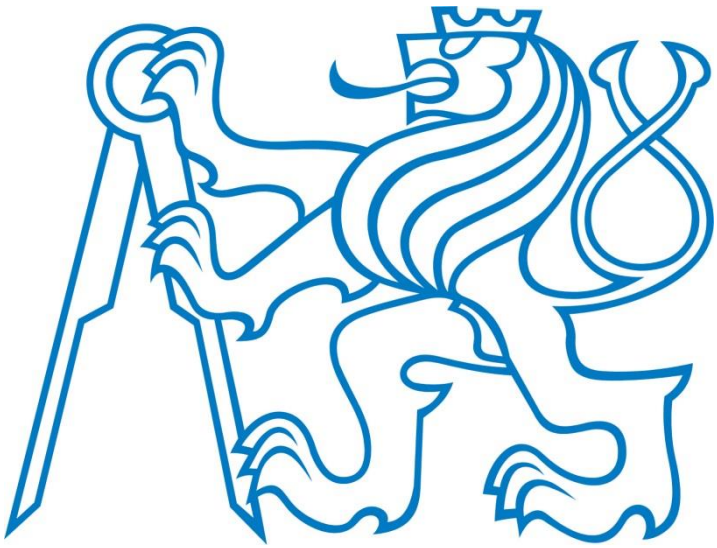
České vysoké učení technické v Praze

Fakulta elektrotechnická

Katedra ekonomiky, manažerství a humanitních věd



Bakalářská práce

Možnosti řízení mobilních zařízení ve firemních sítích

Autor bakalářské práce: Jan Knetl

Vedoucí bakalářské práce: Ing. Pavel Náplava

Rok zpracování: 2015

České vysoké učení technické v Praze
Fakulta elektrotechnická

Katedra ekonomiky, manažerství a humanitních věd

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **Knetl** Jan

Studijní program: Softwarové technologie a management
Obor: Manažerská informatika

Název tématu:

Možnosti řízení mobilních zařízení ve firemních sítích

Pokyny pro vypracování:
1. Historie, současnost a trendy v používání mobilních zařízení, způsoby řízení používání mobilních zařízení.
2. Analýza existujících řešení pro podporu řízení a používání mobilních zařízení ve firemních sítích a mimo ně.
3. Případová studie (technická i ekonomicko-manažerská) smysluplnosti využití a nasazení vybraného vhodného nástroje pro firmu ze segmentu středních a menších firem, orientovaná na služby. Firma bude upřesněna po dohodě s vedoucím práce.

Seznam odborné literatury:
1. Schlager T.: Selecting Mobile Device Management Systems: Practical Functions, Tips and Checklist, CreateSpace Independent Publishing Platform; 1.0 edition, January 17, 2013.
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 letního semestru 2015/2016

L.S.

Doc.Ing. Jaroslav Knápek, CSc. — vedoucí katedry

Prof.Ing. Pavel Ripka, CSc. — děkan

V Praze dne 10.2.2015

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

Nemám námitky proti použití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o autorských právech a právech souvisejících, ve smyslu pozdějších znění tohoto zákona.

V Praze dne …… ……

(podpis autora)

Abstrakt

Tato bakalářská práce se věnuje vytvoření průvodce ve formě dotazníku, který má za úkol pomoci při výběru vhodného Mobile Device Management řešení do společnosti. V teoretické části této práce se zabývám možnostmi nastavení tohoto specializovaného softwaru a vybírám nejdůležitější funkce Mobile Device Managementu, které dále využívám ke zformulování otázek v praktické části mé práce. Následně tyto otázky využiji k vytvoření strukturovaného průvodce, který je zaměřen na tři cílové skupiny zaměstnanců. Jedná se o vedení společnosti, IT oddělení a samotné zaměstnance (uživatele). V závěrečné části vytvořeného průvodce testuji na třech smyšlených společnostech, které ale vycházejí z reálných vzorů a výsledky porovnávám se svými hypotézami.

Abstract

This work is dedicated to creating a guide in the form of a questionnaire that is intended to assist in choosing the appropriate Mobile Device Management solutions in business. The theoretical part of this work deals with the setting of specialized software and selects the most important functions of Mobile Device Management, which I also use to formulate questions in the practical part of my work. Than i use these questions to create a structured guide that is aimed at three target groups of employees. It is a management company, IT departments and the employees themselves (users). In the final part I test the guide on three fictitious companies, which are based on real models and compare the results with my hypotheses.

Klíčová slova

Mobile Device Management, Bring Your Own Device, požadavky vedení společnost, požadavky zaměstnanců, požadavky IT oddělení, průvodce, dotazník, vyhodnocení dotazníků, doporučení Mobile Device Managementu

Key words

Mobile Device Managemetn, Bring Your Own Device, company management, employees' demands, requirements of the IT department, guide, questionnaire, evaulation of the questionnaire, recommendation for deploy Mobile Device Management

Obsah

Seznam zkratek

MDM	…	Mobile Device Management
VPN	…	Virtual Private Network (virtuální privátní síť)
AD	…	Active Directory (adresářové služby)
BYOD	…	Bring Your Own Device (užívání osobních zařízení)
POS	…	Point Of Sale (místo prodeje)
SSL	…	Secure Sockets Layer (vrstva TCP/IP protokolu)
TFS	…	Team Foundation Server (verzovací systém)
AP	…	Access Point (přístupový bod k internetu)

1 Úvod

Tématem mé bakalářské práce je „Možnosti řízení mobilních zařízení ve firemních sítích“. Zvolil jsem si jej proto, že v posledních letech stoupá ve firmách potřeba spravovat všechna mobilní zařízení, která nyní využívá většina zaměstnanců. Díky snižující se ceně chytrých telefonů, tabletů a notebooků využívá dnes tato zařízení téměř každý a na společnostech tedy je, aby se vypořádaly s jejich správou.

V teoretické části práce se zaměřím na nejdůležitější funkce Mobile Device Managementu (MDM). Definuji všechny potřebné pojmy a zaměřím se především na nejdůležitější vlastnosti Mobile Device Managementu, kterými jsou bezpečnostní politiky. Dále stanovím takzvané pilíře MDM, které budou představovat nutné funkční minimum, které by měl každý MDM software nabízet.

V praktické části práce vytvořím rozhodovacího průvodce, který je ve formě dotazníku a je tvořen sadou otázek, které budou obsahově vycházet z teoretické části mé práce. Tento průvodce má za úkol pomoci při rozhodnutí, zda je vhodné Mobile Device Management do společnosti nasadit, či nikoli. Dále vytvořím shrnutí, ve kterém budou všechny důležité informace potřebné k vyhodnocení průvodce.

V poslední řadě definuji tři společnosti, které využiji k tomu, abych na nich rozhodovacího průvodce otestoval. Mnou definované společnosti vycházejí z reálných vzorů firem, ve kterých jsou zaměstnání moji rodinní příslušníci, či známí. Každá z těchto společností bude za pomoci průvodce vyhodnocena jako vhodná, či nevhodná pro nasazení Mobile Device Managementu.

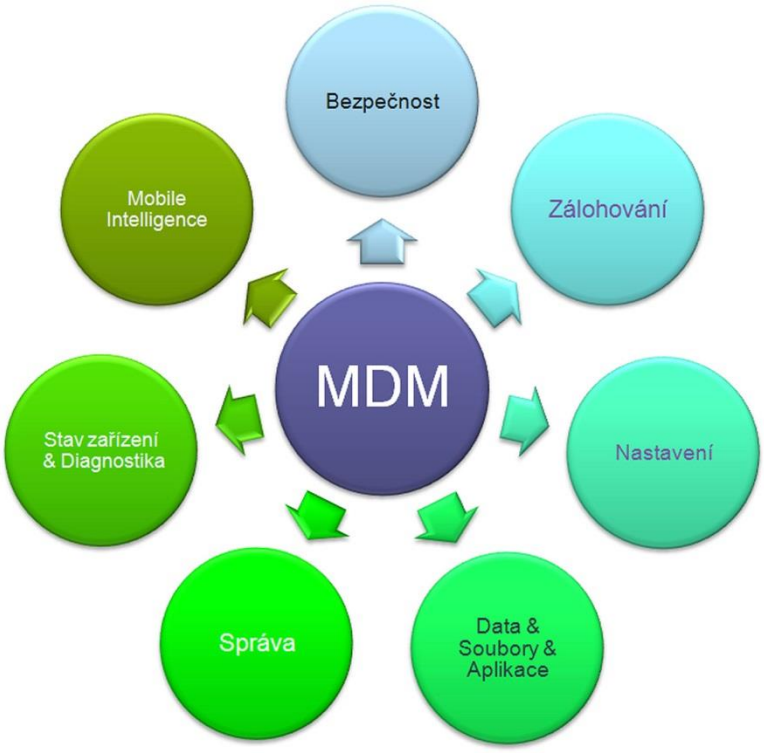
2 Co je Mobile Device Management?

V současné době většina z nás využívá v zaměstnání mobilní zařízení. Ať se pracovník nachází v kanceláři nebo na služební cestě, stále potřebuje být v kontaktu s okolním světem. V poslední době je navíc většina chytrých zařízení snadno dostupná a proto také čím dál tím více lidí přesouvá svou práci právě na ně.

Tento trend s sebou ale přináší kromě výhod jako přenositelnost a rychlost komunikace také jistá rizika. Čím více zaměstnanec využívá své zařízení pro práci, tím více se na něm kumuluje firemních dat. V neposlední řadě zařízení obsahuje uložená hesla firemních Wi-Fi, emailů, aplikací a tako mohou zprostředkovávat přístup k firemním datům pomocí virtuální privátní sítě. Všechny tyto citlivé informace jsou v případě odcizení pro útočníka velmi cenné.

Správa mobilních zařízení (neboli Mobile Device Management) je řešení, které umožňuje na zařízení vzdáleně nastavovat bezpečnostní politiky, zálohování, spravování dat a aplikací, diagnostiku a sledování stavu. Všechny tyto funkce společně utváří Mobile Device Managamenet (MDM).

Obr. č. 1: Nejčastěji využívané služby při využití MDM



Zdroj: *http://www.mobilmania.cz/clanky/firemni-smartphony-na-uzde*

Pomocí MDM je možno na všechna zařízení aplikovat bezpečnostní politiky, jako například vynucení hesla pro přístup k zařízení, VPN do firemní sítě, přístupy do vnitrofiremní Wi-Fi, omezení internetového prohlížeče, či jiná další nastavení konkrétního zařízení, která pomohou chránit data. Dále je možné sledovat stav spravovaného zařízení. Pokud se na zařízení vyskytne problém, MDM nástroj umožňuje vzdálenou diagnostiku zařízení. V neposlední řadě MDM nabízí možnost konfigurovat veškeré služby nabízené konkrétním operačním systémem zařízení.

Mobile Device Management, tak jak ho známe v dnešní podobě, je poměrně mladou záležitostí. Takto komplexní software na správu většiny dostupných zařízení je záležitostí posledních přibližně dvanácti let, kdy byly v roce 2003 založena společnost AirWatch, která je momentálně považována za lídra v tomto oboru. Ostatní společnosti, které se od svého vzniku specializovaly na jiné činnosti, se v průběhu času začaly také orientovat na Mobile Device Management. Například společnost Symantec od roku 2007, nebo BoxTone od roku 2005. Vše iniciovaly především chytré telefony, které se v roce 2005 začaly na trhu objevovat s operačním systémem Android a později v roce 2008 se po jeho zařadil také operační systém iOS. V návaznosti na obecné poznatky o MDM se v další kapitole věnuji problematice, kdy komplexní nástroje pro správu mobilních zařízení ještě neexistovaly.

3 Problematika správy mobilních zařízení v minulosti

V době, kdy internetové připojení nebylo samozřejmostí, neexistovaly chytré telefony, ani tablety a laptopy měly stále rozměry, které je sice umožňovaly přenášet, ale jejich hmotnost a životnost baterie z nich nedělala až tak užitečné pomocníky jako dnes, se do větších firem pořizovaly zejména stolní počítače. Zaměstnanec je využíval pro výkon svého povolání, tedy například tvorbu dokumentů, vedení účetnictví, programování a podobně. Nepočítalo se s tím, že by se uživatel měl připojovat do firemní sítě z jiného místa, než právě z pracoviště a tím odpadaly problémy s narušením bezpečnosti intranetů, které by samozřejmě mohly vést k poškození, či zcizení citlivých firemních dat.

