiron.com/en/products/product-overview/docswork
77. Web@Work - A Mobile Data Security Solution. *Mobileiron* [online]. 2017. [cit. 2017-02-18]. Dostupné z: https://www.mobileiron.com/en/products/webwork
78. Securing Mobile Applications with Apps@Work. *Mobileiron* [online]. 2017. [cit. 2017-02-18]. Dostupné z: https://www.mobileiron.com/en/products/appswork
79. Help@Work. *Mobileiron* [online]. 2017. [cit. 2017-02-18]. Dostupné z: https://www.mobileiron.com/en/products/helpwork
80. Multi-OS App VPN. *Mobileiron* [online]. 2017. [cit. 2017-02-18]. Dostupné z: https://www.mobileiron.com/en/products/tunnel
81. Secure enterprise-class email with Email+. *Mobileiron* [online]. 2017. [cit. 2017-02-18]. Dostupné z: https://www.mobileiron.com/en/products/products-overview/email-plus
82. IBM.MaaS360. *Hubspot* [online]. 2016. [cit. 2017-02-18]. Dostupné z: https://cdn2.hubspot.net/hubfs/478588/ds_maas360_mdm_emm_June16.pdf?t=1472171913033
83. MILES, Darryl. Ten things you might not know about IBM MaaS360. *Wordpress* [online]. 2016. [cit. 2017-02-18]. Dostupné z: https://darrylmiles.wordpress.com/2016/02/23/ten-things-you-might-not-know-about-ibm-maas360/
84. iOS Supervised Mode. *Hexnode* [online]. [cit. 2017-02-18]. Dostupné z: https://www.hexnode.com/mobile-device-management/ios-supervised-mode/
85. Get started with a supervised iPhone, iPad, or iPod touch. *Apple* [online]. 2017. [cit. 2017-02-20]. Dostupné z: https://support.apple.com/en-us/HT202837
86. MobileIron and iOS:The Security Backbone for the Modern Enterprise. *Mobileiron* [online]. 2017. [cit. 2017-02-20]. Dostupné z: https://www.mobileiron.com/sites/default/files/whitepapers/files/iOS-security-backbone_EN_US_1.0.pdf
87. BAYTON, Jason. What is iOS Supervision and why is it used? *Bayton* [online]. 2017. [cit. 2017-02-20]. Dostupné z: https://bayton.org/2017/02/what-is-ios-supervision-and-why-is-it-used/

88. Device Enrollment Program Frequently Asked Questions. *Apple* [online]. 2016. [cit. 2017-02-20]. Dostupné z: https://support.apple.com/en-us/HT204142
89. Apple Deployment Programs Device Enrollment Program Guide. *Apple* [online]. 2016 [cit. 2017-02-20]. Dostupné z: http://images.apple.com/business/docs/DEP_Guide.pdf
90. Corporate-owned deployments made simple. *Apple* [online]. 2017. [cit. 2017-02-27]. Dostupné z: http://www.apple.com/business/dep/
91. Apple Configurator. *Techtarget* [online]. 2012. [cit. 2017-02-27]. Dostupné z: http://searchmobilecomputing.techtarget.com/definition/Apple-Configurator
92. Apple Configurator 2. *Apple* [online]. 2016. [cit. 2017-02-27]. Dostupné z: https://itunes.apple.com/us/app/apple-configurator-2/id1037126344?mt=12
93. Apple Deployment Programs Volume Purchase Program Guide. *Apple* [online]. 2016. [cit. 2017-02-27]. Dostupné z: http://images.apple.com/business/docs/VPP_Business_Guide.pdf
94. Volume Purchase Program for Business. *Apple* [online]. 2017. [cit. 2017-02-27]. Dostupné z: http://www.apple.com/business/vpp/
95. View or Configure Exchange ActiveSync Mailbox Policy Properties. *Microsoft* [online]. 2011. [cit. 2017-02-27]. Dostupné z: https://technet.microsoft.com/en-us/library/bb123994(v=exchg.141).aspx
96. VIOLINO, Bob. Compared: We have the goods on 11 top vendors, in 10 different features categories. *Computerworld* [online]. 2016. [cit. 2017-03-02]. Dostupné z: http://www.computerworld.com/article/3087435/mobile-wireless/mobile-management-vendors-compared.html?nsdr=true&page=2
97. What is the difference between the standalone and integrated Sentry? *Mobileiron* [online]. 2017. [cit. 2017-03-02]. Dostupné z: https://www.mobileiron.com/en/resources/faq#dif-standalone-integrated-sentry
98. Appliance Technical Specifications. *Infinigate* [online]. 2013. [cit. 2017-03-02]. Dostupné z: http://www.infinigate.de/fileadmin/user_upload/Products/MobileIron/Products/MobileIronApplianceTechnicalSpecification571.pdf

