České vysoké učení technické v Praze
Fakulta elektrotechnická

Katedra ekonomiky, manažerství a humanitních věd

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **Musil** Martin

Studijní program: Softwarové technologie a management
Obor: Manažerská informatika

Název tématu:

Možnosti využití vlastních zařízení ve firemním prostředí (BYOD)

Pokyny pro vypracování:
1. Definice BYOD
2. Parametry BYOD
3. Možnosti využití ve společnostech
4. Představení dostupného softwaru na trhu
5. Případová studie využití BYOD pro ukázkového zákazníka

Seznam odborné literatury:
1. Schlager R.: Overview of Mobile Device Management Systems: Vendors, Solutions, Services, Partners. CreateSpace Independent Publishing Platform, 2012.
2. Johnson M.: Mobile Device Management: What you Need to Know For It Operations Management. Tebbo, 2011.

Vedoucí bakalářské práce: Ing. Pavel Náplava

Platnost zadání: do konce zimního semestru 2015/2016

V Praze dne 1.9..2014

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra ekonomiky, manažerství a humanitních věd

BYOD

Možnosti využití vlastních zařízení ve firemním prostředí

BYOD

Bring your own device

Bakalářská práce

Studijní program: Softwarové technologie a management

Studijní obor: Manažerská informatika

Vedoucí práce: Ing. Pavel Náplava

Martin Musil

Praha 2014

Prohlášení

„Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací“.

V Praze dne . . . . . .

. . . . . .

Podpis autora práce

Poděkování

Rád bych poděkoval hlavně vedoucímu Ing. Pavlu Náplavovi za rady, se kterými mi pomohl vytvořit tuto práci a za nemalý čas, který mi věnoval. Dále bych rád poděkoval rodičům, kteří mě podporovali po celou dobu studia.

Abstrakt

CZ

Cílem této práce je analyzovat problematiku trendu BYOD. V teoretické části jsou uvedeny základní informace o tomto trendu a jeho následné využití. V další části je představen dostupný software. V závěrečné části ukazuji na praktickém příkladu aspekty využívání BYOD.

Klíčová slova

BYOD, MDM, Bring your own device, mobile device management, správa mobilních zařízení

EN

The aim of this work is to analyse the issues of BYOD trend. Basic information about this trend and its subsequent use is listed in theoretical part. Available software is introduced in the next section. In the final part I show aspects of using BYOD on practical example.

Keywords

BYOD, MDM, Bring your own device, mobile device management

Obsah

1 Úvod

V poslední době, v rozmezí několika let, zažívá mobilní průmysl výrazné změny. Mobilní telefony přestaly sloužit pouze k hovorové a textové komunikaci. Staly se z nich víceúčelová zařízení, dnes známé jako chytré telefony, které začaly efektivně plnit funkci zdroje informací. Není proto žádné překvapení, že se začaly využívat ve společnostech pro pracovní účely.

Chytrý telefon, a později i tablet, začalo vlastnit více uživatelů, a tak docházelo k nápadům, využít zaměstnancovo soukromé zařízení pro firemní účely. Tomuto směru využití zařízení se začalo říkat BYOD (Bring your own device). Využívání BYOD ve společnosti sebou přináší různá rizika, kterým je třeba se věnovat. To je jeden z hlavních důvodů, proč jsem si téma BYOD vybral.

Cílem mé práce je analyzovat problematiku BYOD, následně ukázat na praktickém příkladu aspekty zavedení BYOD do společností.

Práce je rozdělená do pěti částí: Základní informace, Klíčové výhody a nevýhody BYOD, Aplikace podporující BYOD, Využití BYOD ve firemním prostředí, Případová studie využití BYOD pro ukázkového zákazníka.

V úvodní části definuji, co je to BYOD, uvedu první využití ve větší společnosti a popíši možné důvody, které vedly k tomuto trendu.

Ve druhé části uvedu hlavní výhody a nevýhody využití BYOD.

Další kapitola se zaměří na aplikace pro správu zařízení, které svými vlastnostmi umožňují lepší nasazení BYOD. Ukáži různé produkty, které v závěru kapitoly porovnám.

Následně uvedu základní kroky pro úspěšné zavedení BYOD do společnosti, vhodné nástroje pro mobilní zařízení. Vytvořím scénáře, které při zavedení BYOD nastanou.

Nakonec vytvořím fiktivní společnost, která bude mít požadavek na bezpečné zavedení trendu BYOD.

2 Základní informace

Tato kapitola obsahuje informace o tom, co je to BYOD, jeho první užití v praxi a využívání přenosných zařízení bez užití BYOD.

2.1 Definice

"Bring your own device" v překladu: "přines si svoje zařízení". Je rostoucí trend zaměřující se na zařízení zaměstnance používaných ve firemní sféře. Tato zařízení jsou například: chytré telefony, notebooky, PDA, tablety. Používá se taky u studentů, kteří si místo školních zařízení nosí a používají vlastní. [1]

Existují také termíny:

- BYOT - Bring your own technology
- BYOP - Bring your own phone
- BYOPC - Bring your own PC

Je možné se setkat s dalšími termíny začínající na BYO, všechny mají společnou myšlenku "osobní zařízení ve společnosti".

2.2 První užití v praxi

V roce 2009, kdy se většina společností z bezpečnostních důvodů snažily zakázat připojování k firemní síti s osobním zařízením, se vedení firmy Intel rozhodlo pro pravý opak a zaměstnancům umožnilo užívání soukromých zařízení pro pracovní účely. Ukázalo se, že to byl velmi populární krok, neboť v roce 2010 se počet vývojářů, kteří používali svá vlastní zařízení ve společnosti Intel, ztrojnásobil z 10 000 na 30 000 a odhaduje se, že v roce 2014 jich bude dokonce 70% z 80 000 zaměstnanců.[2]

Nicméně až do roku 2011 se nejednalo o nic extra zásadního, dokud se o tento trend nezačali zajímat dodavatelé softwaru VMware a Citrix Systems, kteří ho začali podporovat svými produkty.

Ne všude se ale tento trend setkal s kladnou odezvou. V roce 2012 v USA Equal Employment Opportunity Commission (EEOC) nabídla možnost zaměstnancům používat svá mobilní zařízení, ale velká část tuto nabídku odmítla. Hlavní důvody byly následující:

---

[1] http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html

[2] http://www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264

- Zaměstnanci chtěli mít oddělený soukromý život od pracovního, a tento krok by jím to narušoval.
- Neměli soukromý chytrý telefon.
- Obavy ze zvýšení měsíčních nákladů s užíváním svého telefonu v práci.[3]

2.3 Využívání přenosných zařízení před nástupem BYOD.

Když firmy začaly pořizovat pro své zaměstnance přenosná zařízení, jako například notebooky a mobilní telefony, byl to velký posun v před. Jednak se zaměstnanec mohl lépe připravit na svou práci, popřípadě mohl pracovat i z domova, ale na druhou stranu zařízení bylo stále ve vlastnictví firmy a dotyčný ho nemohl používat pro soukromé účely.

Ukažme si jednotlivé etapy na fiktivní firmě, která se snaží jít s dobou a je na trhu už dost dlouho, aby zažila několikrát změny ve využívání nových technologiích.

2.3.1 Práce na stolním PC

Když firma nakoupila stolní počítače pro zaměstnance, kteří je mohli využívat k běžným pracím například k tvorbě dokumentů, řízení účetnictví a podobně. Mohl se zaměstnanec přihlašovat do firemní sítě přes pracovní počítač a nenastal problém s narušením bezpečnosti, tedy pokud byla firemní síť dobře chráněná a omezená.

Myslím si, že v tehdejší době zaměstnance ani nenapadlo nosit si počítač domů, jestliže nebyl např. dlouhodobě nemocný a nemusel pracovat delší dobu z domova. Proto mnoho zaměstnanců pro tyto případy muselo mít počítače dva. A když potřebovali pracovat doma, třeba na nějakém projektu, museli mít samozřejmě potřebný software, což jsou další výdaje navíc.

Nevýhodou bylo také určité nepohodlí v neustálém stahování dat na přenosné zařízení nebo jejich posílání na mail, se kterými potřebovali pracovat mimo firmu. Neustálým opakováním tohoto procesu mohlo dojít k odrazení zaměstnance pracovat doma. A tímto zacházením se výrazně zvyšovalo riziko úniku interních dat.

Řešením je vytvořit virtuální privátní síť (VPN), přes kterou se domácí počítač připojí do firemní sítě. Výhodou pro zaměstnavatele je, že bude mít neustálou kontrolu nad tím, kdo a kdy se přihlašuje k síti. Nevýhodou byla nutnost připojení k internetu (v dnešní době už to není takový problém), zdlouhavé přidávání jednotlivých nových počítačů (zde záleží na nastavení bezpečnosti ve VPN).

[3] http://www.defensenews.com/article/20130107/DEFFEAT02/301070014/BlackBerry-Strategizes-More-U-S-Government-Clients

2.3.2 Práce na přenosném počítači

S příchodem notebooků do firmy pro zaměstnance se mohla zvýšit efektivita práce na počítači. Odpadl problém s přesouváním dat mezi nimi, vše bylo v jednom zařízení. Zaměstnanec mohl pracovat z domova, ale i u zákazníka. Rozměry notebooku byly na některé úkony zbytečně velké. Pokud potřeboval získat rychle určité informace, otevřel si v přenosném počítači dokument a našel, co hledal.

Avšak pro zaměstnavatele zde bylo stále relativně vysoké riziko ztráty dat případným odcizením notebooku a tím i zvýšenými náklady, pokud je nechtěl vymáhat po zaměstnanci. Navíc vznikal další problém, pracovník mohl notebook připojovat do jiných než firemních sítí, v nichž mohl zanést do počítače malware, později do dalších počítačů ve firemní síti. A i když se zaměstnanec zaváže, že nebude používat firemní zařízení na jiné věci, nemusel to dodržet.

Pracování na počítačích bylo čím dál tím častější a delší, proto některým zaměstnancům mohl začít vadit firemní notebook, pokud mu nevyhovoval (rozložení klávesnice, výkon, velikost displeje) a chtěl si pořídit svůj vlastní. Zde se však skoro vrací k původnímu nedostatku se stolními počítači (přesouvání dat, připojování do VPN dalším počítačem) a potom ztrácelo často smysl pořizování firemního notebooku.

Řešením je nechat zaměstnance vybrat si zařízení podle jeho výběru, které musí splňovat důležité firemní požadavky. Náklady na výběr určitých strojů není malý a mnoho pracujících není ochotna připlatit na provoz firemního majetku.

2.3.3 Chytrá zařízení

Když zaměstnanci dostali chytré telefony. Dostavila se zaměstnancům výhoda větší mobility, nemuseli všude brát notebook, často jim právě stačil chytrý telefon. Zaměstnavateli jejich nakoupením vznikaly různé výhody, například pokud pracovník jezdil do terénu, mohl být pomocí chytrého telefonu kontrolován, kde se nachází. S diářem synchronizovaném v telefonu a počítači bylo snadnější nezapomenout na různé pracovní povinnosti. Tímto se dala zvyšovat efektivita práce v různých směrech.

Byl zde ale stejný problém pro zaměstnance, jako u jiných firemních zařízení. Pokud měl osobní a firemní chytrý telefon, tak při pravidelném využívání obou zařízení se často stávalo, že jeden telefon nevyhovoval nárokům zaměstnance. Většinou je to služební telefon, který byl vybrán tak, aby splňoval požadavky firmy - kompatibilita firemních aplikací, cena. Zaměstnanec však mívá větší požadavky na telefon, než firma - ovládání, výdrž baterie, výkon, velikost displeje,…

Časem se začínají používat cloudové úložiště, které pomáhají se sdílením dat nejen mezi vlastními počítači, ale i mezi jinými uživateli. Tím odpadává nepohodlná část s kopírová-

ním dat mezi zařízeními, protože všechno už je na internetu. Problém s cloudovým řešením je ten, že nikdy nemáte záruku toho, jestli náhodou nezneužijí vaše data, co se stane s daty, když firma starající se o cloud zkrachuje nebo jinak skončí.

Tam, kde nestačily chytré telefony a notebook byl pořád neprakticky velký, se nasadil tablet. Jeho přednosti oproti notebooku jsou v lehkosti a výdrži baterie. Chytrý telefon má příliš malý displej a na tabletu, který může mít velikost displeje i kolem deseti palců, se dá zvládnout víc věcí a hlavně rychleji. Tablet je proto vhodný zejména pro techniky, kteří jezdí k zákazníkům a potřebují různé manuály, pracovní schémata. Dále je vhodný pro čtení zpráv a smluv. To ocení například manažeři. Nevýhody jsou v psaní delších článků, je obtížné sepisovat smlouvu na tabletu, avšak i to se dá částečně vyřešit přídavnou klávesnicí, částečně proto, že je pořád malá a relativně nepohodlná.