Pokud byl zaměstnanec nucen pracovat z domova, využil přenosová média, na která nahrál potřebná data a poté pracoval offline. Tímto způsobem se ale zvyšovalo riziko úniku firemních dat. Pokud zaměstnanec v průběhu práce z domova zjistil, že potřebuje další data,

která si předem nezkopíroval, neměl v daný okamžik k dispozici žádné prostředky, jak se k potřebným datům dostat.

Řešením bylo vytvořit virtuální privátní síť (VPN – virtual private network), pomocí které mohl uživatel po speciální konfiguraci připojit svůj domácí počítač do firemní sítě. Nutností však bylo připojení k internetu, které nemuselo být samozřejmostí, tak jako dnes a také nastavení všech počítačů, které měly mít do intranetu přístup. Zaměstnavatel měl sice přístup k informacím, kdo a kdy se do sítě připojil, ale v zásadě mu to nijak neumožňovalo spravovat připojené zařízení a měnit jeho nastavení. V té době se to ještě nejevilo jako problém, protože pracovníků, kteří využívali tento způsob pro přístup k datům, nebylo mnoho.

Postupem času se však notebooky stávaly dostupnějšími a také potřebnějšími pro zaměstnance, kteří byli často na cestách a nemohli být tedy závislí na stolním počítači. Firmy tedy začaly notebooky pořizovat i jako primární pracovní stroje, kdy bylo možno si je v případě nutnosti přenášet mezi domovem a prací. Tento postup mohl v některých případech zefektivnit práci a také odstranit nutnost přenášení dat mezi počítači.

Zaměstnavatel ale i nadále musel čelit zvýšenému riziku ztráty dat, které mohlo být zapříčiněné odcizením přenosného počítače. Navíc zde přibývaly další problémy, které plynuly z toho, že zaměstnavatel neměl kontrolu nad přenosným počítačem. Pracovník se totiž mohl připojovat k jakémukoli AP a tím zvyšoval riziko infikování počítače nevyžádanými programy (viry, malware a jiný škodlivý software). Po opětovném připojení notebooku do interní sítě vznikalo tedy riziko zanesení viru i do ostatních počítačů, které jinak striktně podléhaly firemní bezpečnostní politice.

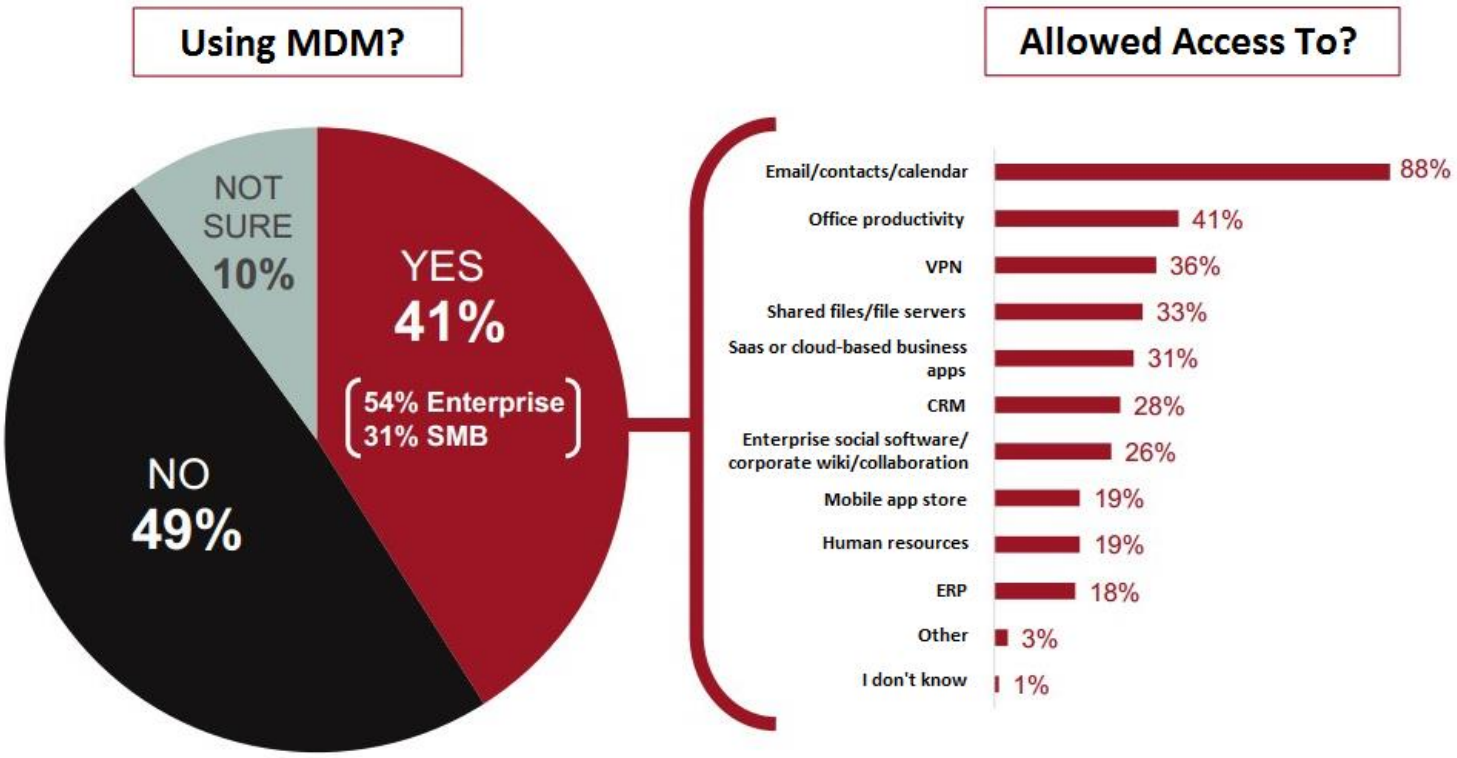
4 Chytrá zařízení dnes

S příchodem chytrých telefonů a tabletů do firem, se zvýšila mobilita zaměstnanců o další stupeň. Na obchodních cestách, nebo kdekoli jinde mimo pracoviště, tak získali možnost přístupu k firemnímu kalendáři, emailu a kontaktům, což jsou nejvyužívanější služby, které jsou pomocí těchto zařízení dostupné. Zaměstnavatel měl v některých případech dokonce možnost sledovat, kde se pracovník nachází a mohl pružně měnit důležité termíny ve sdíleném kalendáři. Tablety i chytré telefony dnes poskytují perfektní konektivitu a v mnoha

směrech dokáží při určitých činnostech plnohodnotně zastoupit a dokonce i předčít osobní počítače.

Následující graf znázorňuje služby a aplikace, které jsou nejvyužívanější ve velkých, středních a malých společnostech, po nasazení Mobile Device Managementu.

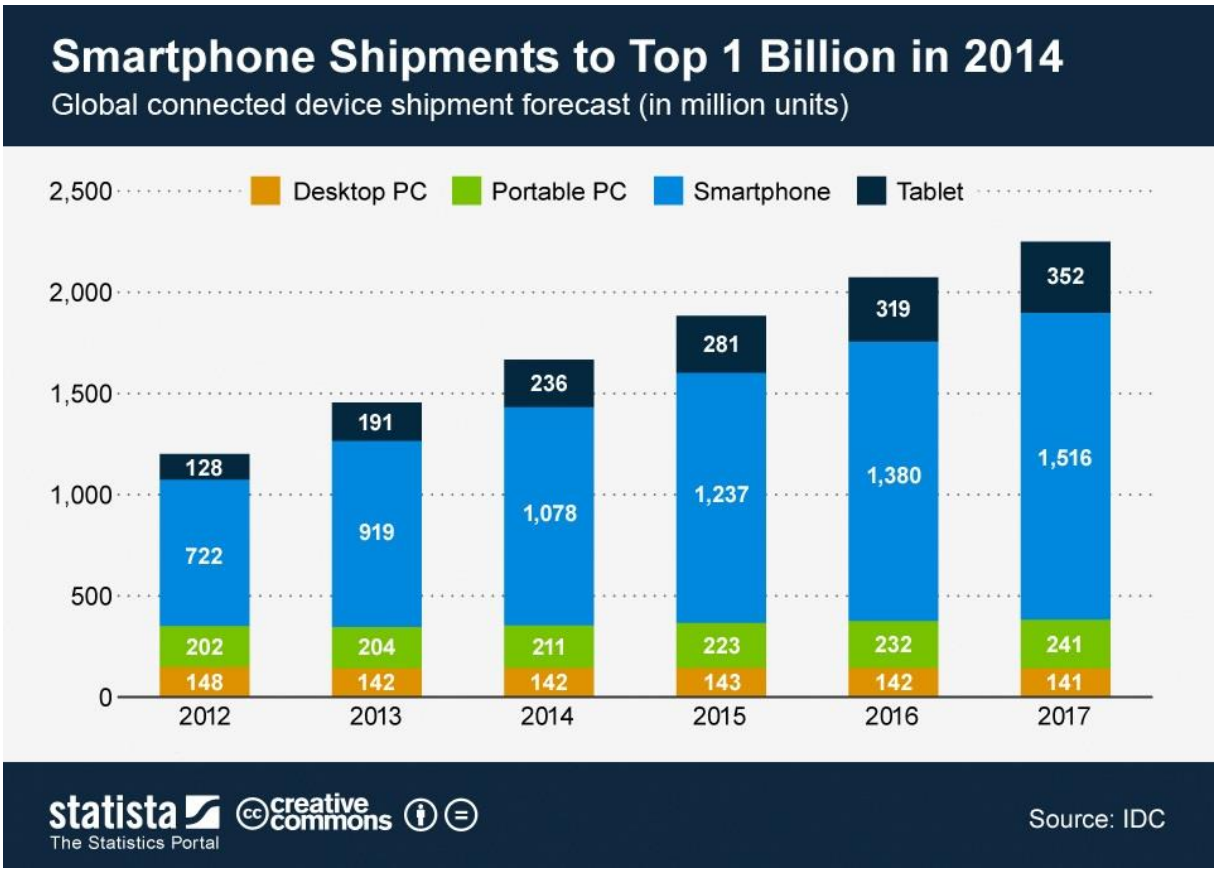
Obr. č. 2: Nejčastěji využívané služby při nasazení MDM



Zdroj: *http://www.forbes.com/sites/louiscolumbus/2014/11/26/computerworlds-2015-forecast-predicts-security-cloud-computing-and-analytics-will-lead-it-spending*

Zde je prognostický graf, který predikuje budoucí vývoj na trhu se stolními počítači, notebooky, chytrými telefony a tablety. Z grafu jednoznačně vychází, že množství distribuovaných tabletu a především chytrých telefonů v následujících letech 2015, 2016, 2017 prudce vzroste. Již teď je ale z grafu zřejmé, že chytré telefony a tablety již pomalu nahrazují stolní a přenosné počítače. Dle odhadu by se dokonce množství vyrobených stolních počítačů měl snižovat, nebo přinejmenším stagnovat.

Obr. č. 3: Předpověď počtu distribuovaných elektronických zařízení



Zdroj: *http://www.forbes.com/sites/louiscolumbus/2014/11/26/computerworlds-2015-forecast-predicts-security-cloud-computing-and-analytics-will-lead-it-spending*

Při takto velké popularitě, které se mobilní zařízení dnes těší, se často setkáváme s tím, že zaměstnanci pro pracovní účely začínají využívat vlastní zařízení, na která jsou zvyklí a která jim pomáhají zefektivňovat jejich práci. Nejčastěji se jedná o tablety a chytré telefony. Pokud společnost zaměstnancům umožní vlastní zařízení využívat, bavíme se o trendu Bring Your Own Device (BYOD), neboli "přines si své zařízení". Společnost poté stojí před problémem, kterým je správa těchto uživatelských zařízení, která se připojují do korporátních sítí a jsou na nich ukládána citlivá data.

5 Bring Your Own Device (BYOD)[1]

U tabletů a chytrých telefonů se při koupi klade důraz na požadavky firmy. Ve většině případů se jedná o kompatibilitu firemních aplikací a cenu. Kvůli tomuto přístupu je možné, že ne každému zaměstnanci přiřazené zařízení vyhovuje. Tento problém může samozřejmě

[1] http://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important--1175088

vzniknout i u notebooků a tak jsou často zaměstnanci postaveni před rozhodnutí, zdali by pro ně nebylo pohodlnější využívat pro práci osobní přístroje, které si samozřejmě vybrali dle vlastních priorit. Tento trend, kdy zaměstnanci využívají vlastní zařízení pro pracovní účely, se nazývá Bring Your Own Device.