99. MobileIron architecture. *Managenet* [online]. [cit. 2017-03-02]. Dostupné z: https://www.managenet.com.au/upload/files/MobileIron%20architecture%20small.png
100. Mobile Device Management. *Managenet* [online]. [cit. 2017-03-02]. Dostupné z: https://www.managenet.com.au/solutions/mobile_device_management
101. MobileIron Mobile@Work™ Client. *Knicket* [online]. [cit. 2017-03-02]. Dostupné z: http://en.knicket.com/iphone/mobileiron-mobile-work-client/a17u7
102. LI, Richard, MobileIron VSP/Sentry + Office 365. *Wireless-richard.blogspo* [online]. 2013. [cit. 2017-03-02]. Dostupné z: http://wireless-richard.blogspot.cz/2013/03/mobileiron-vspsentry-office-365.html
103. Šifrované zálohy v iTunes. *Apple* [online]. 2016. [cit. 2017-03-12]. Dostupné z: https://support.apple.com/cs-cz/HT205220
104. MobileIron MarketPlace. *Mobileiron* [online]. [cit. 2017-03-12]. Dostupné z: https://marketplace.mobileiron.com
105. MobileIron Docs@Work. *Apple* [online]. 2016. [cit. 2017-03-12]. Dostupné z: https://itunes.apple.com/us/app/mobileiron-docs-work/id909492889?mt=8#
106. File Sync & Share. *Mobileiron* [online]. [cit. 2017-03-12]. Dostupné z: https://marketplace.mobileiron.com/asb_home_clone?filter=ct%3DFile+Sync+%26+Share
107. MobileIron Pricing and Packaging. *Mobileiron* [online]. 2017. [cit. 2017-03-12]. Dostupné z: https://www.mobileiron.com/en/products/pricing-and-packaging
108. CHASE, Benjamin. How To Use MobileIron Assemble. *Chaseoriginal* [online]. 2014. [cit. 2017-03-12]. Dostupné z: http://www.chaseoriginal.com/techcell/technotes/how-to-use-mobileiron-assemble/

Přílohy

Příloha č. 1 - Vybrané části porovnání EMM platforem

Možnosti nasazení

	AirWatch/ VMware	Blackberry	Citrix	IBM	Landesk	Microsoft	MobileIron	SAP	Sophos	Soti	Symantec
Product Name(s)	VMware AirWatch Enterprise Mobility Management	BES12	Citrix XenMobile	IBM MaaS360	Landesk Management Suite and Mobile Security Suite 2016 + Wavelink Avalanche 6.1	Enterprise Mobility Suite (includes Microsoft Intune, Azure Active Directory Premium, Azure RMS, and Advanced Threat Analytics)	MobileIron	SAP Mobile Secure - Enterprise Mobility Management	Sophos Mobile Control	MobiControl	Symantec Mobility: Suite
On premises	Yes	Yes	Yes	Yes	Yes	Yes, integrated solution: Microsoft Intune and System Center Configuration Manager	Yes	Yes and support for Hybrid environments	Yes	Yes	Yes
Cloud/SaaS	Yes	Yes	Yes	Yes	Yes (Landesk Mobile Security Suite 2016 + Wavelink Avalanche 6.1)	Yes	Yes				