Stále ale nebyl využit potenciál přenosných zařízení. Proč by měl mít zaměstnanec dva podobné přístroje, když mu stačí jeden? Možná i proto se v posledních letech rozmáhá BYOD. O tom, zda je to správný krok se nedá ještě s určitostí říct, neboť je to stále velmi mladý trend. Nicméně v další kapitole si ukážeme základní výhody a nevýhody, které pomohou při rozhodování.

3 Klíčové výhody a nevýhody BYOD

Zde jsou zobrazeny hlavní obecné výhody a nevýhody, které nastanou při zavedení BYOD do společnosti.

3.1 Výhody

Společnosti, které užívají BYOD, mohou mít několik výhod oproti konkurenci.

Zvýšení produktivity

Hlavní výhodou BYOD je zvýšení efektivity zaměstnance. Ten při využívání BYOD má větší mobilitu, tím šetří čas, tudíž i náklady. Společnost Intel ve své analýze z roku 2011 uvedla, že 17 tisíc zaměstnanců, kteří užívají své zařízení pro práci, ušetří téměř hodinu svého času denně.[4]

Placení nákladů

S BYOD si všechny (nebo většinu) nákladů spojené s hardwarem platí sám pracovník, neboť on sám chce pracovat s přístrojem, který mu vyhovuje. Zde však nastávají právní problémy viz. Kapitola 3.2 Nevýhody.

Může se zdát, že zaměstnancům tyto náklady budou vadit, avšak podle průzkumu: *Good Technology's 2nd Annual State of BYOD report* zhruba polovina společností využívající BYOD uvedlo, že zaměstnanci si platí všechny náklady, 24% společností dává stipendium na užívání nefiremních zařízení a 19% proplácí zaměstnavatel veškeré náklady, které jsou v souladu s pravidly firmy, viz Obr. 1. [5]

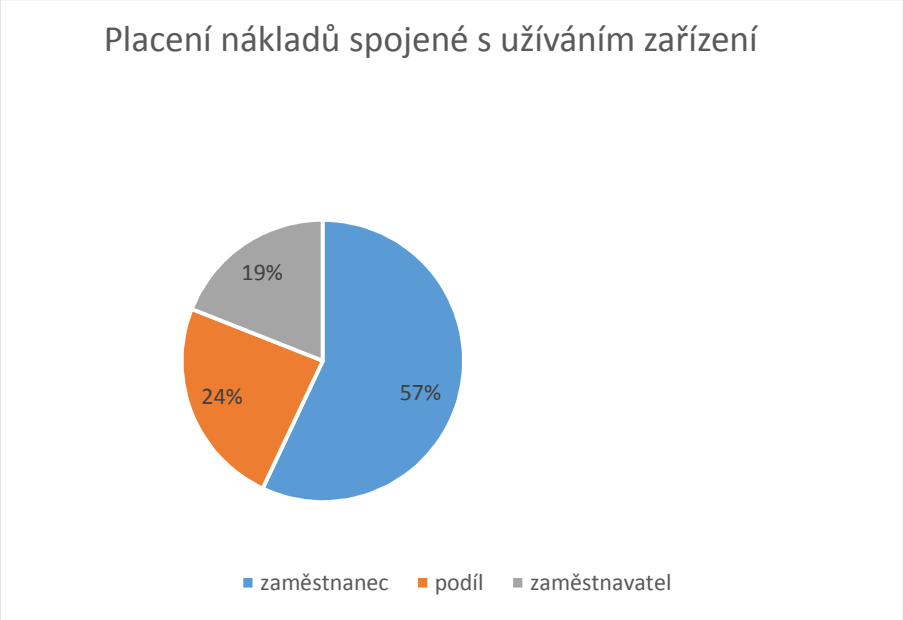
Lehčí inovace hardwaru

Uživatel si své zařízení pořizuje většinou častěji než společnost. Tím také firma čerpá z nově vynalezených funkcí pravidelněji. [6]

[4] http://www.forbes.com/sites/centurylink/2013/04/26/byod-employees-bring-their-own-efficiency-to-work/

[5] Good Technology http://media.www1.good.com/documents/Good-BYOD-Report-2013.pdf

[6] http://www.computerweekly.com/news/2240161202/Nearly-half-of-firms-supporting-BYOD-report-data-breaches

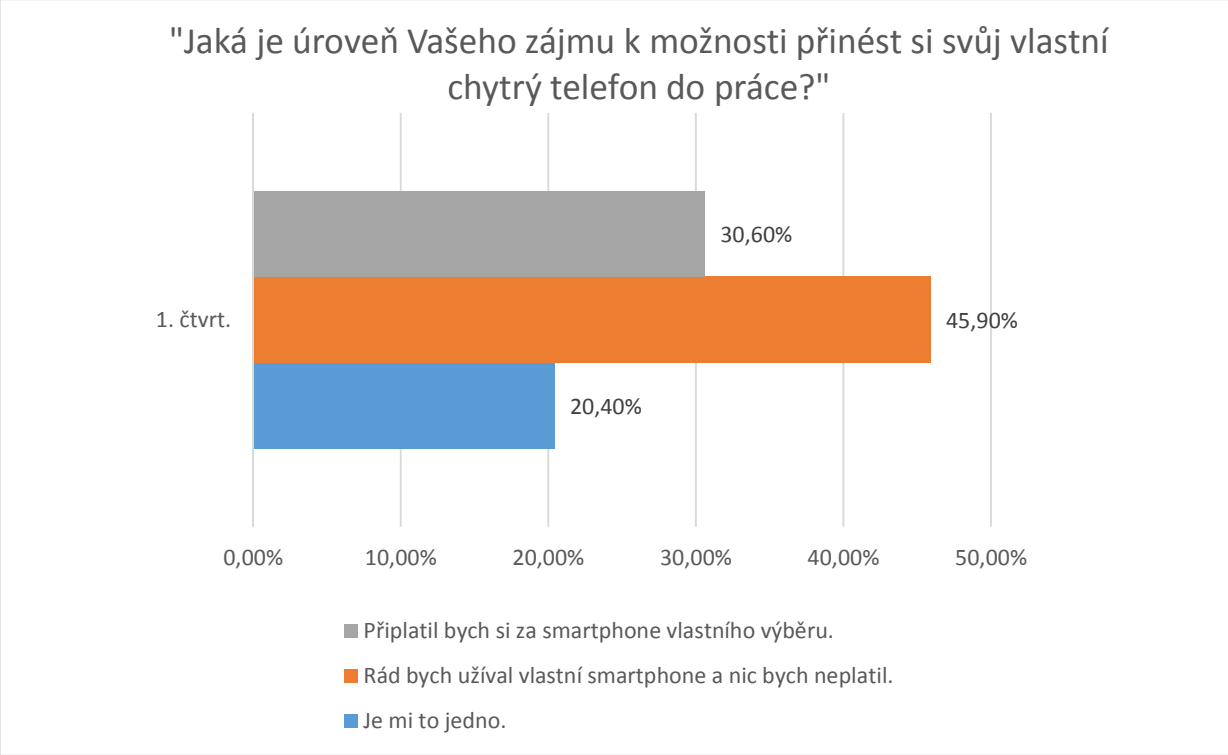


Obr. 1. Kdo platí náklady spojené s užíváním zařízení.

Spokojenost zaměstnance. Zaměstnanec si kupuje své přístroje tak, aby mu vyhovovaly. A je téměř jisté, že tato zařízení užívá raději než firemní, která musí často splňovat jen základní požadavky na funkčnost, nikoliv požadavky na užívání.

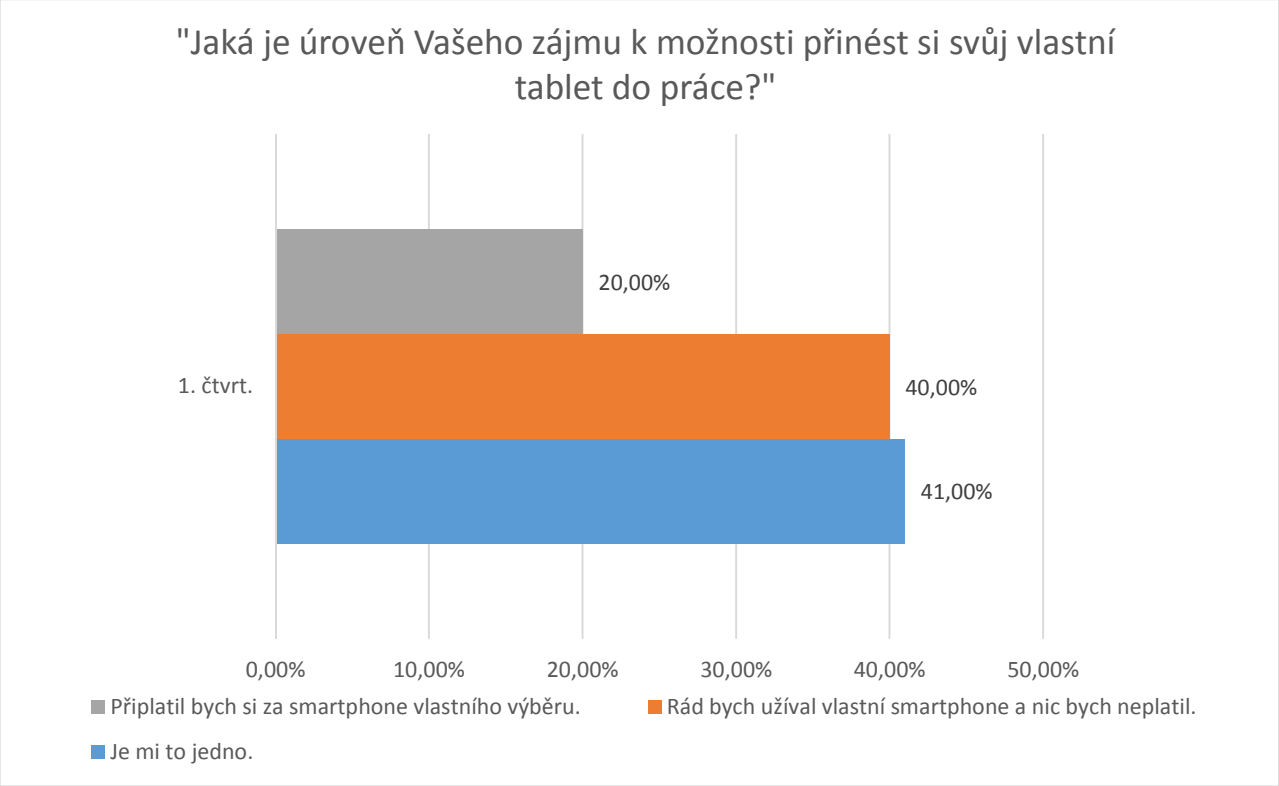
Podle průzkumu společnosti Forrester vydaným v únoru 2012, ve kterém se ptali zaměstnanců různých firem: "Jaká je úroveň Vašeho zájmu k možnosti přinést si svůj vlastní chytrý telefon do práce?" (Obr. 2) Na stejnou otázku, ale tentokrát ohledně tabletu (Obr. 3) byly rozdílné odpovědi. Předpokládám, že je to kvůli strachu o větší ztrátu soukromí, přeci jen tablet se dá využívat k více osobním věcem, které si zaměstnanec chce nechat pro sebe. Může to být ale i kvůli menšímu zájmu o tablet než o chytrý telefon. [7]

[7] http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf



Obr. 2. Zájem zaměstnanců užívání vlastního chytrého telefonu[8]

[8] 322 respondentů z firem mající 100 - 1 500 zaměstnanců



Obr. 3. Zájem zaměstnanců užívání vlastního tabletu[9]

3.2 Nevýhody

Při využívání BYOD programů v přístrojích musí společnosti zabývat určitými problémy.

Komplikovanější legislativa

Příspěvky zaměstnavatele na nákup zařízení užívané v práci jsou ze zákona povinné.

Otázka bezpečného užívání zařízení.

IT oddělení spravuje a aktualizuje bezpečnostní pokyny, kterými definují pravidla, jak mohou zaměstnanci využívat svá zařízení tak, aby neohrozili a nepoškodili společnost.