Jak bylo již zmíněno, ne všechna zaměstnavatelem přidělaná zařízení mohou být pro pracovníka dostačující a tak se nabízí možnost přinést si do firmy vlastní počítač, chytrý telefon, či tablet. Tento trend je poslední dobou hojně využíván. Jedná se o speciální odvětví Mobile Device Managementu, protože správci IT oddělení musí čelit skutečnosti, že každý uživatel může vlastnit chytrý telefon a tablet jiné značky, stáří a s odlišnými operačními systémy. V neposlední řadě je nutné oddělit firemní a osobní data uživatelů.

Není snadné vyhovět všem a pokoušet se manuálně nastavovat přístup k firemním datům, emailům a kalendáři. Správci samozřejmě využívají pro administraci těchto zařízení specializovaný software (tato technika se nazývá MDM), ale vždy je elegantnějším řešením spravovat více zařízení od stejného dodavatele, nebo minimálně se stejným operačním systémem. S trendem BYOD tedy po zavedení MDM řešení hrozí, že některé funkcionality nebudou plně kompatibilní s operačními systémy uživatelských zařízení.

BYOD tedy na jednu stranu zvyšuje atraktivitu pracovního prostředí, zvyšuje flexibilitu pracovníka a v neposlední řadě snižuje náklady firmy za nákup IT vybavení. Je ale nutné počítat s tím, že všechna zařízení je třeba spravovat a zabezpečit je v případě krádeže, což znamená, že firma musí investovat určité prostředky k přizpůsobení se této situaci. Dále se mohou vyskytnout problémy s kompatibilitou s MDM řešením.

Z výše uvedeného je zřejmé, že nasazení MDM je sice užitečné, ale v žádném případě to neznamená, že s sebou přináší pouze pozitiva. Vyšší kontrola nad zařízeními s sebou nese určité problémy týkající se soukromí zaměstnanců a také je nutné řešit problematiku nasazení MDM. Níže uvádím podrobnější popis této problematiky.

6 Pro a proti MDM

Mobile Device Management poskytuje způsob, jakým lze kontrolovat a spravovat bezpečnostní nastavení zařízení. Způsob takové kontroly je vyžadován již i ve firmách s malým, nebo středním počtem zaměstnanců. Většina firem, dokonce i ty s nízkými bezpečnostními požadavky mají zájem o využívání MDM technologie, aby mohly lépe kontrolovat všechna pracovní zařízení a jejich uživatele. Firmy mohou navíc získat výhody pro své zaměstnance, jako například přístup k firemním emailům, důležitým firemním datům a aplikacím, což jednoznačně vede ke zvýšení jejich produktivity a efektivity.

Zařízení mohou být ovládána odkudkoli, zatímco uživatel přistupuje k informacím pomocí zabezpečené linky. Organizace tak již nejsou v ohrožení a uživatelé by neměli mít strach o zabezpečení aplikací a dat, která si ukládají a to i v případě, že zařízení ztratí, nebo jim jej někdo odcizí.

MDM funkce napomáhají firmám, aby měly přehled o všech důležitých informacích, které se týkají spravovaného zařízení. Všechny aplikace a přístup k hardware by měl být řízeny a kontrolovány správcem. Společnost, ani zaměstnanec by se již neměli dále zaobírat verzemi instalovaných aplikací a vše by za ně měl obstarat MDM.

Jeden z největších výhod MDM je, že může být aplikován napříč různými platformami. Specializované nástroje jsou schopné řídit nejrozšířenější platformy na trhu, které s největší pravděpodobností využívají také zaměstnanci firmy. Z tohoto důvodu není třeba dbát přísných výběrových kritérií při koupi nových chytrých zařízení, nebo strachu ze zavedení BYOD, protože naprostou většinu zařízení bude možno pomocí MDM spravovat.

Jsou zde ale také nevýhody pro zaměstnance plynoucí z využívání MDM. Ti přichází o určitou volnost kontrolovat svá zařízení. Již si například nemohou stahovat jakékoli aplikace z internetu, jejich zařízení jsou pod stálým dohledem specializovaného softwaru a tím přichází i o část soukromí. Některé společnosti nejsou nakloněny tomu, aby zaměstnanci používaly osobní zařízení i pro práci. Tím jsou tedy nuceni přijmout bezpečnostní politiku firmy a musí se smířit s tím, že v pracovní době mohou být sledování a kontrolováni. Některým zaměstnancům nevyhovuje, že díky mobilním zařízením mohou být k zastižení prakticky kdykoli a kdekoli a považují za narušení soukromí, když jsou vyrušeni například kvůli novému pracovnímu příkazu.

Podstatná část podnikové mobility je závislá na internetu. V prostředí bez internetového připojení tak uživatel přichází o výhody čtení emailů, připojení k VPN, nebo prohlížení sdílených kalendářů. Neznamená to ovšem, že by všechny funkcionality MDM byly závislé na internetovém připojení. Velká část bezpečnostních politik, jako například šifrování telefonu, vynucení hesla při odemykání zařízení, nebo pracovní prostory, které oddělují privátní a pracovní části zařízení, je stále aktivní.

Další nevýhodou MDM je možná závislost firmy na společnosti třetí strany, která bude provádět veškerou správu mobilních zařízení pomocí specializovaných nástrojů v případě, že společnost nemá kvalifikovaný personál.

Pokud se společnost rozhoduje, jestli MDM nasadit, je důležité předem specifikovat, jaké funkcionality od tohoto řešení očekává. I přesto je ale důležité sledovat, zda MDM řešení nabízí alespoň základní bloky (či dále pilíře) konfigurace, které musí systém pro správu mobilních zařízení obsahovat.

7 Vyžadované vlastnosti MDM[2]

Podniky v zásadě vyžadují od Mobile Device Managementu tři základní pilíře, což jsou možnost nastavení mobilních zařízení, bezpečnostní pravidla a politiky a vzdálené vymazání. Níže jsou tyto takzvané pilíře podrobně rozebrány a podrobněji vysvětleny.

7.1 Nastavení mobilních zařízení

Firemní IT potřebuje zajistit defaultní provozní nastavení všech mobilních zařízení. Tím se rozumí nastavení jazyka, instalace bezpečnostních certifikátů, spárování uživatelských účtů s podnikovou poštou, aplikačním obchodem a dalšími interními zdroji v podnikové síti. Dále je v zařízení, které je přiřazeno konkrétnímu zaměstnanci, možno nastavit dle jeho pracovního zaměření další bezpečnostní pravidla a politiky.

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

7.2 Bezpečnostní pravidla a politiky

7.2.1 Předkonfigurace a nastavení

Mobilní zařízení se často střídají mezi zaměstnanci firmy a tak je velmi důležité, aby v nich bylo možné jednoduše přednastavit služby a účty, jakou jsou Wi-Fi sítě, VPN, poštovní účty atd. Telefon, nebo tablet je tedy pro uživatele připraven k provozu bez nutnosti pracného ručního nastavení. Je to velice výhodné v případech, kdy podniková zařízení rotují, nebo je třeba novému zaměstnanci nové zařízení v co nejkratším čase přidělit. V praxi se jedná o nastavení přístupů k účtům uživatele, nastavení VPN, sdílených kalendářů, firemního emailu a všech ostatních přístupů, které jsou vázány na zaměstnance a je tak nutné je nastavit až v okamžiku, kdy je už známo, jakému uživateli bude zařízení přiřazeno.

7.2.2 Předinstalované aplikace

Tato funkce spočívá v tom, že v mobilním zařízení mohou být automaticky nainstalovány aplikace, které bude zaměstnanec z podnikového, nebo veřejného aplikačního obchodu potřebovat. Uživatel pak má dle svého pracovního zařazení okamžitě přístup ke všem důležitým aplikacím. To je užitečné především při hromadném nákupu aplikací. Další variantou je využití Mobile Device Management řešení, které umožnuje správcům vytvořit vlastní interní aplikační obchod pro zaměstnance. Zde se mohou nacházet také aplikace vyvinuté na míru konkrétní společnosti. Ty jsou pak zaměstnancům dostupné z jednoho zdroje (aplikačního obchodu).

7.2.3 Bezpečný přístup

Mezi další důležité aspekty MDM patří mimo jiné bezpečný přístup k datům a zamezení jejich poškození či ztráty. Konfigurace dostupných bezpečnostních služeb umožňuje bezpečný transfer dat mezi podnikovým systémem a mobilními zařízeními. V praxi to znamená nastavení VPN, SSL certifikátů pro přístup k firemnímu e-mailu nebo webovým službám. Nejčastěji se tedy jedná o šifrovaná spojení mezi firemními servery a mobilními zařízeními, která zabezpečují datové přenosy.

7.2.4 Omezení synchronizace

Omezení synchronizace a zálohování je často aplikováno u zařízení s iOS, kde dochází k používání iTunes a iCloud. iOS je velmi uzavřený operační systém a pro správu zařízení společnosti Apple se tak využíva specializovaný software, který v defaultním nastavení

automaticky zálohuje a synchronizuje mnoho dat a nastavené. Ostatní operační systémy (Android, Windows Phone) nejsou při svém využívání nutně vázány ke specializovanému softwaru. Lze je tedy spravovat přímo v operačním systému Windows, bez nutnosti využití speciálních aplikací. U produktů společnosti Apple je tedy zvýšené riziko toho, že se mobilní zařízení bude synchronizovat nebo zálohovat na jiné úložiště. Tím by se mohla citlivá data uložit na neověřený počítač, nebo již zmínění iCloud. Tím by se na chytrý telefon, nebo tablet mohlo uložit mnoho potenciálně nebezpečných dat, nebo i nastavení, která byla předtím vynucena za pomocí Mobile Device Managementu. Tato politiku lze aplikovat i na dalších mobilních platformách a využívá se zejména, pokud firma využívá trendu BYOD.

7.2.5 Omezení lokalizace

Velké množství aplikací dnes vyžaduje lokalizační data pro svou správnou funkčnost. Poskytování citlivých údajů, v tomto případě informací o poloze, by tedy mělo být jistým způsobem řízeno tak, aby nedocházelo k narušení soukromí uživatele. Možnost lokalizace je tedy buď omezena, nebo je omezen přístup aplikací k těmto datům. V některých případech jsou ale lokalizační data nezbytná a proto by měly být vybrány aplikace, které budou spadat do tzv. podnikového "white listu". Jedná se o aplikace, jejichž přístup k lokalizačním datům je nezbytný pro jejich správnou funkčnost. V praxi se může jednat o navigace, nebo bezpečnostní aplikace, která zaznamenává informace o poloze, které mohou být následně užitečné při stopování odcizeného zařízení.

7.2.6 Šifrovaný paměťový prostor

Jedná se o řešení, které v mobilním zařízení vytváří šifrovaný sektor. Ten obsahuje všechna důležitá firemní data a zajišťuje tak bezpečnou komunikaci s firemními systémy. Nutností je instalace klientské aplikace, která má za úkol spravovat šifrovaný obsah. Toto řešení nabízí například MDM společnosti Good Technology. Citlivá data jsou po celou dobu své existence šifrována a proto i v případě infikování zařízení virem, nebo jeho krádeže, není možné tato data zneužít. Toto řešení je vhodné především pro podnikovou politiku BYOD, kdy zaměstnavatel nemá potřebnou kontrolu nad tím, kdo zařízení využívá.

7.2.7 Omezení provozu

Především u služebních telefonních účtů je důležité kontrolovat překročení volacích limitů, počet SMS zpráv a datová připojení včetně využití těchto služeb v roamingu. Například MDM řešení od společnosti MobileIron je schopno aplikovat tarifní plány dle

potřeb jednotlivých pracovníků. Správci a uživatelé tak mohou být informování o blížícím se vyčerpání nastaveného limitu. Pokud zaměstnanec za prací necestuje do zahraničí, je mu obvykle provoz v roamingu zcela znemožněn. Užitečné to může být především pro velké organizace s vysokým počtem mobilních telefonů.

7.2.8 Omezení obsahu

Toto nastavení omezuje obsah, který je přístupný z daného zařízení. V praxi se jedná o video, audio, webové stránky. Nejrozšířenějším omezením jsou ta, která se týkají sociálních sítí, kdy si zaměstnavatel nepřeje jejich navštěvování v pracovní době. Výše uvedené je užitečné jak pro zaměstnanecká zařízení, tak pro zařízení sloužící k prodeji nebo sdílení firemních informací, kde je nevyžádané, aby tyto přístroje sloužily jinému účelu.