MDM

	AirWatch/ VMware	Blackberry	Citrix	IBM	Landesk	Microsoft	MobileIron	SAP	Sophos	Soti	Symantec
Product Name(s)	VMware AirWatch Mobile Device Management	BES12	Citrix XenMobile	IBM MaaS360	Landesk Management Suite 2016 + Landesk Mobile Security Suite 2016 + Wavelink Avalanche 6.1	Enterprise Mobility Suite	MobileIron	SAP Mobile Device Management _ Mobile Device Management	Sophos Mobile Control	MobiControl	Symantec Mobility: Device Management
Password protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password reset	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote device wipe	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Selective wipe	Yes	Yes, work data	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote lock	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Set VPN, Wi-Fi, APN, proxy/ gateway settings	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Disable Wi-Fi	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes (only for Samsung)
Disable carrier data connection	Yes	Yes	Yes (while roaming on iOS, base policy KNOX etc.)	Yes	Yes	Yes (Roaming)	Yes	Yes	Yes, for Samsung SAFE, LG Gate, Sony; iOS and WinMobile restrict data	Yes	Yes (for iOS, Samsung)

COMPUTERWORLD

MAM

	AirWatch/ VMware	Blackberry	Citrix	IBM	Landesk	Microsoft	MobileIron	SAP	Sophos	Soti	Symantec
Product Name(s)	VMware AirWatch Mobile Device Management	BES12	Citrix XenMobile	IBM MaaS360	Landesk Management Suite 2016 + Landesk Mobile Security Suite 2016 + Wavelink Avalanche 6.1	Enterprise Mobility Suite	MobileIron	SAP Mobile Device Management _ Mobile Device Management	Sophos Mobile Control	MobiControl	Symantec Mobility: Device Management
Password protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password reset	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote device wipe	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Selective wipe	Yes	Yes, work data	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote lock	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Set VPN, Wi-Fi, APN, proxy/ gateway settings	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Disable Wi-Fi	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes (only for Samsung)
Disable carrier data connection	Yes	Yes	Yes (while roaming on iOS, base policy KNOX etc.)	Yes	Yes	Yes (Roaming)	Yes	Yes	Yes, for Samsung SAFE, LG Gate, Sony; iOS and WinMobile restrict data	Yes	Yes (for iOS, Samsung)

COMPUTERWORLD

MCM

	AirWatch/ VMware	Blackberry	Citrix	IBM	Landesk	Microsoft	MobileIron	SAP	Sophos	Soti	Symantec
Product name(s)	VMware AirWatch Enterprise Mobility Management	BES12	Citrix XenMobile	IBM MaaS360	Landesk Management Suite 2016 + Landesk Mobile Security Suite 2016	Enterprise Mobility Suite	MobileIron	SAP Mobile Secure; SAP Mobile App Protection _ Mobile App Wrapping for App Security; SAP Mobile Platform Mobile SDK	Sophos Mobile Control	MobiControl	"Symantec Mobility: Threat Protection, Symantec Mobility: Workforce Apps (Secure Mail, Secure Web)"
Encrypted document container	Yes	Yes	Yes	Yes	Yes	Yes	MobileIron	Yes	Yes	Yes	Yes (for iOS)
Secure email	Yes	Yes, via Good	Yes	Yes	Yes	Yes (Outlook)	Yes	Yes via iOS OS API and Android for Work. Also can deploy and manage 3rd party email from Symantec, Microsoft Outlook	Yes	Yes, via partner	Yes
File server access	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No
SecureSharePoint access	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Integates with enteprise document management software	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes

COMPUTERWORLD

Celé srovnání je dostupné na webu Computerworld. Zdroj: [96]