Podpora mnoha různých zařízení

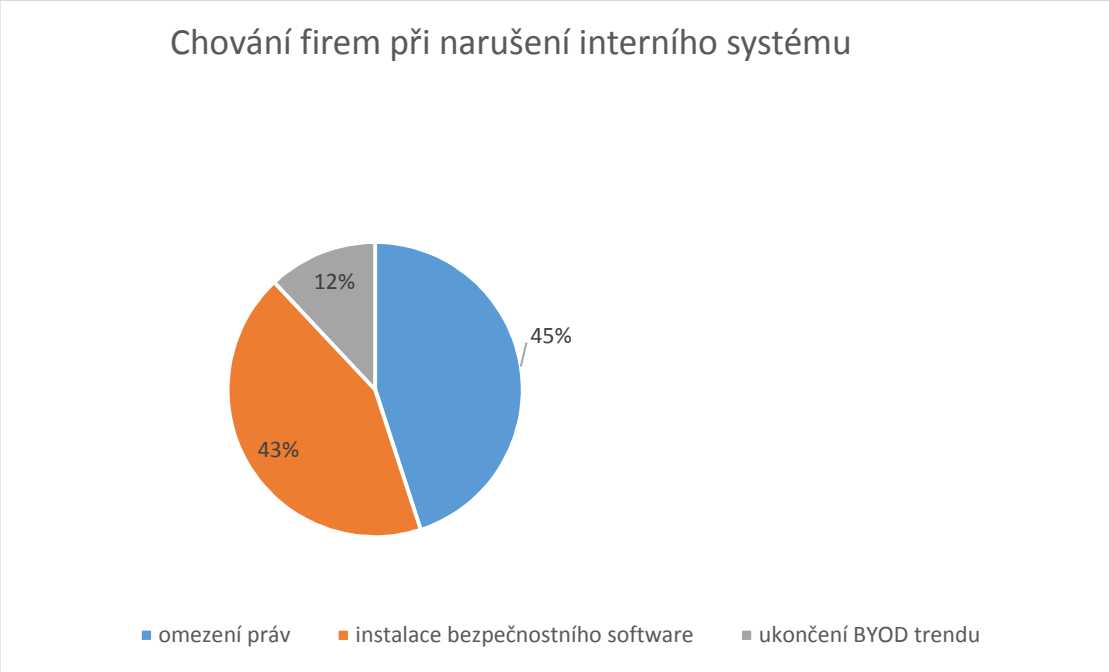
Pokud zaměstnanec bude mít možnost používat své zařízení, je zřejmé, že IT oddělení bude muset řešit problém s podporou odlišných zařízení a odlišných typů operačních systémů.

[9] 286 respondentů z firem mající 100 - 1 500 zaměstnanců

Narušení interních dat

Pokud se někdo cizí dostane k datům společnosti, myslím, že problém není v trendu BYOD, ale ve špatně nastavených podmínkách ve správě mobilních zařízení nebo že vůbec takový nástroj nepoužívají. [10]

Podle Decisive Analytics téměř polovina podniků, ve kterých je dovoleno pracovníkům připojovat se do vlastní sítě má zkušenosti s narušením dat. Nejčastěji společnost omezila přístupová práva (45%) nebo nainstalovala bezpečnostní software (43%). 12% podniků se rozhodlo skončit s politikou BYOD, viz Obr. 4.[11]



Obr. 4. Chování firem při narušení interního systému

[10] http://www.mbtmag.com/articles/2013/01/benefits-and-risks-byod

[11] http://www.computerweekly.com/news/2240161202/Nearly-half-of-firms-supporting-BYOD-report-data-breaches

4 Aplikace podporující BYOD

Jsou aplikace, které umožňují spravovat administrátorům zařízení uživatelů vzdáleně. Dokáží začlenit soukromá zařízení do firmy, následně administrátoři mohou kontrolovat jeho stav (míru zabezpečení, síťová připojení, přístup do systému), popřípadě může přinutit zaměstnance, aby změnil bezpečnostní pravidla. Konkrétně se zaměřím na aplikace pro správu mobilních zařízení.

4.1 Mobil device management (MDM)

Aplikace pro správu mobilních zařízení se anglicky nazývají Mobile Device Management (MDM).

4.1.1 Zaměření MDM aplikací

Některé funkce, které nabízejí MDM řešení, jsou v zařízení automaticky poskytovány. Například zjišťování polohy telefonu pomocí GPS, automatické připojování k Wi-Fi síti, pokud jsme v dosahu, automatické uzamknutí obrazovky. Avšak výhoda v MDM řešení je jeho komplexnost. Další služby, které mohou navíc MDM řešení poskytovat jsou zejména vzdálené zablokování zařízení, jejich sledování (polohy, nainstalovaných aplikací) a mimo jiné také vzdálené vymazání dat.

Správci potřebují mít kontrolu nad všemi zařízeními, které jsou přes daný software přihlášeny ve firemní síti. Všechna práce se zařízením a jeho správou musí probíhat zabezpečeně! Důležité pro BYOD je, aby MDM řešení podporovala široké spektrum operačních systémů mobilních zařízení. Všechny tyto vlastnosti musí mít aplikace pro podporu BYOD.

V začátcích BYOD se firmy musely rozhodnout, jaká chytrá zařízení budou smět zaměstnanci používat, protože podpora více druhů operačních systému byla nákladnější. Myslím si ale, že nyní firmy tvořící nástroje pro správu mobilních zařízení jsou konkurencí tlačeny tak, aby pokrývaly široké spektrum operačních systémů.

4.2 Druhy MDM produktů

Zde je uvedeno několik nejznámějších firem, které poskytují komplexní správu mobilních zařízení. Vybral jsem je z vyhledávání na internetu podle jejich popularity. Důvodem uvedení těchto produktů je, získání přehledu, co daná řešení nabízí. Vlastnosti aplikací jsem čerpal ze stránek výrobců.

Většina programů jsou placené, ale najdou se i aplikace, které jsou zdarma. Takové jsem našel dvě. Podrobněji se jim budu věnovat v páté kapitole, kde je využiju v případové studii. Nyní pouze porovnám jejich vlastnosti s ostatními placenými produkty.

4.2.1 Miradore[12]

První se nazývá Miradore, tato aplikace je jednoduchá na správu, bohužel má pouze základní funkce jako jsou například vzdálené uzamknutí telefonu, odstranění hesla (pouze pro iOS), resetovaní hesla, odstranění všech dat. Chybí například pokročilá správa aplikací, správce pouze zjistí, jaké aplikace jsou nainstalované v zařízení, ale instalovat nové aplikace nebo některé zakázat už nemůže.

4.2.2 WSO2[13]

Druhá aplikace se jmenuje WSO2 a oproti Miradore, podporuje správu aplikací. Správce může nastavit, které aplikace se mají nainstalovat, buď pro všechny, nebo jen pro vybranou skupinu zaměstnanců. Stejná možnost je i pro odinstalování programů, stačí jen vybrat aplikaci a zařízení, kterých se to má týkat. Jestliže bude chtít zakázat určitou aplikaci, může jí dát na seznam zakázaných aplikací a zaměstnanec si jí nebude moct nainstalovat. Na druhou stranu, pro zavedení do systému, je potřeba mít server, na kterém poběží.

4.2.3 MobileIron – MobileIron[14]

Vlastnosti aplikace

Podpora platforem

- Android, iOS, BlackBerry, Windows Phone 7/8, Windows Mobile, Symbian, Palm OS, Mac OS X, Windows

Konfigurace

- Vzdálená správa
- Nastavení přístupu na firemní sítě (Wi-Fi, VPN, bluetooth), mail, klientské certifikáty
- Centrální správa aplikací
- Samoobslužná správa zařízení

Zabezpečení

- Seznam povoleného a zakázaného software

[12] http://www.miradore.com/

[13] http://wso2.com/products/enterprise-mobility-manager/

[14] https://www.mobileiron.com

- emailový filtr
- vlastní síť

Sledování

- Aktuální stav
- Využívání služeb
- Automatické upozorňování na problémy uživatelských zařízení

4.2.4 AirWatch – AirWatch B2[15]

Vlastnosti aplikace

- Podpora platforem - Android, iOS, BlackBerry, Symbian, OS Windows, Windows Phone 7/8/, Windows Mobile, Mac OS X 10.7+

Konfigurace

- Nastavení přístupu na firemní sítě (Wi-Fi, VPN), email, klientské certifikáty
- Seznam povoleného a zakázaného software
- Vzdálená správa softwaru

Zabezpečení

- Vzdálené zamykání zařízení

Sledování

- Aktuální stav
- Využívání služeb
- Automatické upozorňování na problémy uživatelských zařízení

[15] http://www.air-watch.com

4.2.5 BlackBerry - Enterprise Service 10 [16]

Vlastnosti aplikace

- Podpora platforem - Android, iOS, BlackBerry, do budoucna OS Windows

Konfigurace

- Nastavení přístupu na firemní sítě (Wi-Fi, VPN), email, klientské certifikáty
- Zaměření na bezpečnou správu firemních dat
- Hromadná správa uživatelů a zařízení
- Vzdálená správa softwaru

Zabezpečení

- Vzdálená správa zařízení (mazání, zamykání)

4.2.6 Citrix - XenMobile[17]

Vlastnosti aplikace

- Podpora platforem - Android, iOS, BlackBerry, Windows Phone 7/8, Symbian

Konfigurace

- Hromadná správa uživatelů a zařízení
- Nastavení přístupu na firemní sítě (Wi-Fi, VPN), mail, klientské certifikáty
- Seznam povoleného a zakázaného software
- Centrální správa aplikací

Zabezpečení

- Vzdálená správa zařízení (mazání, zamykání)
- Omezení funkčnosti na určité státy
- Vymazání zařízení kompletní nebo selektivní

[16] http://us.blackberry.com/enterprise.html

[17] http://www.citrix.cz

- Identifikace nečinných zařízení

Support

- Možnost řešení problémů skupinově nebo jednotlivě

Sledování

- Pohyb zařízení
- Aktuální stav
- Využívání služeb
- Automatické upozorňování na problémy uživatelských zařízení

4.3 Porovnání vybraných produktů

Zde je shrnutí vybraných produktů. V tabulce č. 1 jsou podporované platformy a v tabulce č. 2 jsou funkce, které jednotlivé produkty poskytují.

Tabulka 1. Podpora platforem[18]

Prodejce	Airwatch B2	BlackBerry	Citrix	MobileIron	Miradore*	WSO2*
Jméno produktu	AirWatch Enterprise Mobility Management	BlackBerry Enterprise Service 10	XenMobile	MobileIron	Miradore Online	Enterprise Mobility Manager
iOS	Ano	Ano	Ano	Ano	Ano	Ano
Android	Ano	Ano	Ano	Ano	Ano	Ano
BlackBerry	Ano	Ano	Ano	Ano	Ne	Ne
Windows Mobile	Ano	Ne	Ano	Ano	Ne	Ne
Windows Phone 7	Ano	Ne	Ano	Ano	Ne	Ne
Windows Phone 8/8.1	Ano	Ne	Ano	Ano	Ano	Ne
Ostatní	Mac OS X 10.7+, Windows 8/RT			Mac OS X, OS Windows		

* Služby poskytované zdarma.

Citrix, Ariwatch a MobileIron podporuje všechny nejrozšířenější mobilní platformy[19], Miradore poskytuje podporu jen pro nejnovější platformy a BlackBerry s WSO2 podporují pouze iOS a Android.

[18] Částečně převzato z http://www.computerworld.com/article/2497055/mobile-device-management/mdm-tools-features-and-functions-compared.html

[19] http://www.sunmarketing.cz/mobilni-aplikace/informace-o-mobilnich-platformach

Tabulka 2. Porovnání MDM funkcí[20]

Prodejce	Airwatch B2	Blac-kBerry	Citrix	MobileI-ron	Miradore*	WSO2*
Jméno produktu	AirWatch Enterprise Mobility Ma-nagement	BlackBerry Enterprise Service 10	XenMobile	MobileIron	Miradore Online	Enterprise Mobility Manager
Ochrana heslem	Ano	Ano	Ano	Ano	Ano	Ano
Resetování hesla	Ano	Ano	Ano	Ano	Ano	Ano
Smazání zaří-zení	Ano	Ano	Ano	Ano	Ano	Ano
Výběrové ma-zání	Ano	Ano	Ano	Ano	Ne	Ano
Odstranění zámku	Ano	Ano	Ano	Ano	Ne	Ano
Nastavení VPN, Wi-Fi, APN, proxy/brány	Ano	VPN, Wi-Fi, proxy	Ano	Ano	Wi-Fi, VPN jen iOS	Ano
Zakázání Wi-Fi	Ano	BlackBerry	Ano	Ano	Ne	Ne
Zakázání mobil-ního přenosu dat	Jen roa-ming pro iOS	Ne	Ano	Ano	Jen roa-ming pro iOS	Ne
Sledování/repor-tování	Ano	Ne	Ano	Ano	Ano	Ano
Zakázání ka-mery	Ano	Ano	Ano	Ano	Ne	Ano
Zakázání Blue-tooth	Ano	BlackBerry	Ano	Ano	Ne	Ne
Správa připoje-ných zařízení (jako tiskárny, scannery)	Ano	Ne	Ano	Ne	Ne	Ne
Více uživatelů na jedno zaří-zení (podle aktu-álního přihlá-šení)	Ano	Ne	Ano	Ano	Ne	Ne

* Služby poskytované zdarma.