7.2.9 Omezení nákupu aplikací

Hlavním úkolem je zamezit možnosti přidání nových aplikací, které mohou vést k bezpečnostním problémům, nebo ke snížení produktivity zaměstnance. V závislosti na platformě mohou být omezení aplikována na nákupy z aplikačních obchodů, jako například iTunes, nebo Google Play. Toto řešení není vhodné pro společnosti, ve kterých funguje politika BYOD, protože není možné narušit svobodu uživatelů na jejich osobních zařízeních. Využití je spíše zaměřeno pro zařízení vlastněná společnostmi.

7.2.10 Kompletní omezení mobilního zařízení

V tomto případě nemá uživatel možnost měnit jakoukoli konfiguraci zařízení, nastavení emailového klienta, přidávat, nebo odebírat aplikace. Přístup do jiných než korporátních sítí je striktně zakázán. Toho nastavení je vhodné pro zařízení v terminálech, nebo v místech prodeje (POS – Point of sale), kde je primárním úkolem těchto zařízení informovat, nebo pouze nabízet například výrobky určitého sortimentu.

7.2.11 Povolení podnikových cloudových služeb

Cloudových služeb je v současnosti velmi mnoho a Mobile Device Management samozřejmě poskytuje nástroje pro možnost jejich správy. Zařízení jsou tedy předkonfigurována pro přístup k podnikovým nebo jiným schváleným veřejným cloudovým službám.

7.2.12 Vzdálená plocha

Přístup k podnikovým datům může být poskytnut prostřednictvím virtuálního desktopového řešení. Tuto možnost nabízí například MDM společnosti Citrix XenMobile. Uživatel má tedy přístup ke kompletnímu PC podnikovému prostředí, nebo jen k určitým podnikovým aplikacím, kde má uživatel k dispozici omezená data a funkce. Nasazení je vhodné pro prostředí, kde je vyžadován vysoce zabezpečený přístup, jako například bankovnictví nebo zdravotnictví.

7.3 Vzdálené vymazání

Klíčová je možnost vzdáleně vymazat firemní data a to při ztrátě, nebo odcizení zařízení. Další situací, kdy lze očekávat, že by měla být citlivá data odstraněna je ukončení pracovního poměru se zaměstnancem. Pokud se jedná o podnikové zařízení, je možné jej dle potřeby smazat kompletně. Tedy veškerá nastavení i data. Pokud ovšem zařízení patří zaměstnanci, může správce vzdáleně využít pouze částečného vymazání (Selective Wipe), kdy jsou na zařízení ponechána uživatelova soukromá data.

7.4 Vyvážený přístup

Výše uvedená trojice, nebo takzvané pilíře, jsou v reálném nasazení standardními požadavky společnosti na MDM řešení. Stále se ale jedná o nastavení, která umožňují relativní svobodu zaměstnanců a zároveň lepší kontrolu správců nad zařízením. V opačném případě, kdy by se IT oddělení snažilo řídit úplně vše spojené s mobilními zařízeními, ale také nefunguje.

Uživatelé by byli prakticky paralyzování, protože by svá zařízení neměli šanci rozumně využívat, IT správa by byla velice komplikovaná a vyčerpávala by lidské i finanční zdroje. IT by svým téměř stoprocentním dohledem budil znepokojení mezi zaměstnanci a to především pokud by se jednalo o jejich osobní zařízení (BYOD).

Z těchto důvodů je velice obtížné stanovit určitou hranici mezi IT správou a uživateli. Pokud by zaměstnancům správa jejich zařízení přišla až příliš přísná a dotěrná, mohlo by dojít k narušení firemních vztahů mezi zaměstnanci a IT správou. Je tedy velice důležité najít takové řešení, aby uživatelé byli ochotni dobrovolně a s důvěrou svěřit svá zařízení do péče IT oddělení a ti byli za pomocí MDM nástroje schopni účinně jejich zařízení spravovat.

V kapitole 7 jsem jmenoval nejdůležitější funkce, které by Mobile Device Management měl obsahovat. Jedná se především o funkce, které se týkají nastavení bezpečnostních politik. Považoval jsem za důležité je podrobněji popsat, abych v následující kapitole této práce mohl na jednotlivých MDM řešeních zkoumat, zda tyto funkčnosti opravdu mají. Dále vytvářím průvodce v podobně dotazníku, jehož otázky jsou definovány tak, aby postihly co nejvíce z uvedených možných nastavení z kapitoly 7.1, 7.2 a 7.3.

8 Základní vlastnosti vybraných MDM řešení

8.1 AirWatch by VMWare[3]

AirWatch nabízí jedno z nejvíce komplexních řešení pro správu podnikových mobilních zařízení, které může pracovat jak v Cloudu, tak přímo na firemním serveru. AirWatch Workspace umožňuje rozčlenit a spravovat podnikové aplikace a údaje, aniž by bylo nutné řídit celé zařízení. Využitím principu dvojího režimu (Dual-Persona) na zařízení, jsou společnosti schopny umožnit zaměstnancům pracovat ve standardizovaném firemním prostředí napříč všemi zařízeními a oddělit tak firemní a osobní data. AirWatch byl nedávno odkoupen společností VMWare a je nyní považován za lídra v podnikovém managementu mobilních zařízení.

AirWatch dále podporuje všechny dostupné operační systémy iOS, Android, Blackberry, Windows Phone a Windows Mobile. Jedná se zároveň o nejvyužívanější operační systémy na mobilních zařízeních.

Pro snadnější správu uživatelů umožňuje AirWatch napojení na firemní systém Active Directory, kde je možné spravovat uživatele, nebo celé skupiny uživatelů. Všem spravovaným zařízením je poté možno aplikovat jakékoli bezpečností politiky firmy. Samotné přihlášení zařízení do systému MDM probíhá za využití mobilní aplikace, ve které se za pomoci například jednorázového hesla, zařízení připojí.

Mezi základní funkčnosti systému AirWatch patří vynucení politiky hesel, které tak ochrání zařízení proti neoprávněnému využívání v případě, že se dostane do nepovolaných rukou. Dále je možno nastavit délku hesla, jeho složitost nebo nutnost heslo měnit ve stanovených časových intervalech. Aby se předešlo využívání stále stejných hesel, je možné sledovat historii hesel a zamezit tak nevyžádaným duplicitám.

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

Aby ochrana heslem měla opravdu smysl, je důležité, aby byla zařízení uzamykána uživateli. Na to se ovšem nelze spoléhat a proto AirWatch umožňuje vynucení uzamčení zařízení po stanoveném časovém intervalu. Pokud by bylo zařízení ztraceno, další bezpečnostní politika dovoluje správci, aby nastavil maximální počet pokusů o zadání hesla, po kterém se zařízení na určitý čas zablokuje a znemožní tak další pokusy o odemčení.

Další možností je nastavení vzdáleného smazání zařízení. Administrátor AirWatch má tak kdykoli možnost celé spravované zařízení vymazat. To může učinit i zaměstnanec, pokud je mu umožněn přístup do samoobslužného portálu. Dále AirWatch umožňuje vymazat pouze selektivní mazání, kdy se může jednat o vzdálené odstranění e-mailových účtů, aplikací, či firemních dat.

V neposlední řadě AirWatch nabízí šifrování interní paměti mobilního zařízení a dále i paměťové karty do něj vložené. Tím se zamezí přenositelnosti dat, která jsou čitelná pouze na zařízení, které tato data zašifrovalo.

AirWatch dále nabízí takzvanou kontejnerizaci, v rámci které je možné pracovat s firemními daty v takzvaných kontejnerech, které oddělují firemní a soukromá data a zároveň veškerou práci s těmito daty zabezpečuje. V rámci MDM je možné definovat, jaké operace se v rámci kontejneru mohou s daty vykonávat. Například je možné omezit přenosy souborů ze zabezpečeného kontejneru do jiných aplikací. Mohou ale existovat výjimky, kdy se data z kontejneru mohou využívat i v aplikacích, které implementují bezpečnostní politiku AirWatch.

Řešení AirWatch dovoluje monitorovat mobilní zařízení. Správce může například sledovat délku hovorů, počet odeslaných SMS, či objem přenesených dat. Dále je možné zařízení vystopovat, pokud je ovšem připojené k síti internet.

V prostředí AirWatch je možné vytvořit firemní obchod s aplikacemi, odkud mohou zaměstnanci stahovat aplikace vyvinuté pro potřebu firmy, nebo ostatní povolené aplikace z veřejného aplikačního obchodu. Pro tyto potřeby je možné v MDM definovat takzvaný Blacklist a Whitelist, ve kterém je možné definovat schválené, či nevyžádané aplikace.

Kromě správy aplikací umožňuje MDM také správu souborů uložených v konkrétním kontejneru. Správce má tedy přehled o všech datech v kontejneru a může je vzdáleně aktualizovat, mazat, nebo nahrávat nová.

8.2 MaaS360 by Fiberlink, společnost IBM[4]

MDM řešení MaaS360 společnosti Fiberlink poskytuje své řešení formou SaaS (Software as a Service). Prakticky dochází k hostování aplikace provozovatelem služby, která je dále nabízena zákazníkovi přes internet. V současnosti se jedná o jedno z nejznámějších MDM řešení.

Obdobně jaké výše zmiňované řešení AirWatch, podporuje MaaS360 nejrozšířenější operační systémy mobilních zařízení, což jsou Android, iOS, BlackBerry, Windows Phone a Windows Mobile. Společné s AirWatch je také napojení na firemní systém ActiveDirectory, díky kterému je umožněna snadnější správa uživatelů, nebo skupin. Uživatelské údaje z ActiveDirectory jsou posléze využívány pro přihlašování zařízení do MDM.

Ke zvýšení bezpečnosti MaaS360 umožňuje vynucení hesel napříč všemi spravovanými zařízeními. Tím je myšleno definování délky hesla a jeho složitosti. Aby se předešlo opětovnému využívání stejných hesel, umožňuje MDM nastavení intervalu, po jehož uplynutí bude nutno zadat heslo nové, které však bude jiné než hesla použitá předtím. Aby byla ochrana heslem plně využita, je velmi důležité, aby se zařízení uzamykalo v případě, že jej uživatel nevyužívá. Správce může do jisté míry spoléhat na to, že zaměstnanec mobilní zařízení zamyká, ale přesto je možné tento proces automatizovat a vynutit jej pomocí MDM.

Dále je možné nastavit maximální počet nesprávného zadání hesla, po kterém se zařízení zablokuje a znemožní tak případné pokusy o prolomení zabezpečení.

Pro zajištění bezpečnosti umožňuje MaaS360 vzdálené vymazání celého zařízení. Jedná se buď o odstranění všech dat a uvedení zařízení do továrního nastavení, nebo pouze o selektivní smazání, které umožňuje odstranit pouze firemní data. Zařízení je možné také vzdáleně zamknout, či odemknout. Tyto operace může provést i uživatel sám, pokud ovšem dostane přístupové údaje do samoobslužného portálu.

Ke zvýšení zabezpečení na samotných zařízeních je možné využít šifrování. Tímto způsobem lze zašifrovat interní paměť telefonu i například externí paměťovou kartu, která může obsahovat firemní data.

MaaS360 automaticky detekuje zařízení, na kterých byl proveden jailbreake (operační sytém iOS), nebo root (operační systém Android). Po detekci takto modifikovaných

[4] http://www.maas360.com/

operačních systémů je možné je úplně zablokovat, smazat, omezit jejich přístupy k firemním datům, nebo jakkoli jinak ošetřit, že tato zařízení jsou více zranitelná. MDM zároveň detekuje všechna zařízení, která nejsou konfigurována v souladu s bezpečnostními politikami, což později může správce dle potřeby řešit.

U zařízení pracujících se systémem iOS je možné blokovat některé služby, či aplikace, které využívají iCloud. Vzniklo by totiž riziko, že by se firemní data mohla zálohovat na soukromé uložiště zaměstnance, což by znamenalo narušení bezpečnostní politiky firmy. Stejně jako u MDM AirWatch využívá MaaS360 kontejnerizace. Data v kontejneru jsou tedy chráněna proti kopírování mimo něj. Kontejnerizace dále znemožňuje upravování dat a jejich využívání v aplikacích, která nedodržují bezpečnostní pravidla MDM MaaS360.

Řešení MaaS360 dovoluje také monitorovat mobilní zařízení. Správce může například sledovat délku hovorů, počet odeslaných SMS, či objem přenesených dat. Je možné omezit využívané služby a nastavovat jejich limity. Dále je možné zařízení vystopovat, pokud je ovšem připojené k síti internet.

Obdobně jako jiná zmiňovaná MDM řešení, i MaaS360 poskytuje možnost vytvořit firemní aplikační obchod, ve kterém se budou s největší pravděpodobností nacházet aplikace, které byly vyvinuty přímo pro interní potřeby společnosti. Dále je zde možné umožnit přístup k aplikacím, které jsou dostupné z veřejných aplikačních obchodů. MaaS360 nedokáže zamezit instalaci nevyžádaných aplikací, ale za použití již zmiňovaných White a Black listů je možné sledovat, která zařízení nedodržují bezpečností politiky. Těm je poté možno adekvátním způsobem omezit, či jinak upravit přístup k firemním datům a využívání podnikové sítě.

8.3 Good Technology[5]

MDM řešení společnost Good Technology se zaměřuje především na podporu trendu BYOD, tedy na správu osobních mobilních zařízení, která zaměstnanci využívají pro pracovní účely. Produkt je možné využívat v Cloudu, nebo si jej nechat nainstalovat přímo na firemní servery.

[5] https://www1.good.com/

Good Technology podporuje operační systémy a technologie Android, iOS, Apple Watch, Windows Phone, Windows Mobile a Samsung KNOX. Opět se zde setkáváme s napojením na firemní systém Active Directory, díky kterému je umožněna snadnější správa uživatelů, nebo skupin. Uživatelské údaje z ActiveDirectory jsou posléze využívány pro přihlašování zařízení do MDM.

Ke zvýšení zabezpečení zařízení umožňuje MDM vynutit politiku hesel. Nastavení této služby je totožné jako u výše zmíněného MDM řešení AirWatch a MaaS360, proto ji zde nebudu dále popisovat.

Jak je již zvykem, i tento MDM umožňuje spravované zařízení vzdáleně smazat. Smazat je možné opět celé zařízení, nebo selektivně pouze firemní data. Dále je dostupné vzdálené uzamčení, či odemčení zařízení, které je možné provést také pomocí uživatelské samoobsluhy.

MDM Good Technology dokáže také detekovat, zda byl operační systém násilně otevřen jailbreakem, nebo rootem a nastavení možných omezení je opět stejné jako u AirWatch a MaaS360.

Dále nabízí takzvanou kontejnerizaci, v rámci které je možné pracovat s firemními daty v takzvaných kontejnerech, které oddělují firemní a soukromá data a zároveň veškerou práci s těmito daty zabezpečuje. V rámci MDM je možné definovat, jaké operace se v rámci kontejneru mohou s daty vykonávat. Například je možné omezit přenosy souborů ze zabezpečeného kontejneru do jiných aplikací, které již nedodržují potřebné bezpečnostní politiky. Opět je zde možné nastavit potřebné výjimky. V rámci monitoringu umožňuje toto MDM sledovat především délky hovoru, počty odeslaných SMS a objemy přenesených dat.

Stejně jako předešlá MDM řešení podporuje Good Technology správu aplikací. Je možné vytvořit firemní aplikační obchod, ve kterém budou dostupné aplikace, navržené speciálně pro společnost a také některé aplikace, které jsou dostupné z veřejného aplikačního obchodu. Za pomocí White a Black listů je posléze možné sledovat, která zařízení porušují politiku týkající se schválených aplikací a podle toho tato zařízení spravovat.

9 Výsledky srovnání vybraných MDM řešení

V této části práce jsem se pokusil shrnout nejdůležitější a nejvyužívanější funkcionality MDM softwaru. Ke každé jsem uvedl stručný popis toho, jak funguje a k čemu se využívá. Celkový souhrn těchto funkcionalit by měl čtenáři pomoci vytvořit obraz toho, jak MDM software funguje a co by od něj měl očekávat.

Dále jsem zvolil tři MDM řešení, která se momentálně řadí na špičku v odvětví správy mobilních zařízení, a pokusil jsem se popsat jejich vlastnosti, které je nejlépe charakterizují. Vybraná MDM řešení jsou AirWatch společnosti VMWare, MaaS360 společnosti IBM a Good Technology.

Po sepsání a opětovném přečtení této časti, práce jsem si uvědomil, že mnou vybraná MDM řešení a jejich funkce se téměř neliší. Rozhodnul jsem se ale, že i přesto podrobnější popis funkcí jednotlivých MDM řešení ve své práci ponechám, abych zdůraznil to, že tyto společnosti, které vyvíjí MDM software jsou v současnosti na srovnatelné úrovni. Například absence možnosti nasazení v Cloudu by v dnešní době měla za následek, že by se dané řešení stalo neatraktivním pro velkou skupinu společností, které nemají vyhovující infrastrukturu pro nasazení On Premise.

Níže uvedená tabulka přehledně znázorňuje vybrané funkce u tří zvolených výrobců MDM. Z tabulky opět vyplývá, že tyto funkce nabízí, až na malé výjimky každý ze zvolených produktů. Proto je při výběru řešení zvážit také uživatelskou podporu a cenu.

To vše vede společnosti spíše k tomu, aby nejprve pečlivě zvážily, zda je vhodné MDM software vůbec nasadit. Proto se v další části své práce zaměřím na vytvoření průvodce, který by měl pomoci při rozhodování, zda je nasazení MDM vhodným krokem, či nikoli.

Tabulka. č. 1: Porovnání vlastností vybraných MDM řešení[6]

Název produktu	AirWatch by VMWare	MaaS360 by Fiberlink	Good Technology
Nasazení On premise	Ano	Ano	Ano
Nasazení v Cloudu	Ano	Ano	Ano
Výběrové vymazání zařízení	Ano	Ano	Ano
Nastavení VPN, Wi-Fi, proxy	Ano	Ano	Ano
Zakázání Wi-Fi	Ano	Ano	Ano
Zakázání mobilních dat	Ano	Ano	Ano
Podpora kontejnerizace	Ano	Ano	Ano
Detekce malware	Ano	Ne	Ne
Vzdálené vymazání zařízení	Ano	Ano	Ano
Ochrana heslem	Ano	Ano	Ano
Podpora iOS	Ano	Ano	Ano
Podpora Android	Ano	Ano	Ano
Šifrování paměťového prostoru	Ano	Ano	Ano
Šifrování emailů a složek	Ano	Ano	Ano
Detekce jailberaku/rootu	Ano	Ano	Ano
Vzdálené ovládání	Ano	Ne	Ano

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

10 Cílové skupiny průvodce

V této části práce se zaměřím za zformulování průvodce, který má za úkol pomoci zodpovědět otázku, zda je do společnosti vhodné MDM nasadit, či nikoli. Ten se skládá z 24 otázek, které jsou koncipovány tak, aby dotazovaný ve většině případů měl možnost odpovědi pouze ano, či ne. Průvodce je navržen tak, aby na otázky bylo možné odpovědět pouze možnostmi ano, či ne. Tento systém je jednodušší pro vyhodnocení a zároveň snazší pro dotazované, kteří jej vyplňují. Otázky jsou formulovány tak, aby postihly co nejvíce důležitých aspektů při rozhodování zda MDM nasadit či nikoli. Dotazovaný tak nemusí vybírat odpovědi z mnoha podobných možností, které mohou být komplikované a nemají zase až takovou vypovídající hodnotu.

Otázky jsou strukturovány dle tří různých pohledů na firmu. Jedná se o pohled zaměstnanců, společnosti a IT oddělení. Společně tvoří dle mého názoru nejvíce zainteresované skupiny, které je třeba brát v potaz při rozhodování, zda přejít na hromadnou správu mobilních zařízení za pomoci nástrojů MDM. Samotné otázky ale obsahově vychází ze tří pilířů, které jsou podrobněji rozebrány v kapitole 8. Je ovšem důležité si uvědomit, že tyto pilíře definují jakési vyžadované minimum na funkce MDM. Pokud se ale pokoušíme zjistit, zda je implementace MDM řešení vhodná, je nutné zformulovat za pomoci těchto tří pilířů otázky, které ovšem není možné klást pouze jedné osobě. Je tedy nutné definovat zainteresované skupiny zaměstnanců, které bude nutné před nasazením MDM oslovit. V našem případě tedy vedení společnosti, IT oddělení a zaměstnanci.

Sdílení informací a komunikace mezi těmito třemi skupinami je naprosto zásadní. Na vrcholu všeho stojí samozřejmě vedení společnosti. Podnět ke zvážení implementace MDM řešení ale nemusí nutně přijít od vedení společnosti. Mohou ho iniciovat samotní zaměstnanci, nebo například IT oddělení, které vidí jasné nedostatky, které znemožňují efektivní správu zvětšujícího se počtu firemních zařízení.

10.1 Vedení společnosti

Vedení společnosti, jako takové, by mělo mít obecný přehled o tom, jaký počet mobilních zařízení je zaměstnanci využíván, zda plánuje v budoucnu například nákup nových chytrých telefonů a tabletů, nebo jaké strategie zavedla při využívání těchto zařízení. V praxi se jedná především o to, jestli firma podporuje trend BYOD, nebo zaměstnancům přiřazuje firemní zařízení.

Dále by si dle statistik mělo být vědomo efektivnosti práce svých zaměstnanců. Pokud například po konzultaci s IT oddělením dojde k závěru, že na firemních přístrojích jsou často navštěvovány nevyžádané weby jako například sociální sítě, je možné, že vyvstávají mnohé otázky, jak by se tomu dalo zabránit.

Další možností je jednoduchá potřeba donutit zaměstnance pracovat efektivněji. Pokud se jedná o efektivitu práce a mobilní zařízení, dojde vedení jistě k závěru, že rozmáhající se trend BYOD by mohl být zajímavým řešením. Pokud ale k tomuto kroku přistoupí, musí si být vědomo všech rizik, která toto řešení s sebou přináší. Minimalizovat tato rizika je možné zavedením MDM do společnosti. Dále je nutné zjistit, zda uživatelé o takové řešení mají vůbec zájem a zda alespoň podstatná většina zaměstnanců vlastní osobní chytré zařízení.

Pokud jsou často hlášený ztráty, nebo krádeže mobilních zařízení, může se jednat o další důvod k zavedení MDM. Uživatelé často pro výkon svého povolání potřebují přístup k datům uložených na serverech společnosti, nebo využívají speciálně vyvinuté aplikace, které byly navrženy firmě na míru.

Všech těchto informací by si mělo být vedení vědomo, jelikož každá z nich je malým dílkem, který ve výsledku tvoří potřebu zavedení MDM do společnosti. Pokud by byla tato potřeba dlouho přehlížena, mohlo by dojít k narušení vztahů mezi všemi třemi skupinami, což by mohlo mít pro budoucí vývoj společnosti velmi nekalý dopad.

10.2 Uživatelé

Je důležité pozorovat, jaké potřeby mají zaměstnanci společnosti. Obvykle se mezi nimi profesním zařazením a zkušenostmi vytvoří několik málo skupin, které mají odlišné požadavky na funkce svého mobilního zařízení. Tyto skupiny nelze přesně definovat a můžou se lišit v každé společnosti, dle oboru, ve kterém se pohybuje.

Nutno říci, že všichni zaměstnanci mají určité požadavky, které mají společné. Jedná se o přístupy k firemnímu e-mailu a kalendáři a další běžné služby, které elektronicky gramotný člověk každý den využívá. Dále je nutné udržovat ve všech zařízeních základní bezpečnostní politiky, které musí být vynucovány bez ohledu na to, jakou funkci zaměstnanec zastává.

Rámcově se ale můžeme bavit o zaměstnancích, kteří většinu svého času pracují z místa sídla společnosti. Ti většinou nemají speciální požadavky, pokud nezastávají

důležitější posty a nepotřebují se například připojovat vzdáleně do firemní sítě, aby mohli i z domova pracovat s korporátními daty.

Dále se může jednat o zaměstnance, kteří pracují mimo sídlo společnosti, ale stále spadají pod IT správu, která se fyzicky nachází v hlavním sídle. Tito pracovníci nemají většinou možnost svá zařízení v případě problému odnést a řešit své problémy s IT personálem. Pro ty je velmi výhodné, když jsou jejich zařízení konfigurována tak, aby se dala vzdáleně nastavovat. Může se například jednat o jednoduchou službu vzdálené plochy (Remote Desktop), která v některých případech může částečně suplovat MDM řešení.

Třetí skupinou zaměstnanců jsou ti, kteří jsou nuceni pracovat často mimo sídlo společnosti. Může se jednat o obchodní manažery, nebo jakékoli jiné zaměstnance, jejichž pozice je nutí být často na cestách. Ti pak vyžadují nastavení roamingu, vzdálených přístupů k datům, či sdílení kalendářů s jinými zaměstnanci. Vedení společnosti poté může zajímat objem přenesených dat v zahraničí, nebo stanovení volacích limitů.