Z tabulky č.Tabulka 2 shrnující funkce pro jednotlivé produkty je vidět, že Airwatch B2 a Citrix obsahují nejvíce funkcí. MobileIron kromě správy připojených zařízení podporuje

[20] Částečně převzato z http://www.computerworld.com/article/2497055/mobile-device-management/mdm-tools-features-and-functions-compared.html

také vše. Z placených služeb dopadlo nejhůře řešení od BlackBerry a funkčně se podobá WSO2. Miradore poskytuje omezené množství funkcí.

5 Využití BYOD ve firemním prostředí

Pokud se společnost rozhodne používat BYOD, je potřeba se seznámit s dopady, které tato změna přinese, to je popsáno v následující podkapitole. Když už bude společnost informována o dopadech BYOD, může ho zavést do firmy. V podkapitole 6.1 si ukážeme zavedení dvou odlišných nástrojů pro správu mobilních zařízení do fiktivní společnosti, které porovnáme z hlediska času a financí.

5.1 Základní kroky pro úspěšné využívání BYOD

Pro užívání mobilních zařízení ve firmě, z pohledu zaměstnavatele, je potřeba se připravit na změnu. Musíme si uvědomit, že implementace BYOD, musí podpořit stávající chod firmy, zefektivnit její práci a pomoct dosáhnout jejích cílů. Systém je potřeba přizpůsobit firmě, ne firma systému.

5.1.1 Prvotní nastavení nového zařízení

Při připojení nového zařízení do společnosti je potřeba nainstalovat důležité aplikace, které firma používá, připojení firemních účtů, vložit bezpečnostní certifikáty a další…

5.1.2 Bezpečnostní prvky

Základní prvky zabezpečení musí být takové, aby se zařízení automaticky po chvíli uzamklo a nebylo přístupné pro cizí osoby, pokud zaměstnanec nechá své zařízení bez dozoru. Uzamknutí má být v podobě kvalitního hesla, které se pravidelně mění. Kvalitním heslem je míněno heslo, které je dostatečně dlouhé, skládá se z velkých a malých písmen a čísel. Pokud uživatel několikrát zadá špatně heslo, musí se obsah telefonu automaticky smazat. Zde si dovolím tvrdit, že kvalitní heslo a jeho častá pravidelná změna, snižuje bezpečnost dat, protože taková hesla si pracovník někam píše. Je to podobně jako s platební kartou a PIN kódem, který si někdo nechá v telefonu pod kontaktem „Karta“.

V zařízení je potřeba zašifrovat firemní data, jednak na vnitřní, tak na vyjímatelné paměti.

Důležité je také zaškolit uživatele zařízení v tom, co si mohou dovolit se zařízením a podat jim správné odůvodnění, aby našli pochopení pro daná omezení.

5.1.3 Vymazání dat

Pokud je se zaměstnancem ukončen pracovní poměr, je velmi důležité vymazat firemní data z telefonu. Což je vhodné provést vzdáleně. Existuje metoda tzv. "Selective wipe" (částečného/výběrového vymazání dat), kde se uživateli smažou pouze firemní data.[21]

[21] http://www.systemonline.cz/sprava-it/mobile-device-management.htm

5.1.4 Nutnost neustálého připojení k internetu

Aby uživatel posílal údaje o své aktivitě, je nutné, aby byl připojen k internetu. Pokud uživatel nebude připojen, všechny příkazy od serveru, změny, resety se neprovedou do doby, než se opět připojí. Když uživatel zapomene heslo a není připojen k internetu, heslo se mu nepřenastaví a máme zde problém jako bez MDM řešení a musíme uvést zařízení do továrního nastavení.

5.2 Vhodné nástroje pro mobilní zařízení

Ještě před využitím soukromých zařízení ve firemním prostředí zde uvedu prvky, které má mít každá společnost využívající přenosná zařízení.

5.2.1 Zabezpečení zařízení

Pokud firma pracuje na projektu, který ztrácí hodnotu při zveřejnění její myšlenky, např. nová aplikace, která ještě nikoho nenapadla, určitě je nanejvýš důležité, aby se k datům nikdo nedostal. Nejčastěji se tak může stát při odcizení přenosného zařízení, ale i infikováním malwarem při nešikovném používání zařízení, odposlouchávání sítě apod.

Šifrování dat

Abychom předešli možným problémům při odcizení nebo ztrátě zařízení, je dobré šifrovat data. V případě telefonu a operačním systému Android je šifrování již v systému a stačí jej jenom zapnout. Poté vždy, když bude telefon v nečinnosti, se může nastavit zamknutí obrazovky na heslo. Pokud se telefon připojí k počítači, nebude povolen přístup k datům, dokud se nezadá heslo do telefonu. V případě, že nepoužíváme operační systém Android, můžeme využít nějakou bezplatnou šifrovací aplikaci, jako příklad uvádím aplikaci „Secret Space Encryptor“[22], kde se dají šifrovat i jenom určité části. V základním nastavení, při zašifrování určité složky nebo souboru, se nesmažou dešifrované data. Doporučuji změnit nastavení.

Pro počítače pak můžeme použít programy jako Bitlocker[23], který je v lepších edicích systému Windows nebo můžeme použít například externí program TrueCrypt[24], se kterým je možné šifrovat jak celý disk, tak pouze vybraná data.

Musíme si uvědomit, že šifrování zpomaluje zařízení i několikanásobně, proto ne vždy je vhodné řešení zašifrovat kompletně celý disk a jeho další paměťové uložiště. [25]

---

[22] http://www.paranoiaworks.mobi/sse

[23] http://technet.microsoft.com/en-us/library/hh831713.aspx

[24] www.truecrypt.org

[25] Http://www.cnews.cz/sifrovani-v-androidu-nekolikanasobne-zpomaluje-zapis-i-cteni-z-interniho-uloziste

Správa hesel
Další důležitou zásadou je mít odlišná hesla k důležitým účtům, soborům a dalším… Pro lepší správu těchto hesel může sloužit program, který si hesla bude pamatovat, a vy si nebudete muset pamatovat příliš mnoho hesel. Největší riziko je, že si heslo někam zapíšeme, anebo nebude dostatečně silné. Je jasné, že mít hesla na jednom místě bezpečnost zrovna nezvyšuje, spíše naopak, bohužel není moc reálné, pamatovat si všechna hesla. Takových aplikací je nespočet, a pokud používáme pro šifrování program „Secret Space Encryptor“, pak nemusíme hledat další program.

Antivirový program nejen do PC
S chytrými zařízeními existuje riziko nakažením malwarem stejně jak do počítače, pokud chytrá zařízení budeme používat na důležité věci, určitě je vhodné ho nějak zabezpečit. Předejitím nebo minimalizováním šance na nakažení zařízení je především vyhýbat se pochybným stránkám, neotvírat neznámé přílohy, neinstalovat nedůvěryhodné aplikace. Pro větší jistotu doporučuji i antivirový program například „avast! Free Mobile Security“, ten navíc podporuje možnost *sledování zařízení*, což je opět vhodný prvek k zabezpečení, v případě odcizení telefonu či tabletu.

Pro počítače s operačním systémem Windows Vista a Windows 7 je možné používat nástroj Windows Security Essentials. Pro novější operační systémy Windows 8 a Windows 8.1 zas může použít nástroj Windows Defender. Bohužel tato služba nefunguje stoprocentně a tak jednou za čas je dobré použít i jiný nástroj. A jelikož se jedná o jednorázovou záležitost, doporučuji využití takzvaného online scanneru například od firmy ESET. [26]

5.2.2 Synchronizace dat a jejich záloha
Pro synchronizaci dat ať už jen mezi přístroji jednotlivce nebo celého kolektivu, je dobré použít některé z cloudových řešení. Opět uvedu příklad, nyní od Microsoftu OneDrive, kde je hned v základu prostor 15GB, díky různým bonusům však můžete dostat více místa na uložišti. Synchronizace prohlížečů je jednoduchá, stačí si vytvořit účet na prohlížeči a data se ukládá na cloudové uložiště výrobce prohlížeče. Pro připojení dalšího zařízení se pak stačí jenom přihlásit ke stávajícímu účtu a prohlížeče se po chvíli synchronizují.

Pokud používáme cloudové úložiště, z části může fungovat jako záloha dat, ale určitě je dobré zálohovat data i někam jinam, například na přenosný disk, či optická média. Tyto zálohy, pokud je to nutné, se mohou opět zašifrovat. Vhodným řešením je provádět zálohu na firemní server. V takové malé firmě může být server právě nějaké cloudové uložiště.[27]

---

[26] http://www.antivirovecentrum.cz/antiviry/srovnani.aspx

[27] http://www.zive.cz/clanky/nejlepsi-cloudova-uloziste-pro-vase-data/sc-3-a-174542/default.aspx

5.2.3 Kancelářské aplikace

Pro větší mobilitu při práci se vyplatí mít v zařízení software pro práci s dokumenty. Je potřeba také poštovní klient, který přijme tyto dokumenty, popřípadě někam odešle.

Kancelářský balík

Pro zobrazení PDF, textových, tabulkových nebo prezentačních souborů si vystačíme s integrovanou aplikací „OfficeSuite“ pokud chceme upravovat soubory (což se i v telefonu někdy hodí), musíme si zaplatit plnohodnotnou verzi OfficeSuite, nebo využít jiný program. „Kingsoft Office“ je zdarma a umí číst, vytvářet a upravovat soubory běžných typů.[28]

Pro počítače je nejznámější kancelářský balík Microsoft Office, ten však není zdarma a jeho alternativou je Open Office, který je open source a obsahuje textový editor, tabulkový procesor, prezentační nástroj, ale také i grafický nástroj pro vytváření databáze a matematických vzorců.[29]

Velice přínosné je využívání online kancelářských programů, které jsou vhodné pro sdílení. Populární službou je Google Docs[30].

Poštovní klient

E-maily je nezbytné mít pod dohledem a existuje mnoho dostupných prvků, které se starají o příchozí zprávy, interně je v Androidu zabudován, někomu ale nevyhovuje a požaduje jiného klienta například K-9 Mail.

V počítačích s Windows 8 a Windows 8.1 je interní poštovní klient, kterému stačí pouze jméno účtu a heslo z klasických emailových účtů jako je Gmail, Yahoo!, Seznam a pod… U méně známých poštovních serverů jsou potřeba dodatečné údaje (IMAP a SMTP server).[31]

5.3 Scénáře týkající se mobility zařízení

Využívání soukromých mobilních zařízení sebou přináší různé nové situace, které jsou zobrazeny v této kapitole. Využiju při tom volně dostupné MDM nástroje, konkrétně

---

[28] http://www.svetandroida.cz/ctenari-doporucuji-4-kancelarske-baliky-201205

[29] http://www.linuxexpres.cz/kancelar/srovnani-libreoffice-openoffice-org-a-microsoft-office

[30] https://docs.google.com/

[31] http://technet.idnes.cz/e-malovy-klient-zdarma-069-/software.aspx?c=A130310_133052_software_dvr