10.3 IT oddělení

Pokud má vedení dostatek podnětů ke zvážení nasazení MDM řešení přichází na řadu zmapovat situaci ve firemním IT oddělení. To může být při nasazování velmi nápomocné, nebo se mohou vyskytnout další problémy týkající se nízkých znalostí MDM problematiky. V každém případě i vedoucí IT segmentu, který nemá s řízením mobilních zařízení dostatečné zkušenosti, může iniciovat jeho zavedení. Jen toto oddělení má totiž skutečný přehled o tom, jak komplikované je spravování mobilních zařízení a jak je těmito úkony zatěžováno. V případě, že správa těchto zařízení překročí určitou mez a IT pracovníci jsou zbytečně vytěžováni častým konfigurováním uživatelských přístrojů, měli by sami navrhnout odpovídající řešení.

IT oddělení společnosti má také jako jediné přehled o aktuální infrastruktuře společnosti a o jejím fungování. Dle požadavků je na zaměstnancích IT aby zvážili, zda je pro nasazení MDM řešení ve společnosti dostupný dostatečný hardware, nebo by upřednostnili správu za využití Cloudu.

Díky těmto skutečnostem je ve vytvořeném průvodci mnoho otázek směřováno právě k IT zaměstnancům, kteří jako jediní mohou řešit technické problémy spojené s nasazením a

ve výsledku to budou právě oni, kteří budou celý software řídit. Je proto velmi důležité, aby veškeré požadavky na MDM řešení byly prodiskutovány také s nimi a je velmi pravděpodobné, že se dle vlastních zkušeností přikloní i k nějakému konkrétnímu softwaru.

Na základě výše uvedených zainteresovaných skupin a definici tří základních pilířů MDM, jsem zformuloval 24 otázek. Jejich úkolem je, aby co nejvíce pokryly problematiku tří pilířů, tedy funkčního minima MDM softwaru. Dále jsou všechny otázky strukturovány tak, aby byly pokládány pouze zainteresovaným skupinám zaměstnanců. Tím je zajištěno, že na otázky bude odpovídat pouze skupina zaměstnanců, kteří mají k jejich zodpovězení potřebné informace. Průvodce je formulován v následující kapitole.

11 Průvodce ve formě dotazníku

11.1 Část pro vedení společnosti

1. Má Vaše společnost více než 70 zaměstnanců?

Zcela zásadní dotaz, který společně s odpovědí na otázku č. 2 pomůže utvořit přibližný obraz o tom, kolik zaměstnanců ve firmě využívá mobilní zařízení. Pokud bude zařízení podstatně méně, než zaměstnanců a zároveň jich bude více než 50, můžeme vypozorovat, že společnost má ještě jisté rezervy v mobilitě zaměstnanců.

(ANO) Více než 70 zaměstnanců – 1 bod

(NE) Méně než 70 zaměstnanců – 0 bodů

2. Využívá Vaše společnost více než 50 mobilních zařízení?

Počet 50 zařízení mi dle mého názoru naznačí, že je dostatečný k tomu, aby se MDM řešení mohlo nasadit. Odpověď, která bude hodnocena negativně (0 bodů), bude počet zařízení menší než 50. Řízení mobilních zařízení má smysl i u menších firem s přibližným počtem zařízení kolem padesáti. V praxi je reálné do takovéto firmy MDM nasadit za využití Cloudu. Společnost bude tedy hradit poplatky za každé spravované zařízení.[7]

(ANO) Více než 50 mobilních zařízení vyžadujících správu – 1 bod

[7] http://www.techrepublic.com/blog/apple-in-the-enterprise/mdm-platforms-are-a-must-even-for-small-businesses/

(NE) Méně než 50 mobilních zařízení vyžadujících správu – 0 bodů

3. Umožňujete zaměstnancům používat soukromá zařízení pro pracovní účely (BYOD)?

Tato otázka jasně ukazuje, zda při nasazování MDM ve společnosti musíme počítat také s faktem, že zaměstnanci budou využívat vlastní zařízení pro pracovní účely. To je samozřejmě varianta, která nepatrně komplikovanější, protože je nutné oddělovat osobní a firemní data na zařízení a celkově celou bezpečnostní politiku navrhnout tak, aby uživatel byl co nejméně limitován při využívání přístroje. Kladnou odpověď zde tedy hodnotím 2 body do celkového součtu, protože pokud společnost se zájmem o MDM bude trend BYOD podporovat, správa mobilních zařízení by byla velice výhodná. Více v kapitole 5.

Tato otázka je hodnocena 2 body, protože jediné efektivní řešení, jak spravovat početnou skupinu zařízení, která jsou v osobním vlastnictví, je nasazení MDM.

(ANO) Pokud BYOD podporujete – 2 body

(NE) Pokud neumožňujete zaměstnancům využívat vlastní zařízení – 0 bodů

4. Plánujete v blízké budoucnosti (do 3 let) ve Vaší společnosti využívat více mobilních zařízení?

Každá společnost, která uvažuje nad tím, že nasadí MDM, by měla mít plán alespoň na následující tři roky. V plánu by měl být zvážen budoucí vliv mobilních zařízení na fungování společnosti. Pokud společnost plánuje koupi nových zařízení, je třeba uvažovat nad tím, jak dlouho budou moci být tato zařízení spravována pomocí MDM. Dále je třeba vhodně zvolit operační systém, který bude na zařízeních nasazen a zvážit zda vybrané MDM řešení pro něj nabízí všechny požadované funkcionality.

Tato otázka logicky navazuje na č. 1, č. 2 a č. 3. Pokud společnost plánuje nákup nových zařízení, bude také třeba je spravovat. Důležité je také, jestli firma zařízení nakoupí, nebo osloví zaměstnance a ti si budou moci přinést svá chytrá zařízení, která ovšem budou muset respektovat určité firemní politiky.

(ANO) Pokud neplánujete využívat větší počet mobilních zařízení – 0 bodů

(NE) Pokud plánujete využívat větší počet mobilních zařízení – 1 bod

5. Potýkáte se s častými ztrátami firemních mobilních zařízení?

Konkrétní dotaz, který má za úkol zjistit, zda společnost trápí větší počet ztracených zařízení, na kterých byla uložená korporátní data. Pokud jsou data citlivá, může se jednat o nepříjemnou situaci bez možnosti vzdáleného smazání. Více v kapitole 7.3.

Tato otázka je hodnocena 2 body, protože přímo vystihuje jeden ze tří pilířů kapitoly 8. Jedná se tedy o podstatnou funkci celého MDM softwaru.

(ANO) Pokud se potýkáte s častými ztrátami zařízení - 1 bod

(NE) Pokud se nepotýkáte s častými ztrátami zařízení – 0 bodů

6. Máte ve Vaší společnosti nezanedbatelnou (dle vlastního uvážení) skupinu zaměstnanců, kteří pracují převážně na cestách a v zahraničí?

Vedení společnosti by mělo samo zvážit, jestli počet zaměstnanců, kteří často cestují, nebo pracují mimo firemní síť je natolik vysoký, že by bylo výhodné spravovat jejich zařízení pomocí MDM. Odpověď na tuto otázku bude možná vyžadovat spolupráci s IT oddělením, které má přehled o tom, jak časově náročné je spravovat zařízení těchto uživatelů bez možnosti využití MDM.

Kladnou odpověď zde hodnotím 2 body z důvodů, že správa mobilních zařízení uživatelů, kteří často cestují, je spíše nutností, než malým usnadněním. Tito uživatelé vyžadují speciální péči a vzdálená správa jejich zařízení je prakticky jedinou možností, jak poskytovat těmto zaměstnancům určitou podporu.

(ANO) Pokud ve Vaší společnosti takováto skupina existuje – 2 body

(NE) Pokud ve Vaší společnosti takováto skupina není – 0 bodů

7. Potřebujete ve Vaší společnosti hromadně upravovat tarifní plány na mobilních zařízeních?

Otázka navazuje na předchozí, dá se předpokládat, že pokud společnost má mnoho zaměstnanců na cestách, bude potřeba kontrolovat i zpoplatněné služby na jejich zařízeních. Není to ovšem pravidlem. Tarifní plány mohou být upravovány i zaměstnancům, kterým společnost přiřadila pracovní zařízení. Těm poté hradí určité množství zpoplatněných služeb.

(ANO) Pokud je pro Vás řízení tarifních plánů a řízení objemů přenesených dat důležité – 1 bod

(NE) Pokud řízení tarifních plánů a objemů přenesených dat nepovažujete za důležité – 0 bodů

8. Potřebujete ve Vaší společnosti umožnit nezanedbatelné (dle vlastního uvážení) skupině zaměstnanců přístup k firemním datům pomocí Virtual Private Network (VPN)?

Jedná se o další z menších ukazatelů toho, že nasazení MDM řešení pro Vás má smysl. Samotné nastavení VPN není až tak složité, ale jedná se především o to, kolik zařízení je takto třeba nakonfigurovat. Může se jednat o naprostou většinu, nebo pouze o malou skupinu lidí. Jako vždy, při vysokém počtu zařízení, je výhodné využít MDM řešení, které umožní dle nakonfigurovaných profilů nastavit například i nově zakoupené zařízení, které ještě není přidělené žádnému zaměstnanci.

(ANO) Pokud ve Vaší společnosti často využíváte VPN pro přístup ke korporátním datům – 1 bod

(NE) Pokud VPN ve Vaší společnosti nevyužíváte – 0 bodů

9. Chtěli byste Vašim zaměstnancům omezit určité internetové služby v rámci zvýšení efektivity práce na firemních zařízeních?

Pokud dle statistik navštěvovaných webových stránek ve Vaší společnosti usoudíte, že zaměstnanci příliš často navštěvují sociální sítě, nebo jakékoli jiné weby, které nejsou přímo spojené s jejich prací, je vhodné jim některé weby zakázat. V korporátní síti je toho možno docílit pomocí vhodné konfigurace proxy serveru společnosti.

Pracovní zařízení, která zaměstnanci užívají i mimo firemní síť a nejsou v jejich osobním vlastnictví, jsou ale po připojení k jiné než firemní síti opět funkční bez omezení. Pokud společnost cítí potřebu zamezit jakémukoli nevyžádanému využívání firemního zařízení, dá se pomocí MDM řešení nastavit také web filtr, který bude zamezovat přístupu na weby, na které se zaměstnanec připojuje i z jiné, než korporátní sítě a které jsou označeny správcem jako nevyžádané.

(ANO) Pokud byste chtěli omezit firemní zařízení i mimo korporátní síť – 1 bod

(NE) Pokud tuto možnost nevyužijete – 0 bodů

10. Využívá většina zaměstnanců aplikace, které byly navrženy speciálně pro Vaši společnost, nebo aplikace, které nejsou veřejně dostupné?

Mnoho společností si pro zjednodušení interních procesů buď sama navrhuje, nebo nechává navrhnout speciální software. Může se jednat o jednoduchý software výkazu odpracovaných hodin, docházkový systém, nebo software pro rezervování obědů. Dále se může jednat o sofistikovanější software, který si například mohou vyvíjet společnosti, které podnikají přímo v odvětví programování softwaru.

V tom případě by se společnosti vyplatilo vytvořit aplikační obchod s vlastními aplikacemi, ze kterého by MDM software sám identifikoval, které aplikace jsou potřebné pro konkrétního

uživatele, a automaticky je nainstaloval na všechna spravovaná zařízení. V obchodě mohou být také umístěný aplikace z veřejného aplikačního obchodu, které je možné instalovat.

Pokud tedy bude odpověď kladná, dá se předpokládat, že se jedná o případ, kdy by nasazení MDM řešení poskytlo jisté výhody. Více v kapitole 7.2.2.

(ANO) Pokud ve Vaší společnost zmíněné aplikace hojně využíváte – 1 bod

(NE) Pokud tyto aplikace nevyužíváte – 0 bodů

11.2 Část pro zaměstnance (uživatele)

11. Jsou zaměstnanci schopni učinit ústupky, které se budou týkat jejich soukromí v případě, že zařízení budou spravována pomocí MDM softwaru?

Otázka, která má za úkol zhodnotit, zdali jsou zaměstnanci ochotni přijmout tato omezení v zájmu jejich většího pohodlí při správě a konfiguraci mobilních zařízení. Je důležité, že informace, které mohou správci o zařízeních vyčíst, jsou samozřejmě chráněné a nebudou nijak zneužity. Slouží především pro usnadnění práce IT správců. Více v kapitole 6.