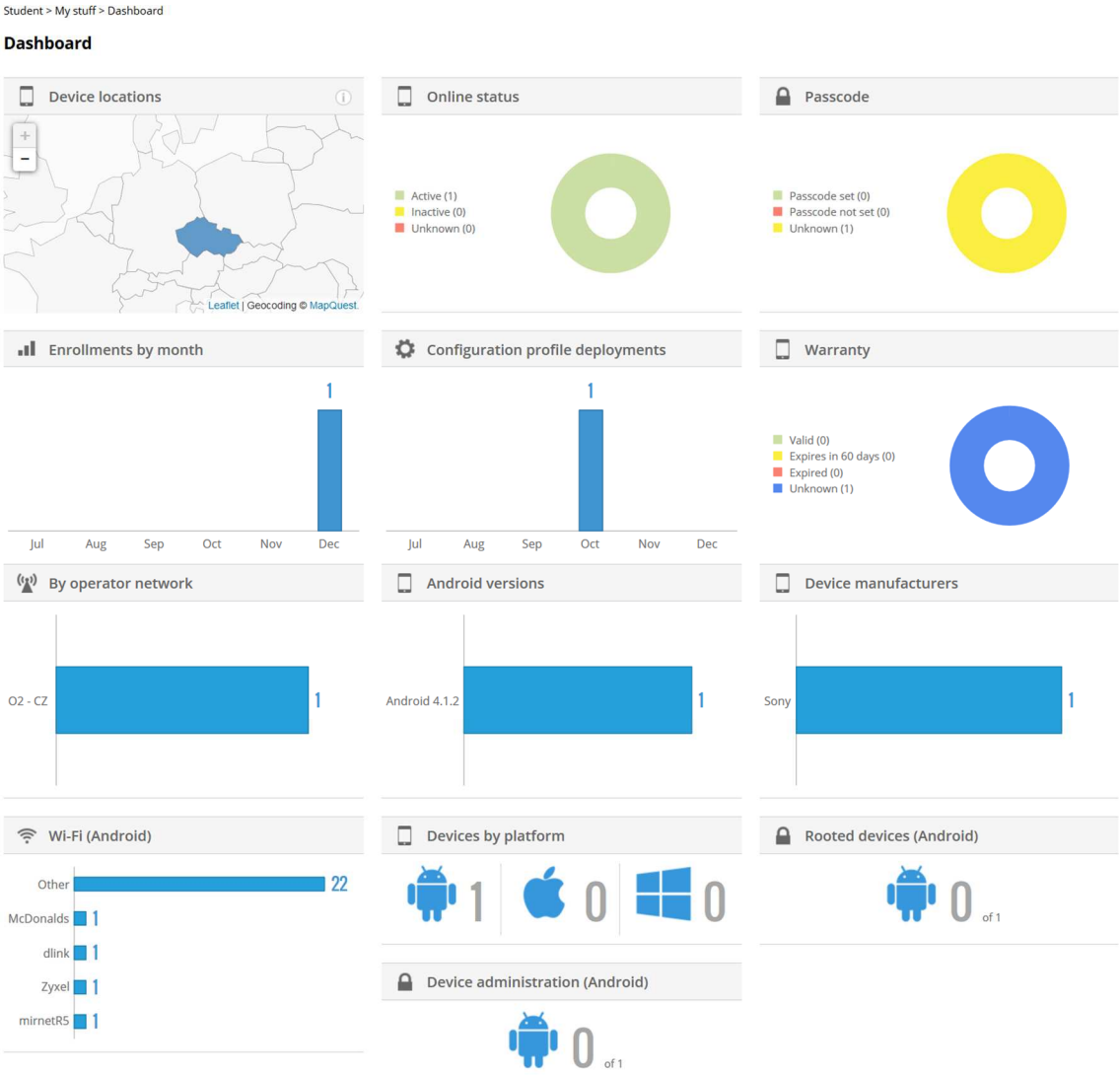
Miradore viz kapitola 4.2.1 a WSO2 z kapitoly 4.2.2. Dále v každém scénáři (mimo: zavedení MDM nástroje do podniku, nastavení serveru a aktualizace MDM) ukážu postup bez využití MDM řešení.

5.3.1 Zavedení MDM nástroje do podniku

Pokud se zaměstnavatel společnosti rozhodne použít MDM software, musí si vytvořit server, ať už vlastní nebo u výrobce MDM aplikace nebo u třetí osoby, záleží na konkrétním řešení. Zde ukážu postupy pro aplikaci Miradore a WSO2. Rozdíl v zavedení mezi nimi je ten, že Miradore běží na serveru poskytovatele softwaru. Pro WSO2 je potřeba zajistit server.

Miradore

Založení nového účtu u webové aplikace Miradore je velice lehké a rychlé. Stačí se zaregistrovat na stránkách výrobce (jméno, příjmení, email, tel číslo, název společnosti, heslo pro přihlášení). Poté se přihlašovat pomocí internetu na firemní účet. Po přihlášení se zobrazí úvodní obrazovka, viz Obr. 5.



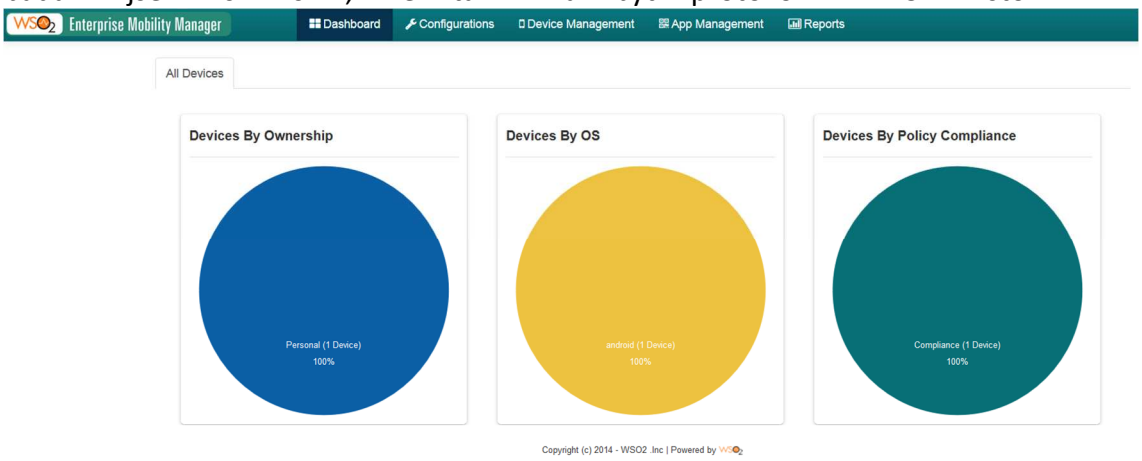
Obr. 5. Úvodní strana Miradore, zobrazující informace o zařízeních ve společnosti

WSO2

Zde se musí firma také registrovat u výrobce, poté se musí stáhnout archiv s aplikací. U této aplikace je potřeba, aby někde fungovala, tudíž je nutné si pronajmout server, nebo mít vlastní. Pro potřeby testování si vystačíme s aplikací pracující v lokální síti. Po stažení aplikace je potřeba mít ještě nainstalováno Oracle JDK 6*-7*, novější verze není podporována. Po instalaci JDK ještě nastavit systémové proměnné JAVA_HOME a CARBON_HOME. Poté se už může spustit samotný server. Nastavení serveru se provádí přes protokol https. Úvodní strana po přihlášení administrátora na Obr. 6.

Nastavení pomocí manuálu na stránkách výrobce bylo velice nepřehledné a mnoho informací jsem musel dohledat na internetu. Manuál byl sice veden krok za krokem, ale

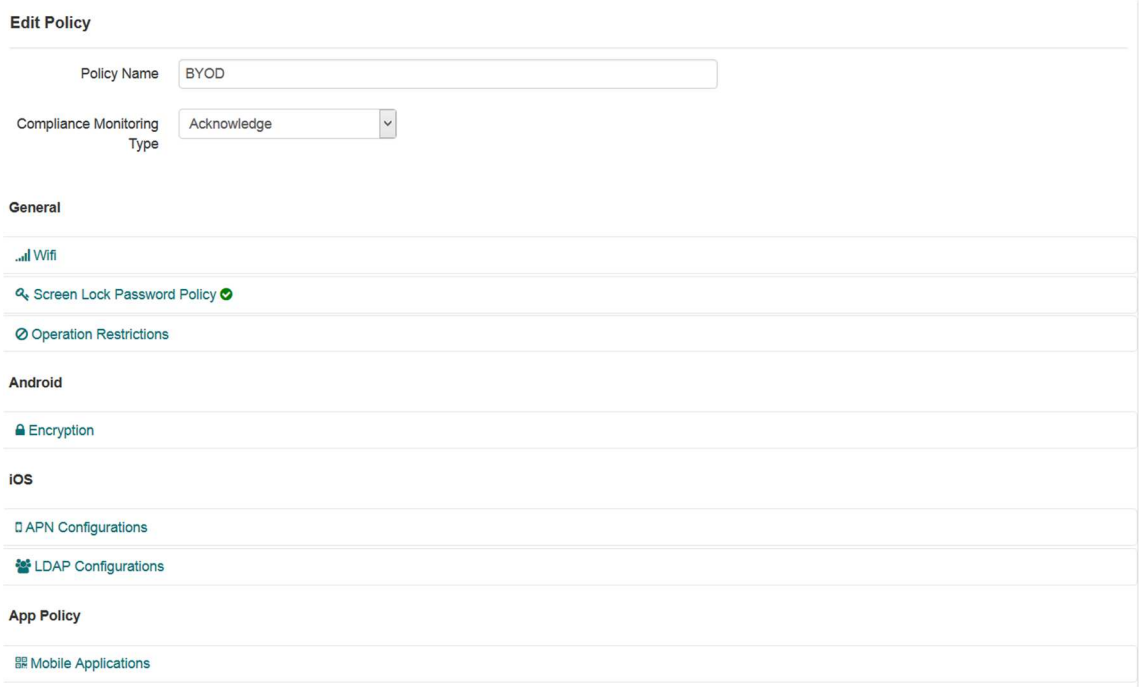
přitom v něm byly chyby. Např. odkaz na správu aplikace byl: „http://localhost:9443/emm/“ a když se zadá do vyhledávače, tak stránku nenalezne. Po dlouhém bádání jsem si všiml, že tam má být protokol HTTPS místo HTTP.



Obr. 6. Úvodní strana WSO2 je skromnější

5.3.2 Nastavení serveru

Nastavení serveru je v principu stejné u obou řešení. Je dobré nastavit konkrétní profily (pravidla), která budou ve firmě platit. Například požadavek na uzamknutí obrazovky (kolik musí mít znaků, jak složité musí být, …). Dále usnadnění připojování do firemní sítě tzn. nastavit SSID a heslo, tudíž se uživatel nemusí o připojení do firemní sítě starat a nemusí znát všechny údaje. Zda se má zařízení šifrovat. Další možnosti záleží na typu operačního systému. Tyto nastavení se mohou pro jednotlivé skupiny nebo uživatele měnit. Uživatelé se mohou roztřídit do jednotlivých skupin, které budou mít různá nastavení. Pokud má správce nastavený server, mohou se přidávat noví členové do systému kapitola 5.3.3. Snímek z obrazovky je na Obr. 7.



Obr. 7. WSO2: Nastavení pravidel pro určitou skupinu zařízení

5.3.3 Přidání nového člena

Při navázání spolupráce s novým členem v zaměstnání, je potřeba jeho zařízení začlenit do bezpečnostní politiky a vybavit potřebným softwarem, který potřebuje pro práci.

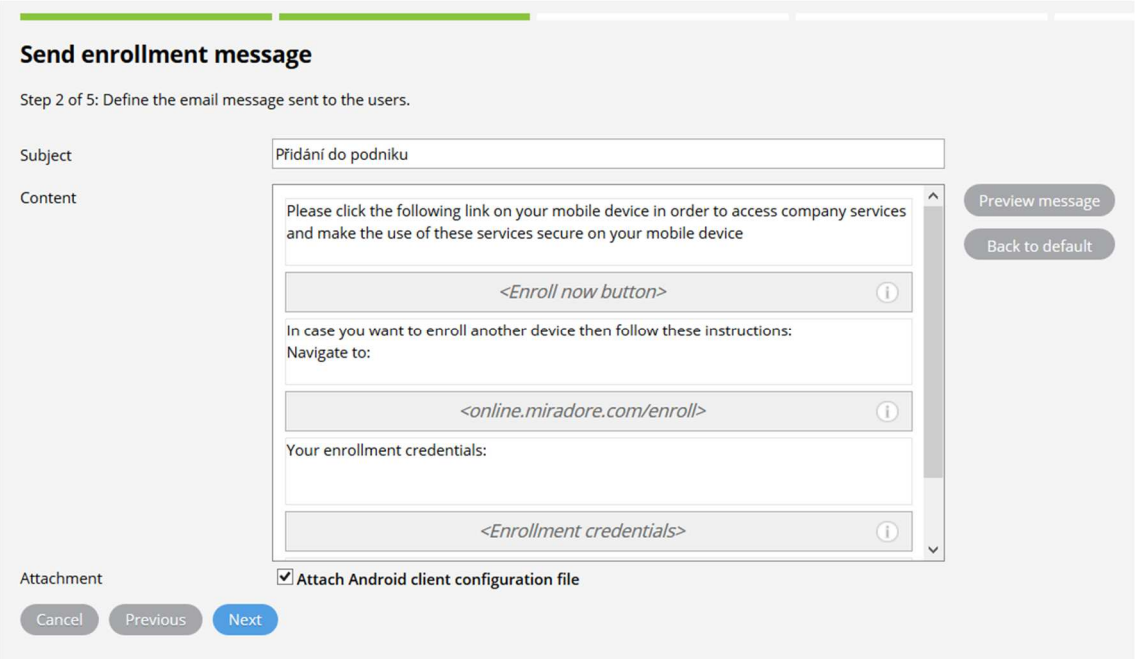
Bez MDM nástroje

Pokud chceme, aby měl nový zaměstnanec všechny data a programové vybavení, musí si sám nainstalovat všechny aplikace, musí se mu povolit sdílení u firemních dat (vytvoření účtů), ke kterým potřebuje přístup, nastavit šifrování, to všechno ručně. Všechny tato nastavení jsou zdlouhavé, je dobré si připojit zařízení k jednomu účtu a nahrát automaticky všechny potřebné aplikace s daty.