(ANO) Pokud jsou zaměstnanci ochotni učinit menší ústupky – 1 bod

(NE) Pokud mají zaměstnanci obavy z větší kontroly nad jejich zařízeními – 0 bodů

12. Jsou zaměstnanci spokojeni s přidělenými firemními zařízeními?

V případě, že zaměstnanci nejsou spokojení s přidělenými zařízeními, je možné, že častěji využívají pro práci svá osobní zařízení, která zřejmě poskytují lepší komfort. Tím se ale zvyšuje riziko, že se firemní data budou stěhovat na uživatelská zařízení, která nespadají pod žádnou bezpečnostní politiku.

V tomto případě se dá očekávat, že by firma měla zareagovat nákupem vyhovujících zařízení, nebo umožnit zaměstnancům, aby do zaměstnání nosili svá zařízení, na která by se v budoucnu nasadil MDM software. Více v kapitole 5, aneb problematika trendu Bring Your Own Device.

(ANO) Pokud zaměstnanci nejsou spokojeni s firemními zařízeními – 1 bod

(NE) Pokud zaměstnancům firemní zařízení dostačují – 0 bodů

13. Vzrůstá zájem zaměstnanců využívat mobilních zařízení (vlastních i firemních)?

Zvláště pokud se jedná o společnost, ve které se příliš neholduje správě mobilních zařízení, ale uživatelé by uvítali, kdyby mohli využívat svá zařízení, nebo kdyby jim firma nějaké přidělila, je na místě zvážit budoucí využití MDM řešení.

Tlak uživatelů většinou vyústí v to, že vedení společnosti bude muset dříve, či později začít řešit otázku, jak spravovat větší počet mobilních zařízení a to ať už těch, které sama nakoupila, nebo zařízení osobních.

(ANO) Pokud zájem o mobilní zařízení vzrůstá – 1 bod

(NE) Pokud zájem o mobilní zařízení stagnuje, nebo dokonce klesá – 0 bodů

14. Jsou zaměstnanci často nuceni kontaktovat IT oddělení kvůli nastavením Wi-Fi sítí, přístupu k e-mailu, kalendáři a firemním datům?

Pokud jsou uživatelé často limitováni špatným nastavením mobilních zařízení, které mohou například převzít po zaměstnanci, který ve společnosti už nepracuje, může se jednat o problém, který zbytečně zatěžuje IT oddělení korporace.

To je poté nuceno řešit mnoho standardních problémů, či obvyklých konfigurací. Snižuje to jak produktivitu zaměstnanců, tak pracovníků IT oddělení.

(ANO) Pokud zaměstnanci s funkčností svých zařízení spokojeni nejsou a zařízení neposkytují kvůli těmto problémům očekávanou využitelnost, nebo mobilitu (lze také konzultovat s IT oddělením) – 1 bod

(NE) Pokud jsou zaměstnanci spokojeni s konfigurací svých zařízení a nepozorují žádné časté problémy (lze také konzultovat s IT oddělením) – 0 bodů

15. Využívají zaměstnanci firemní zařízení často také k osobním účelům?

Jestliže jsou firemní zařízení často využívána i k osobním účelům, jednoduše proto, že zaměstnanec žádné lepší zařízení nevlastní, bylo by vhodné konfigurovat jej tak, aby tento provoz nijak neohrožoval data společnosti a neomezoval samotného zaměstnance.

(ANO) Pokud jsou firemní zařízení často využívána k osobním účelům – 1 bod

(NE) Pokud zařízení slouží především pro pracovní účely a je k tomu i uzpůsobeno konkrétními nastaveními – 0 bodů

11.3 Část pro IT oddělení

16. Chtěli byste nově zakoupená zařízení snadno konfigurovat podle předem definovaných bezpečnostních politik?

Pokud Vaše společnost hojně využívá mobilní zařízení a zároveň je pořizuje a poté přiděluje zaměstnancům, je výhodné tato nová zařízení hromadně konfigurovat dle základních bezpečnostních politik. Více v kapitole 7.2.

(ANO) Pokud byste tuto možnost uvítali – 1 bod

(NE) Pokud o ni nemáte zájem – 0 bodů

17. Chtěli byste zjednodušit proces vymazání firemních dat ze zařízení, které patřilo zaměstnanci, jenž nyní z firmy odchází?

V mnohých případech, kdy zaměstnanec ukončí pracovní poměr ve společnosti, si s sebou odnáší i mobilní zařízení, které mu patří, ale obsahuje mnoho citlivých firemních dat. Je proto velmi doporučeno mít možnost vymazat firemní data i ze zařízení, která se nemohou fyzicky dostat do rukou IT správců.

To samé platí i pro zařízení vlastněná společnosti. Celý proces obnovení zařízení do výchozího nastavení, které je definováno IT oddělením, je tím pádem mnohem rychlejší a zvyšuje efektivitu přiřazování zařízení dalším čekajícím zaměstnancům. Více v kapitole 7.3.

(ANO) Pokud byste chtěli zjednodušit proces vzdáleného vymazání firemních dat ze zařízení, které již nadále nebude přítomno ve firemní síti – 1 bod

(NE) Pokud o tuto možnost nejevíte zájem – 0 bodů

18. Chcete zvýšit kontrolu nad tím, jak zaměstnanci využívají svá mobilní zařízení?

Je pro Vaše IT oddělení klíčové sledovat, jakým způsobem uživatelé využívají svá zařízení pro práci a na základě toho poté upravovat jednotlivé uživatelské profily s předdefinovanými konfiguracemi?

(ANO) Pokud chcete zvýšit kontrolu nad spravovanými zařízeními – 1 bod

(NE) Pokud nechcete kontrolu nad spravovanými zařízeními zvýšit – 0 bodů

19. Jsou citlivá data Vaší společnosti často uchovávána právě na mobilních zařízeních zaměstnanců?

Pokud jste vypozorovali, že zaměstnanci mnoho citlivých firemních dat ukládají právě na mobilní zařízení, je vhodné uvažovat například o šifrování interní a externí paměti. V tom případě by se jako vhodné řešení jevilo nasazení MDM, které za pomoci kontejnerizace zabezpečuje datové toky a také uložená data, která není bez znalosti bezpečnostních hesel možno dešifrovat.

(ANO) Pokud zaměstnanci na mobilních zařízeních často ukládají citlivá data společnosti – 1 bod

(NE) Pokud zaměstnanci citlivá data na mobilní zařízení nepřesouvají – 0 bodů

20. Chcete mít větší kontrolu nad tím, jaké aplikace budou moci zaměstnanci instalovat?

Jak již bylo řešeno dříve, mnoho aplikací může narušit křehký ekosystém bezpečnostních politik aplikovaných ve společnosti. Proto je důležité mít možnost kontrolovat, která zařízení tyto politiky nerespektují a dle toho je konfigurovat. Více v kapitole 7.2.9.

(ANO) Pokud byste uvítali možnost hromadné kontroly instalovaných aplikací – 1 bod

(NE) Pokud kontrola instalovaných aplikací pro vás není důležitá – 0 bodů

21. Chtěli byste zaměstnancům vytvořit firemní aplikační obchod a usnadnit jim tak instalování důležitých aplikací?

V mnohých případech je pro uživatele zbytečně složité, aby si na internetu sami vyhledávali doporučené aplikace a mnohdy tápali, jestli jsou to skutečně ony. Pokud je IT oddělení zatíženo častými dotazy na to, kde doporučené aplikace stáhnout, nebo vyskytují-li se jiné problémy s tímto spojené, je vhodné přemýšlet o firemním aplikačním obchodu. MDM řešení takovou možnost nabízí a zcela jistě se jedná o zjednodušení správy aplikací pro zaměstnance. Více v kapitole 7.2.2.

(ANO) Pokud cítíte potřebu vytvořit interní aplikační obchod – 1 bod

(NE) Pokud aplikační obchod vytvářet nechcete – 0 bodů

22. Má Vaše společnost potřebnou infrastrukturu pro nasazení MDM na Vaše servery?

- Pokud ne, jste obeznámeni s variantou nasazení MDM v Cloudu?

Vlastní Vaše společnost dostatečné hardwarové vybavení k tomu, aby bylo možno nasadit MDM tzv. On Premise (řešení, kdy se software nasadí na hardware, který se fyzicky nachází v budově společnosti)?

Pokud tomu tak není, je IT vedení obeznámeno s řešením, kdy se využívá Cloudu, jako hostitelského serveru a aplikace je poté dostupná přes běžné webové rozhraní? Více v kapitole 10.3.

(ANO) Pokud vlastního potřebnou infrastrukturu – 1 bod

(NE) Pokud dostatečnou infrastrukturu nevlastníte

- *(ANO) Pokud jste obeznámeni s Cloudovým řešením – 1 bod*
- *(NE) Pokud o řešení s nasazením v Cloudu nemáte žádné informace - 0 bodů*

23. Je Vaše IT oddělení natolik zkušené, aby zvládlo nasazení Mobile Device Managementu?

Je IT personál natolik zkušený, že zvládne nasazení a počáteční konfiguraci zcela sám?

Pokud ne, je důležité kontaktovat společnost, jejíž MDM řešení nasazujeme a požádat o podporu při nasazení a případné integraci s existujícími řešeními (např. Active Directory). Více v kapitole 10.3.

(ANO) Pokud máme zkušené IT oddělení – 1 bod

(NE) Pokud IT oddělení samo nezvládne nasazení ani integraci s existujícími řešeními ve firme – 0 bodů

24. Víte, jaké operační systémy pracují na mobilních zařízeních ve Vaší společnosti?

Je důležité mít přehled o operačních systémech aktuálně využívaných mobilních zařízení. Mnoho MDM řešení totiž nabízí určité funkcionality například pouze pro operační systém iOS, nebo Android. Je pak důležité zjistit, zda vámi požadovaná funkce je kompatibilní s operačními systémy ve Vaší společnosti.

(ANO) Pokud máte dobrý přehled o využívaných operačních systémech – 1 bod

(NE) Pokud nemáte přehled o tom, jaké operační systémy jsou využívány ve Vaší společnosti – 0 bodů

12 Vyhodnocení průvodce

12.1 Obecná pravidla

Za každou kladnou odpověď v průvodci je možno získat 1, nebo 2 body. Záporná odpověď je hodnocena 0 body. Pokud dotazovaný nezná odpověď na otázku, bude mu přidělen -1 bod. Priority jednotlivých otázek jsou vysvětleny v kapitole 11, kde je každá z otázek podrobně vysvětlena a jsou jí přiděleny odpovídající body.

Po vyplnění průvodce je tedy možné získat maximálně 26 bodů. Dosáhnout lze maximálně 12 bodů z části pro vedení společnosti, 5 bodů z části pro zaměstnance (uživatele) a 9 bodů z části pro IT oddělení.

Každá část průvodce je vyhodnocena zvlášť a poté jsou sečteny body. V případě, že dosáhnete dostatečného počtu bodů pro nasazení MDM řešení, je zde možnost, že společnost jako celek bude přesto mít zásadní nedostatky v jedné ze tří částí průvodce. Může se jednat o situaci, kdy společnost splní požadavky pro nasazení MDM řešení, ale v části pro IT oddělení získá pouze 2 body z 9 možných. V tomto okamžiku je na společnosti, aby sama zhodnotila, jestli jsou nedostatky v IT oddělení řešitelné. Pokud je společnost sama vyřešit nedokáže, je nevhodné, aby se v budoucnu pokoušela MDM řešení nasadit.

Proto je důležité sledovat body získané v jednotlivých částech průvodce. Není možné, aby dotazovaná společnost získala 0 bodů z jakékoli části průvodce. Pokud se tak stane, bude vyhodnocen jako nevhodný pro nasazení MDM.

Dle výsledků v jednotlivých částech průvodce je důležité zmapovat, kde má společnost jako celek stále nedostatky, které by mohly bránit nasazení MDM. Zvýšené pozornosti je tedy třeba v situaci, kdy dotazovaná společnost získá 12 – 17 bodů a nelze u ní jednoznačně doporučit nasazení. V této situaci, kdy je společnost takzvaně hraniční, je třeba zjistit, v jaké části bylo získáno méně než 50% možných bodů a pečlivě zvážit, zda i v takovém případě MDM nasadit.

Otázky, na které neznáte odpověď, jsou hodnoceny -1 bodem.

Dále jsou 0 body hodnoceny všechny případy, kdy není možné uspokojivě odpovědět, kvůli zachování logičnosti průvodce.

Příklad:

Umožňujete zaměstnancům používat soukromá zařízení pro pracovní účely (BYOD)?