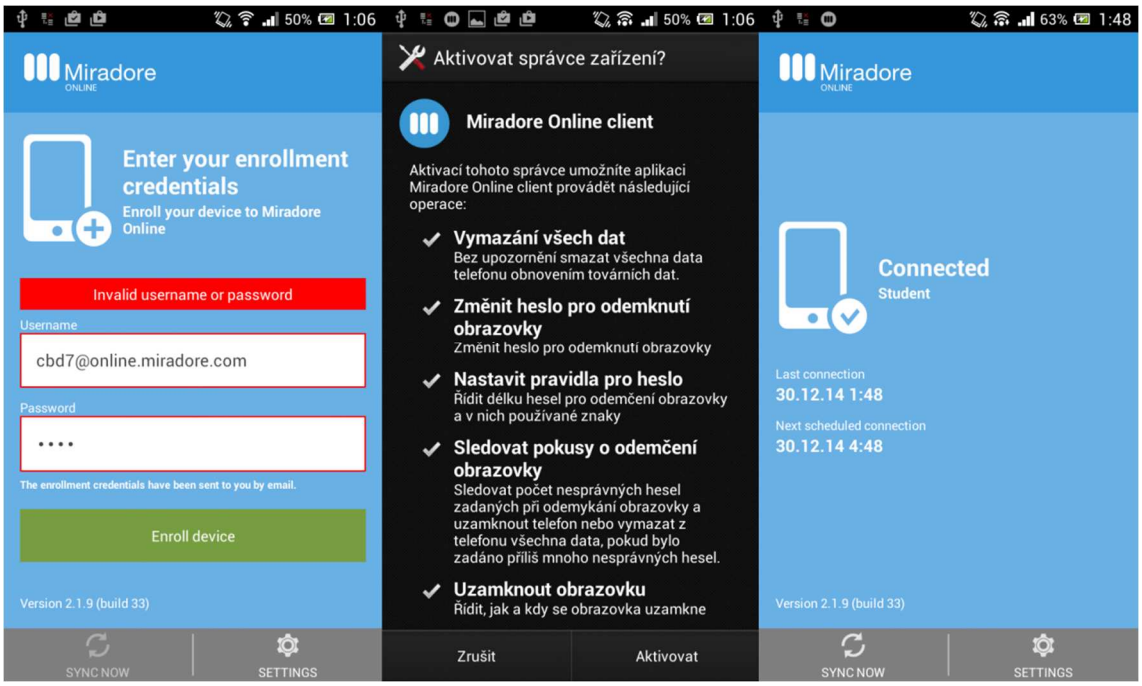
Miradore

Do Miradore je přidání člena jednoduché, správce vytvoří nového uživatele a v sekci Mobile management v záložce enrollment zadá jméno uživatele, ke kterému se má připojit nové zařízení, které má pravděpodobně operační systém. Nastaví datum vypršení nabídky na přihlášení a nakonec odešle notifikační mail, viz Obr. 8, kde bude navíc odkaz na stažení klientské aplikace, jeho uživatelské jméno a heslo. Nový uživatel nainstaluje aplikaci, spustí ji a přihlásí se pomocí svých přihlašovacích údajů, před přihlášením program uživatele obeznámí s tím, že jeho zařízení bude monitorováno a moci ovládáno od správce systému. Systém poté získá kontrolu nad zařízením Obr. 9. Může sledovat jeho sílu zabezpečení, do jakých sítí se přihlašuje, jaké aplikace používá a další.

Přidání firemních aplikací musí být provedeno stejně jako bez MDM nástroje, jelikož tento nástroj nepodporuje správu aplikací.



Obr. 8. Miradore: Přidání zařízení do systému - nastavení zprávy, která se pošle zaměstnanci

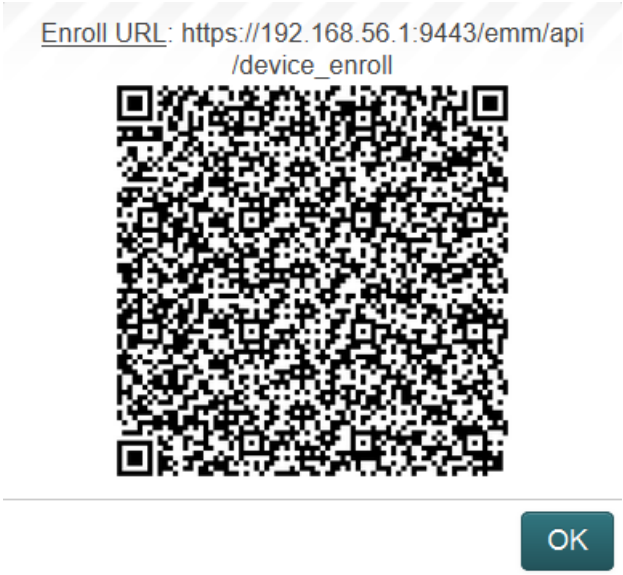


Obr. 9. Miradore: Přihlášení na mobilním zařízení

WSO2

V tomto systému se opět vytvoří nový uživatel, přiřadí se mu typ (uživatel, administrátor), role (nadefinované bezpečnostní politiky) a uživatel se přidá. Zde je to řešeno tak, že se vygeneruje QR kód Obr. 10 s odkazem na stažení klientské aplikace (WSO2 Agent Obr. 11). O doručení se stará sám správce, může například zaměstnanci poslat mailem přihlašovací údaje s odkazem na stažení aplikace. Uživatel tedy poté nainstaluje aplikaci, zadá adresu serveru, vyplní přihlašovací údaje a obeznámí se s podmínkami.

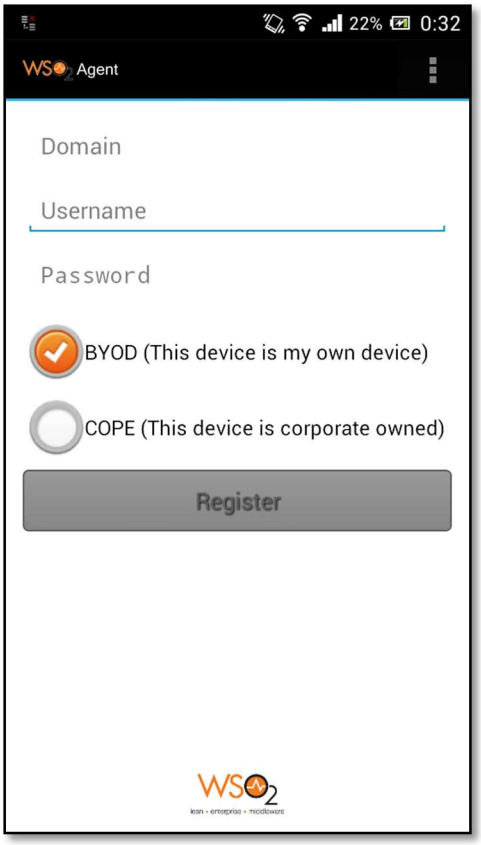
Po přihlášení uživatele do MDM mu budou nabídnuty aplikace, které jsou nastaveny pro danou skupinu zaměstnanců, do které je uživatel přiřazen.



Obr. 10. WSO2: QR Kód pro přidání zařízení do systému

Zde jsem měl opět problém při stahování RQ kódu, sloužící ke stažení klientské aplikace. V prohlížeči Mozilla Firefox[32] mě aplikace navedla na stažení verze pro iOS a ne pro Android, se kterým jsem se chtěl přihlásit, když jsem si aplikaci stáhnul manuálně Obchod play, do aplikace nešla vyplnit adresa serveru. Po několika pokusech a změně prohlížeče se aplikace podařila nainstalovat přes RQ kód a vyplnit údaje o serveru šly následně také.

[32] https://www.mozilla.org



Obr. 11. WSO2: Přihlášení na mobilním zařízení

V obou případech po zaregistrování systém získá kontrolu nad zařízením, pod podmínkou, že zařízení bude připojeno k internetu. Může sledovat jeho sílu zabezpečení, do jakých sítí se přihlašuje, jaké aplikace používá a další.

5.3.4 Ukončení spolupráce se zaměstnancem

Zde uvedu příklad o rozvázání pracovního poměru se zaměstnancem, jak se bude přistupovat k jeho vlastním zařízením.

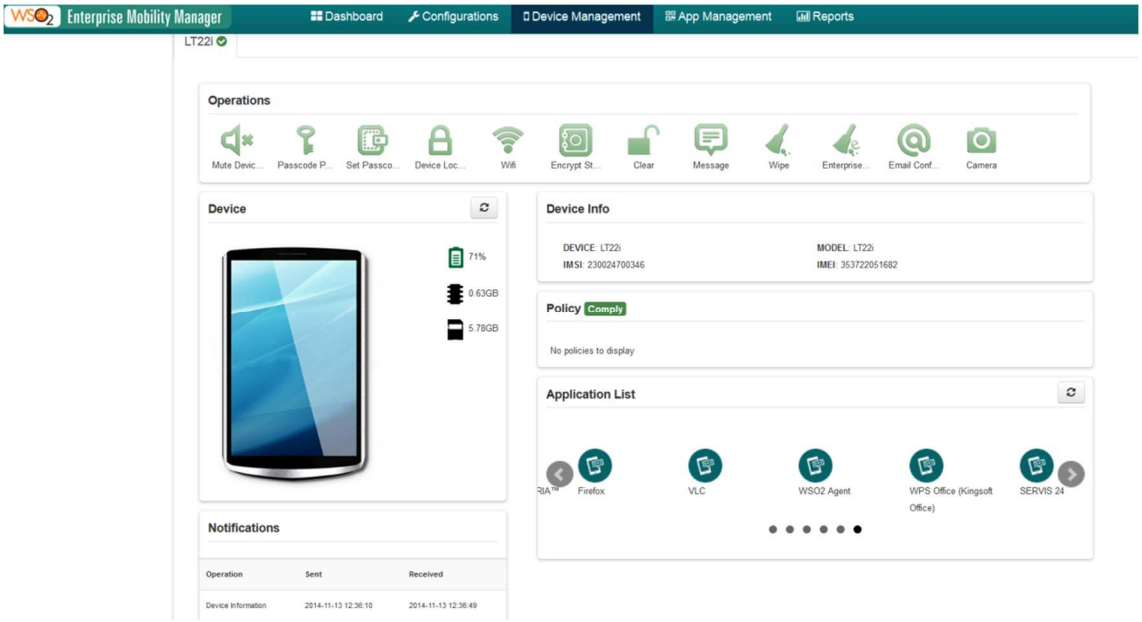
Bez MDM nástroje

Zaměstnavatel požádá svého podřízeného, aby svá data z telefonu smazal, a zakáže mu přístup k firemním souborům. Je zde riziko, jak s daty bývalý zaměstnanec naloží.

S MDM nástrojem

Zaměstnavatel má možnost smazat data ze zařízení vzdáleně bez jakéhokoliv varování. S Miradore může pouze smazat celý obsah zařízení (wipe), u WSO2 je navíc možnost smazání pouze podnikových dat (enterprise wipe). Ať už použijeme kteroukoliv možnost, obnovení dat je znemožněno, protože se nejedná o klasické smazání, ale o přepsání

dat.[33] Na Obr. 12 jsou zobrazeny možnosti vzdáleného ovládání zařízení s nástrojem WSO2, které obsahují mimo jiné i wipe a enterprise wipe.



Obr. 12. WSO2: Správa zařízení

5.3.5 Ztráta zařízení

Scénář zachycuje postup při ztrátě soukromého zařízení.

Pokud jsou data správně zabezpečena, viz kapitola 5.2.1, k informacím se nikdo nedostane. Bez MDM softwaru nemůžeme zjistit, jestli data byla zašifrována. Pokud používáme MDM nástroj, je nutno odstranit zařízení ze systému.

Odebrání zařízení z MDM systému

Nejprve se provede scénář na odstranění dat z telefonu, který je popsán v podkapitole 5.3.4. Následně obě aplikace mají stejný postup. Vybere se zařízení k odstranění a potvrdí se.

U WSO2 se vyskytla opět chyba, i přes odpojení zařízení ze systému je telefon zobrazen ve správě zařízení, i když už opravdu není připojen do systému.

[33] http://technet.idnes.cz/software.aspx?r=software&c=A060124_180218_software_dvr

5.3.6 Zapomenutí hesla

Udělejme si příklad, že jeden zaměstnanec si zašifruje celou paměť u svého smartphonu. Po čase zapomene své heslo a nebude se moct do něj dostat.

Bez MDM nástroje

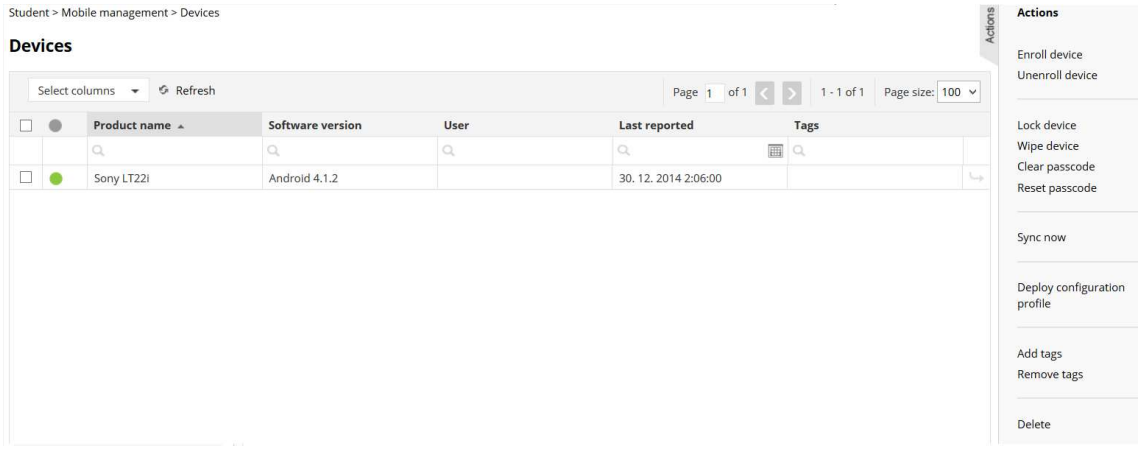
Nevýhoda šifrování je, že se nesmí zapomenout heslo. Pokud se zapomene, tak ztratíme přístup k datům pravděpodobně nadobro. Vždyť zaměstnanec má (podle předešlých navrhovaných aplikací, viz kap. 5.2.1) službu s uloženými hesly. Jestliže je tato služba v zašifrovaném zařízení, tak to heslo potřebujeme, abychom se do zařízení vůbec dostali, tudíž v tomto problému nám aplikace pro správu hesel nepomůže.

Je dobré data mít na místě, kde pokud zapomenete heslo, má k nim přístup ještě někdo další. Nejlepší je mít data synchronizována na firemním uložišti, ze kterého může správce tohoto uložiště data nahrát zpátky do zaměstnancova zařízení.

S MDM nástrojem

Pokud uživatel zapomene heslo nebo ztratí e-mail s přihlašovacími údaji, je možné vygenerovat heslo nové.

U Miradore je možnost vygenerování nového hesla a jeho poslání na e-mail. Pokud uživatel zapomněl údaje i o e-mailové schránce, uživatel si může založit nový e-mailový účet, správce mu poté upraví e-mailovou adresu u účtu a následně vygeneruje nové heslo.



Obr. 13. Miradore: Správa zařízení

WSO2 umožňuje nastavit určité heslo, tudíž ho zná správce. Uživatel si ho může později změnit na své vlastní, podle kritérií, které jsou ve firmě nastaveny.

5.3.7 Aktualizace MDM

Miradore
O aktualizování služby se správce firemního účtu nemusí starat, všechno je na straně poskytovatele služby. V případě proběhnuté aktualizace dostane klient email o proběhnutých změnách, tudíž odpadá povinnost správci firemního účtu hlídat aktualizace a o všem je dostatečně informován.

WSO2
Zde se správce musí v současné době starat o aktualizace sám, jelikož stále není dostupný uživatelský manuál pro aktualizace. Nyní se musí nainstalovat nová verze systému a do něj nakopírovat konfigurační soubory.

5.3.8 Zhodnocení scénářů

Pro přehled se v této kapitole nachází přehled předchozích scénářů a rozdíly mezi jednotlivými řešeními.

Zavedení MDM nástroje
Využití Miradore řešení je pohodlnější, jednodušší. Jelikož server spravuje přímo výrobce řešení, odpadá jeho údržba. Naopak při zavedení WSO2 se musí počítat s možnými komplikacemi.

Nastavení serveru
Nastavení firemních pravidel pro různé skupiny uživatelů je v obou případech jednoduché a přehledné. Kvalita Miradore a WSO2 je stejně vysoká.

Přidání nového zaměstnance
Zde se ukazuje výhoda WSO2, která umí přidat a odinstalovat aplikace vzdáleně a najednou. Kdežto u Miradore se musí všechny aplikace nainstalovat stejně jak bez MDM softwaru.

Ukončení spolupráce se zaměstnancem
S MDM softwarem má zaměstnavatel výhodu, že může odstranit obsah mobilního zařízení.

Ztráta zařízení
Bez MDM není možnost zjistit, jestli data byla v zařízení šifrována. Obě MDM řešení umí zkontrolovat šifrování zařízení a odeslat požadavek na smazání obsahu zařízení.

Zapomenutí hesla
Při zapomenutí hesla je výhoda možnosti obnovení hesla s MDM nástroji, tudíž se nemusí zařízení dávat do továrního nastavení.

Aktualizace MDM
Jak už bylo uvedeno v podkapitole „Zavedení MDM nástroje“ Miradore čerpá výhodu, že server spravuje poskytovatel řešení.

5.3.9 Shrnutí
Jednotlivé scénáře obsažené v této kapitole jsme porovnali s různými řešeními. Výsledkem scénářů je, že budeme-li chtít použít BYOD ve firmě, je riziko ho zavést bez správy mobilních zařízení. Přesvědčili jsme se o tom jak v kapitole 5.3.4, kde jsme ukončovali pracovní poměr, tak v kapitole 5.3.5 u ztráty zařízení.

Pokud mám vybrat MDM, které splní svůj účel, a nechci se zabývat možnými komplikacemi, volím nástroj firmy Miradore. Nemusím se starat o spuštěný server, protože o ten se stará Miradore. Při proběhlé aktualizaci, jsem informován prostřednictvím e-mailové zprávy a notifikace v systému. Z těchto důvodů doporučuji Miradore.

Pokud se mám dívat na komplexnost řešení, zvolím WSO2, protože se nestará jenom o správu mobilních zařízení, ale i o správu aplikací, která mi ušetří množství času. Další výhodou je výběrové mazání dat, které při scénáři v kapitole 5.3.4 dovolí smazat pouze firemní data.

Každé řešení má své pro a proti. Je potřeba podívat se na určitý příklad společnosti pro vybrání konkrétního řešení. To si ukážeme v kapitole 6.

6 Případová studie využití BYOD pro ukázkového zákazníka

Pro zjištění skutečných nákladů na zavedení soukromých zařízení ve firmě jsme provedli případovou studii na fiktivní společnosti, která bude uvedena v následující podkapitole. Z předchozí kapitoly 5.3.9 jsme se rozhodli, využít MDM software. Vyzkoušíme jak WSO2 tak Miradore a porovnáme jejich náklady mezi sebou.

6.1 Fiktivní společnost

Předpokládejme, že čerstvý absolvent vysoké školy dostal nápad udělat projekt, který je finančně zajímavý. Jelikož si je vědom, že není schopen dokončit projekt sám a také se obává, že ho někdo předstihne. Rozhodl se proto, že k sobě přibere několik bývalých spolužáků, kteří mu pomohou s dosažením cíle. Tým se nakonec skládá ze sedmi zaměstnanců. Ti jezdí často ke klientům na jednání, proto firma požaduje, aby měli zaměstnanci přístup k firemním datům z vlastních zařízení, přitom chce, monitorovat zabezpečení těchto zařízení.

Programové vybavení se bude skládat z doporučených produktů v kapitole 5.2. Funkce z MDM nástrojů budou upřednostněny před doporučenými produkty např. pro šifrování dat. Společnost nemá vlastní server.

6.2 Náklady

V této části jsou zobrazeny náklady na zavedení BYOD pravidel pro zaměstnance s MDM nástrojem.

6.2.1 Časové náklady

Náklady na instalaci a nastavení serveru

U Miradore bylo vše přehledné, s možností zobrazení video tutoriálu na nastavení serverových specifikací. Nastavení serveru mi trvalo při prostudování dostupných možností zhruba **50 minut**, což je na seznámení a nastavení firemního účtu velice pěkný čas.

Instalace a nastavení serveru WSO2 bylo horší. Stažení aplikace netrvalo dlouho, ale instalace serveru už tak rychlá nebyla… Nutnost doinstalování dalších služeb konkrétních verzí prodlužuje dobu trvání. Když už se vše nainstalovalo a server byl spuštěn, musel jsem zjistit, proč se nemohu dostat do uživatelského rozhraní, pro nastavení serveru, viz 5.3.1 podkapitola WSO2. Což sice byla jedna banální věc, která ale stála mnoho času. U mně tato banalita trvala zhruba osm hodin a celkem tedy **devět a půl hodiny**.

Náklady na přidání zařízení
Při přidání zařízení zaměstnance vznikají náklady v podobě času stráveného nad přidáním zařízení do systému.

Miradore
Přidání zařízení bylo snadné a bezproblémové. Proto trvalo přidání něco kolem deseti minut.

WSO2
První přidání uživatele u WSO2 trvala zhruba padesát minut, díky problémům, které nastaly v průběhu (problém nainstalování aplikace a následné vyplnění dat, viz kapitola 5.3.3).

Odebrání člena ze systému
U obou aplikací odebrání člena i jeho zařízení bylo časově zanedbatelné a do dvou minut bylo zařízení i člen odebrán. Avšak u WSO2 zůstal telefon viditelný i po jeho odpojení, i když už byl off-line a sám telefon už nemusel dodržovat žádné pravidla a mohl klientskou aplikaci odstranit. A díky tomuto problému jsem strávil dalších dvacet minut zjišťováním, proč nejde zařízení odpojit, přestože už zařízení odpojeno bylo.

6.2.2 Časové náklady po čtrnácti dnech
Po čtrnácti dnech jsem vyzkoušel opětovné nainstalování a nastavení jednotlivých základní úkonů, které byly potřeba při použití MDM ve firmě, a zaznamenal potřebnou dobu na jejich provedení.

Instalace a nastavení serveru
Při založení nového účtu u Miradore a nastavení základních politik trvalo zhruba padesát minut, zatímco u WSO2 byl po prvním pokusu čas devět a půl hodiny, při druhém se čas zredukoval na pouhou hodinu, díky tomu, že už jsem byl seznámen s chybami v systému. Stručné vypsání časů je v Tabulka 3.

Tabulka 3: Instalace a nastavení serveru

Aplikace	První pokus	Druhý pokus
Miradore	50 minut	40 minut
WSO2	570 minut	60 minut

Přidání člena
Zde se čas opět u WSO2 zredukoval a trval v porovnání s Miradore stejně dlouhou dobu 8 minut.

Tabulka 4: Přidání člena a jeho zařízení

Aplikace	První pokus	Druhý pokus
Miradore	10 minut	8 minut
WSO2	50 minut	8 minut

Odebrání člena

Při odebrání člena byl proveden wipe zařízení a odstranění člena s jeho zařízením, časy z Tabulka 5 jsou v druhém pokusu shodné. Pokud se odebírá zaměstnanec ze systému WSO2 poprvé je riziko zdržení.

Tabulka 5: Odebrání člena a jeho zařízení

Aplikace	První pokus	Druhý pokus
Miradore	5 minut	5 minut
WSO2	30 minut	5 minut

Při nasazení do firmy

Následující tabulka poukazuje, zda se při zavádění do systému nemá objednat školení, nebo odborník, který by systém sám zavedl a seznámil budoucího správce o problematice. Tabulka 6 vychází ze zadání v kapitole 6.1.

Tabulka 6: Nasazení do firmy o sedmi zaměstnancích (instalace, nastavení, přidání sedmi uživatelů)

Aplikace	První pokus	Druhý pokus
Miradore	108 minut	96 minut
WSO2	668 minut	116 minut

K časům v Tabulka 6 jsem dospěl následujícím způsobem:

- Hodnoty u prvního pokusu: instalace (první pokus) + přidání člena (první pokus) + 6 *přidání člena (druhý pokus). Např. u Miradore: instalace 50 minut + přidání člena 1 * 10 minut + 6 * přidání člena 8 minut = 108 minut.

- Hodnoty u druhého pokusu: instalace (druhý pokus) + 7 * přidání člena (druhý pokus). Např. u WSO2: instalace 60 minut + 7 * přidání člena 8 minut = 116 minut.

Shrnutí časových nákladů
Z tabulek je vidět, že Miradore je opravdu přehledné a pracuje se s ním rychle už při prvním použití. Naopak u WSO2 z tabulky vyplývá, že je potřeba se trochu seznámit s aplikací. Pokud má správce zkušenosti se systémem, pak už rozdíl dvaceti minut je zanedbatelný.

6.2.3 Odhad finančních nákladů
V této podkapitole se nacházejí jednotlivé náklady, které jsou vyjádřené peněžně.

Zavedení systému do společnosti
Hrubý odhad finančních nákladů na realizaci jednotlivých řešení je zobrazen v následující Tabulka 7. Sazba za jednu hodinu je stanovena na 1000 Kč / člověkohodin (člh) bez DPH, zaokrouhleno na půlhodiny. Data jsou převzata z Tabulka 6.

Tabulka 7: Odhad finančních nákladů na zavedení systému do firmy

Aplikace	Miradore	WSO2
První pokus	2000 Kč	11500 Kč
Druhý pokus	2000 Kč	2000 Kč

Pronájem serveru
U WSO2 je potřeba počítat ještě s pronájmem serveru, jelikož naše fiktivní společnost ho nemá, viz kapitola 6.1. Rozhodl jsem se pro pronájem virtuálního serveru (VPS), protože výkon nemusí být příliš vysoký a firma nevyužije celý server.

Cena virtuálního serveru na 1 rok: **12 200 Kč**[34]

Školení zaměstnanců ve využívání zařízení
Pro ujasnění pravidel, k jakým činnostem mohou používat zaměstnanci svá zařízení, jak mají nakládat s firemními daty, je vhodné zaměstnance důkladně proškolit. Aby později nedocházelo například k nedorozuměním v oblasti vlastnictví duševního majetku.[35]

[34] Cena vychází z ceníku VPS z http://www.master.cz/virtualni-servery-vps

[35] http://www.symantec.com/cs/cz/about/news/release/article.jsp?prid=20130220_01

Tabulka 8. Náklady na školení

Pozice	Počet členů	Sazba na 1 hodinu	Počet hodin	Náklady
Externista*	1	4000 Kč	2	8000 Kč
Zaměstnanec	7	1000 Kč	2	14000 Kč
Celkem				**22000 Kč**

*Sazba u externisty obsahuje náklady na dopravu.

Tabulka 8 zobrazuje náklady na školení před nasazením BYOD. V ceně je zahrnut odborný externista, který pracuje v oboru.

Náklady na správu mobilních zařízení
MDM systém je potřeba udržovat, kontrolovat stav zařízení. Proto musíme do nákladů připočítat navíc práci administrátora. Práci jsem uvedl hrubým odhadem, vychází na 14 minut denně (21 pracovních dnů / 5). Roční náklady na správu systému při sazbě 1000 Kč/h činí 60 000 Kč, viz Tabulka 9. Tyto náklady jsou přibližně stejné u obojího řešení.

Tabulka 9. Náklady na správu systému MDM

Počet hodin za měsíc	Počet hodin za rok	Sazba za 1 hodinu	Celkem
5	60	1000 Kč	**60 000 Kč**

6.3 Celkové náklady na využití BYOD ve společnosti
Z předchozí kapitoly 6.2.3 vytvoříme celkové náklady za zavedení systému, školení personálu, správu systému a pronájem serveru.

Tabulka 10. Celkové finanční náklady za 1 rok

Název nákladu	Cena nákladu pro Miradore	Cena nákladu pro WSO2
Zavedení systému	2 000 Kč	11 500 Kč
Školení personálu	22 000 Kč	22 000 Kč
Správa systému	60 000 Kč	60 000 Kč

Pronájem serveru	0 Kč	12 200 Kč
Celkem	**84 000 Kč**	**105 700 Kč**

Tabulka 11. Celkové finanční náklady za dobu 1 rok až 5 let

Počet let	Miradore	WSO2	Rozdíl [%]	Rozdíl
1	84 000 Kč	105 700 Kč	25,8	21 000 Kč
2	166 000 Kč	199 900 Kč	20,4	33 900 Kč
3	248 000 Kč	294 100 Kč	18,6	46 100 Kč
4	330 000 Kč	388 300 Kč	17,7	58 300 Kč
5	412 000 Kč	482 500 Kč	17,1	70 500 Kč

V Tabulka 10 jsou sečteny jednotlivé roční náklady. Tabulka 11 obsahuje finanční náklady za dobu 1 rok až 5 let. V prvním roce je WSO2 o 25,6% dražší než Miradore, hlavní příčinou jsou pořizovací náklady a pronájem virtuálního serveru. V dalších letech odpadá zavádění systému, díky tomu klesá rozdíl mezi řešeními a po pěti letech provozu je WSO2 dražší o 17,1% než Miradore.

6.4 Zvolení produktu

Před uvedením případové studie se zdála jako nejlepší volba produkt Miradore. Firma požadovala monitorování zabezpečení soukromých zařízení využívaných pro pracovní účely, což Miradore i WSO2 splňuje. Z pohledu nákladů, jsem očekával výrazný propad WSO2. Byl jsem ale překvapen, že náklady oproti Miradore po pěti letech jsou vyšší jen o 17,1%. Kdyby firma požadovala komplexnější řešení, nabídl bych WSO2, jelikož zákazník chce pouze, aby zaměstnanci mohli data využívat z vlastních zařízení a zároveň měli toto řešení zabezpečeno, doporučuji produkt Miradore s využitím školením, ve kterém se zaměstnanci dozví, jak mohou nakládat s daty uloženými v zařízení.

7 Závěr

Cílem mé bakalářské práce byla analýza problematiky BYOD, ukázat jeho možnosti využití na praktickém příkladu pro ukázkového zákazníka.

Tato práce slouží jako úvod do problematiky BYOD. Proč tento trend vznikl, jaké přínosy může mít BYOD ve společnosti, jaké problémy nejčastěji mohou nastat. Práce zároveň ukazuje, jaký nástroj se používá pro eliminování rizik spojených s tímto trendem a k plnému využití BYOD. Pro přehled jsou v práci představeny dostupné produkty, které jsou v stručně porovnány mezi sebou. Scénáře v kapitole 5.3 ukazují základní kroky, bez kterých se, při nasazení BYOD, společnost neobejde. Zda není potřeba pomoc se seznámením jednotlivých řešení. Dále je z práce vidět, že pokud chceme, aby zaměstnanci využívali svá zařízení, musíme zvážit, v jakém rozsahu budeme chtít mít kontrolu nad zařízením a zjistit jaké náklady nám navíc vzniknou. Poté můžeme vybrat konkrétní řešení nejlépe sedící daným požadavkům. V případové studii jsem provedl příklad nasazení trendu BYOD do ukázkové společnosti s vybráním konkrétního nástroje pro správu mobilních zařízení.

Osobně mě zaujalo ověření dostupných řešení pro podporu BYOD formou scénářů. Obě služby jsou zajímavé, a ačkoliv se na venek tváří podobně, rozhodně stejné nejsou. Miradore se snaží jít směrem: „Raději míň služeb, ale kvalitně a přehledně“, u WSO2 dávají přednost většímu pokrytí problematiky. Nevýhodou byla horší dokumentace, podle které se má postupovat. Při dokončování práce jsem se do dokumentace opět podíval a je vidět, že na ní pořád pracují a zdokonalují ji.

Na konec této práce uvádím, že zadané cíle byly splněny. Definoval jsem trend BYOD, popsal jeho parametry, ukázal využití BYOD ve společnostech, představil dostupný software a vytvořil případovou studii pro ukázkového zákazníka, který chtěl zavést BYOD do společnosti.

8 Přílohy

Seznam použitých zdrojů, tabulek, obrázků a použitých zkratek.

8.1 Seznam použitých zdrojů

[1] BRADLEY, Tony. PC World. Pros and cons of BYOD [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html

[2] HARKINS, Malcolm. GOV Info Security. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264

[3] JOHNSON, Nicole Blake. DefenseNews. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.defensenews.com/article/20130107/DEFFEAT02/301070014/BlackBerry-Strategizes-More-U-S-Government-Clients

[4] TWILLEY, Richard. With BYOD, Employee Productivity Surges. [online]. [cit. 2. 1. 2015]. Dostupné z: http://www.forbes.com/sites/centurylink/2013/04/26/byod-employees-bring-their-own-efficiency-to-work/

[5] Forrester Consulting. May 2012. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf

[6] Good Technology. Report 2013. [online]. [cit. 8. 12. 2014]. Dostupné z: http://media.www1.good.com/documents/Good-BYOD-Report-2013.pdf

[7] ASHFORD, Warwick. ComputerWeekly. Report. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.computerweekly.com/news/2240161202/Nearly-half-of-firms-supporting-BYOD-report-data-breaches

[8] Cisco. Expanding Role of Mobility in the Workplace. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.cisco.com/web/solutions/trends/unified_workspace/docs/Expanding_Role_of_Mobility_in_the_Workplace.pdf

[9] Trask. Mobile device management. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.trask.cz/mobile-device-management

[10] VAJNER, Radek. IT Systems. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.systemonline.cz/sprava-it/mobile-device-management.html

[11] MOLÁČEK, Petr. IT Systems. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.systemonline.cz/sprava-it/mobileiron-univerzalni-platforma-pro-spravu-telefonu.htm

[12] Airwatch. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.air-watch.com/cz/

[13] System4u. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.system4u.cz/produkty/mobilni-reseni/

[14] WIECH, Dean. Benefits and risks byod. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.mbtmag.com/articles/2013/01/benefits-and-risks-byod

[15] Cnews. [online]. [cit. 8. 12. 2014]. Dostupné z: Http://www.cnews.cz/sifrovani-v-androidu-nekolikanasobne-zpomaluje-zapis-i-cteni-z-interniho-uloziste

[16] Mobileiron. [online]. [cit. 8. 12. 2014]. Dostupné z: https://www.mobileiron.com

[17] Citrix. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.citrix.cz/

[18] BlackBerry . [online]. [cit. 8. 12. 2014]. Dostupné z: http://us.blackberry.com/enterprise.html

[19] Sun Marketing. Informace o mobilních platformách [online]. [cit. 3. 1. 2015]. Dostupné z: http://www.sunmarketing.cz/mobilni-aplikace/informace-o-mobilnich-platformach

[20] MITCHELL, Robert L. MDM tools: Features and functions compared. [online]. [cit. 3. 1. 2015]. Dostupné z: http://www.computerworld.com/article/2497055/mobile-device-management/mdm-tools-features-and-functions-compared.html

[21] Paranoiaworks. Secret Space Encryptor. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.paranoiaworks.mobi/sse

[22] Microsoft. Bitlocker. [online]. [cit. 8. 12. 2014]. Dostupné z: http://technet.microsoft.com/en-us/library/hh831713.aspx

[23] TrueCrypt. [online]. [cit. 8. 12. 2014]. Dostupné z: www.truecrypt.org

[24] Cnews. Šifrování zpomaluje zápis i čtení z interního uložiště. [online]. [cit. 8. 12. 2014]. Dostupné z: Http://www.cnews.cz/sifrovani-v-androidu-nekolikanasobne-zpomaluje-zapis-i-cteni-z-interniho-uloziste

[25] Linuxexpres. Srovnání kancelářských balíků. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.linuxexpres.cz/kancelar/srovnani-libreoffice-openoffice-org-a-microsoft-office

[26] AV-Comparatives.org. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.antivirovecentrum.cz/antiviry/srovnani.aspx

[27] Živě. Nejlepší cloudová uložiště pro vaše data. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.zive.cz/clanky/nejlepsi-cloudova-uloziste-pro-vase-data/sc-3-a-174542/default.aspx

[28] Google docs. [online]. [cit. 8. 12. 2014]. Dostupné z: https://docs.google.com/

[29] DVOŘÁK, Jakub. Emailoví klienti. [online]. [cit. 8. 12. 2014]. Dostupné z: http://technet.idnes.cz/e-malovy-klient-zdarma-069-/software.aspx?c=A130310_133052_software_dvr

[30] PCWorld Report. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.pcworld.com/article/2013169/review-ninite-turns-setting-up-a-new-computer-into-a-quick-painless-process.html

[31] WSO2. [online]. [cit. 8. 12. 2014]. Dostupné z: http://wso2.com/products/enterprise-mobility-manager/

[32] Mozzila. [online]. [cit. 4. 1. 2015]. Dostupné z: Firefoxhttps://www.mozilla.org

[33] Miradore. [online]. [cit. 8. 12. 2014]. Dostupné z: http://www.miradore.com/

[34] Technet.cz. Zničte bezpečně obsah pevného disku. [online]. [cit. 4. 1. 2015]. Dostupné z: http://technet.idnes.cz/software.aspx?r=software&c=A060124_180218_software_dvr

[35] Master. Konfigurátor VPS. [online]. [cit. 4. 1. 2015]. Dostupné z: http://www.master.cz/konfigurator/?p=VPSBETA&g=VPS

[36] Symantec. Studie Symantec. [online]. [cit. 4. 1. 2015]. Dostupné z: http://www.symantec.com/cs/cz/about/news/release/article.jsp?prid=20130220_01

8.2 Seznam tabulek

8.3 Seznam obrázků

8.4 Seznam použitých zkratek

BYOD - Bring Your Own Device

Člh -	Člověkohodina
GPS -	Global Positioning System
HTTP -	Hypertext Transfer Protocol
HTTPS -	Hypertext Transfer Protocol Secure
IMAP -	Internet Message Access Protocol
IMEI -	International Mobile Equipment Identity
MDM -	Mobile Device Management
OS -	Operating Systém
QR -	QR kód
SMTP -	Simple Mail Transfer Protocol
VPN -	Virtual Private Network
VPS	Virtuální Privátní Server