- *ANO*

Jsou zaměstnanci spokojeni s přidělenými firemními zařízeními?

- *Nelze jednoznačně odpovědět*

Pokud totiž ve společnosti naprostá většina zaměstnanců využívá vlastních zařízení, není možné považovat spokojenost několika jedinců, kteří mohou firemní zařízení využívat, za objektivní. V některých případech takováto skupina ani nemusí existovat, protože firma nikdy žádná mobilní zařízení pro své zaměstnance nenakoupila.

Následující tabulka přehledně zobrazuje jednotlivá doporučení, která budou dle bodového zisku společnostem po vyhodnocení průvodce přidělena.

Výsledné kategorie dle dosažených bodů			
Výsledné hodnocení	Lze doporučit nasazení MDM	Nasazení MDM nelze jednoznačně doporučit	Nasazení MDM není doporučeno
Body	18 - 26	12 - 17	0 - 11

12.2 Nasazení MDM je doporučeno

Aby průvodce mohl být vyhodnocen kladně (doporučil nasazení MDM), musí být dosaženo alespoň 7 bodů z části pro IT oddělení, 3 bodů z části pro uživatele a 8 bodů z části pro vedení společnosti. Tato hranice vychází z kapitoly 7. Není možné nasazení MDM 100% doporučit s nižším počtem získaných bodů, jelikož při větší bodové ztrátě se setkáváme s narušením základních pilířů MDM. Tyto body v součtu tedy stanovují spodní hranici k tomu, aby bylo nasazení MDM doporučeno.

Z toho vyplývá, že 18 – 26 bodů je indikátor, že Vaše firma je vhodný kandidát pro nasazení Mobile Device Management řešení.

12.3 Nasazení MDM nelze jednoznačně doporučit

Pokud bude v průvodci dosaženo alespoň 4 bodů z části pro IT oddělení, 2 bodů z části pro uživatele a 6 bodů z části pro vedení společnosti, bude výsledné hodnocení takové, že

nasazení MDM nelze spolehlivě doporučit. Je důležité poté sledovat, ve kterých částech průvodce bylo získáno méně než 50% bodů. V této situaci se dá očekávat, že více než 1/6 funkcí MDM softwaru nebude vůbec využita. Protože se dotazuji na nutné funkce MDM softwaru, považuji toto číslo za vysoké. Dále je nutno přihlídnout k tomu, že jedna dotazovaná skupina zaměstnanců nasazení MDM spíše nevyžaduje, což je také důležité zvážit.

Nasazení MDM řešení tedy nelze jednoznačně doporučit při zisku 12 – 17 bodů.

V tomto případě se však s touto odpovědí nespokojím a na základě vyplněného průvodce vyhodnotím, zda se společnost blíží spíše k tomu, že nebude vhodným kandidátem, či naopak. Toto rozhodnutí bude individuální u každé zkoumané společnost a nelze jej popsat všeobecně funkčním návodem. V zásadě se jedná o realistické zvážení toho, jaké funkce MDM by společnost reálně využila. Pokud se tyto požadavky dají splnit jinou a efektivnější cestou, není nutné nasazovat tak komplexní řešení jako MDM software. Příklad tohoto rozhodování je uveden v kapitole 14.

12.4 Nasazení není doporučeno

Pokud bude v průvodci dosaženo 0 - 11 bodů, dá se s velkou pravděpodobností říci, že společnost není na nasazení MDM vhodně připravena. Prakticky se jedná o to, že zaměstnanci nemusí mít žádný zájem na tom, aby využívali firemní chytrá zařízení a pokud je jim umožněno pracovat s osobními zařízeními, je pravděpodobné, že se nechtějí vzdát soukromí, které jim jejich osobní zařízení poskytuje. Dále se může jednat o IT oddělení, které nemá dostatečné zkušenost se správou mobilních zařízení, disponuje pouze omezenou infrastrukturou a v poslední řadě ani není nadměrně vytíženo správou uživatelských zařízení. Posledním faktorem tak může být společnost, která nepotřebuje pro své zaměstnance přístupy k datům pomocí VPN, nemá větší počet uživatelů, kteří pracují mimo sídlo společnosti, nebo jednoduše nezaměstnává ani stanovený limit 70 zaměstnanců.

13 Testování průvodce

V této části práce využiji mnou vytvořeného průvodce k tomu, aby mi pomohl rozhodnout zda MDM nasadit do tří smyšlených společností. Společnosti budou vybrány z odlišného oboru podnikání. Očekávám, že každá ze tří společností bude vyhovovat právě jednomu z mnou definovaných výstupů průvodce. Mnou vytvořené firmy mají vzor v reálných společnostech, ve kterých pracují moji rodinní příslušníci, nebo známí.

14 Společnost A

Společnost A se specializuje na návrh a implementaci firemních aplikací. Má široký záběr realizovaných řešení od čistě databázových a backend systémů až po aplikace pro týmovou spolupráci. Aplikace jsou vyvíjeny za pomoci technologií Microsoft .NET a Python. Dále společnost vyvíjí mobilní webové aplikace, které je vyvíjeny za pomoci jQuery Mobile a AngularJS.

Společnost má 100 zaměstnanců, z nichž naprostá většina jsou programátoři, kteří pracují v sídle společnosti. Zaměstnanci ve společnosti využívají osobní mobilní zařízení.

Ze strany zaměstnanců není vyvíjen tlak na větší využívání mobilních zařízení, protože samotná společnost je v tomto směru prakticky nijak neomezuje. Stále více uživatelů však svá mobilní zařízení používá k práci. Samotní uživatelé mají dostatečné znalosti, aby svá zařízení samostatně spravovali, nebo řešili obvyklé problémy. Uvítali by však, kdyby všechny mobilní aplikace, které jejich společnost doporučuje využívat, byly dostupné z jednoho místa.

Společnost využívá nejméně 6 interních aplikací, které si sama vyvinula, protože se pohybuje v oboru a dalších 5 aplikací doporučuje svým zaměstnancům z veřejného obchodu s aplikacemi. Dále by společnost ocenila možnost omezit určité webové služby na několika málo firemních zařízeních, které zaměstnancům pořídila.

Samotní vývojáři využívají pro komunikaci především firemní e-mail a většina citlivých dat je tak uložena na počítačích, které jsou v sídle společnosti. Ostatní informace jako jsou například bugy softwaru, měsíční sprinty, nebo přímo různé verze zdrojového kódu jsou uchovávány na serveru, ke kterému se přistupuje pomocí TFS.

V případě nasazení MDM by se naprostá většina zaměstnanců nikterak neobávala o narušení svého soukromí.

14.1 Očekávané výsledky

Společnost A jsem definoval přibližně tak, aby po vyhodnocení průvodce odpovídala kategorii, ve které nasazení MDM nelze jednoznačně doporučit. Už při vytváření profilu společnosti, jsem si uvědomoval, že pro zaměstnance nehrají mobilní zařízení až takovou roli. Jedná se o společnost, která vyvíjí software, tudíž 80% - 90% pracovních záležitostí bude řešeno na firemních počítačích, na kterých vývojáři programují. Zbylých 10% může tvořit management společnosti, u kterého se může znatelně projevit častější využívání chytrých telefonů a všech funkcí, které nabízí.

Předpokládám tedy, že po sečtení bodů z průvodce a bližším prozkoumáním otázek a odpovědí, bude společnost shledána nevhodnou pro nasazení MDM řešení.

14.2 Dotazník - Vedení společnosti

1. Má Vaše společnost více než 70 zaměstnanců?

- ***ANO –*** *Vyplývá přímo z textu.*

2. Využívá Vaše společnost více než 50 mobilních zařízení?

- ***ANO*** *– Vyplývá přímo z textu.*

3. Umožňujete zaměstnancům používat soukromá zařízení pro pracovní účely (BYOD)?

- ***ANO*** *– „Zaměstnanci ve společnosti využívají osobní mobilní zařízení.“*

4. Plánujete v blízké budoucnosti (do 3 let) ve Vaší společnosti využívat více mobilních zařízení?

- ***NE*** *– Není uvedeno, ale v profilu společnosti není výslovně zmíněno, že by se k tomuto kroku chystala. Zaměstnanci stále využívají svá mobilní zařízení. Jejich počet tedy neroste.*

5. Potýkáte se s častými ztrátami firemních mobilních zařízení?

- ***NE*** *– Tento problém v této společnosti není, protože zaměstnanci využívají svá zařízení.*

6. Máte ve Vaší společnosti nezanedbatelnou (dle vlastního uvážení) skupinu zaměstnanců, kteří pracují převážně na cestách a v zahraničí?

- ***NE*** *– 90% zaměstnanců jsou programátoři, kteří necestují.*

7. Potřebujete ve Vaší společnosti hromadně upravovat tarifní plány na mobilních zařízeních?

- ***NE*** *– Vyplývá mimo jiné z odpovědi na otázku č. 6.*

8. Potřebujete ve Vaší společnosti umožnit nezanedbatelné (dle vlastního uvážení) skupině zaměstnanců přístup k firemním datům pomocí Virtual Private Network (VPN)?

- ***NE*** *- Zaměstnanci nepotřebují přistupovat k firemním datům mimo sídlo společnosti.*

9. Chtěli byste Vašim zaměstnancům omezit určité internetové služby v rámci zvýšení efektivity práce na firemních zařízeních?

- ***ANO*** *– „Dále by společnost ocenila možnost omezit určité webové služby na několika málo firemních zařízeních, které zaměstnancům pořídila.“*

10. Využívá většina zaměstnanců aplikace, které byly navrženy speciálně pro Vaši společnost, nebo aplikace, které nejsou veřejně dostupné?

- ***ANO*** *– Vyplývá z textu.*

Získáno bodů: 6 z 12

14.3 Dotazník - Zaměstnanci (uživatelé)

11. Jsou zaměstnanci schopni učinit ústupky, které se budou týkat jejich soukromí v případě, že zařízení budou spravována pomocí MDM softwaru?

- ***ANO*** *– Vyplývá z textu.*

12. Jsou zaměstnanci spokojeni s přidělenými firemními zařízeními?

- ***Nelze odpovědět*** *– Skupina uživatelů, kteří pracují s firemními mobilními zařízeními je příliš malá na to, aby poskytla objektivní informaci. V textu navíc není o spokojenosti nic zmíněno.*

13. Vzrůstá zájem zaměstnanců využívat mobilních zařízení (vlastních i firemních)?

- ***ANO*** *– Zaměstnanci využívají stále více svých osobních mobilních zařízení.*

14. Jsou zaměstnanci často nuceni kontaktovat IT oddělení kvůli nastavením Wi-Fi sítí, přístupu k e-mailu, kalendáři a firemním datům?

- ***NE*** *– Jsou schopni řešit většinu nastavení samostatně.*

15. Využívají zaměstnanci firemní zařízení často také k osobním účelům?

- ***ANO*** *– Ano, z důvodu, že využívají vlastní zařízení.*

Získáno bodů: 3 z 5

14.4 Dotazník - IT oddělení

16. Chtěli byste nově zakoupená zařízení snadno konfigurovat podle předem definovaných bezpečnostních politik?

- ***NE*** *– V textu není zmíněno.*

17. Chtěli byste zjednodušit proces vymazání firemních dat ze zařízení, které patřilo zaměstnanci, jenž nyní z firmy odchází?

- ***NE*** *– V textu není zmíněno.*

18. Chcete zvýšit kontrolu nad tím, jak zaměstnanci využívají svá mobilní zařízení?

- ***NE*** *- V textu není zmíněno.*

19. Jsou citlivá data Vaší společnosti často uchovávána právě na mobilních zařízeních zaměstnanců?

- ***NE*** *– Nejsou. Veškerá citlivá data jsou uložena na stolních počítačích a firemních serverech.*

20. Chcete mít větší kontrolu nad tím, jaké aplikace budou moci zaměstnanci instalovat?

- ***NE*** *- Společnost využívání aplikací pouze doporučuje a navíc není uvedeno, že by chtěla spravovat i zařízení, která jsou v osobním vlastnictví zaměstnanců.*

21. Chtěli byste zaměstnancům vytvořit firemní aplikační obchod a usnadnit jim tak instalování důležitých aplikací?

- ***ANO*** *– Společnost by chtěla zpřehlednit a usnadnit instalaci doporučených aplikací.*

22. Má Vaše společnost potřebnou infrastrukturu pro nasazení MDM na Vaše servery?

    - Pokud ne, jste obeznámeni s variantou nasazení MDM v Cloudu?

- ***ANO*** *– Ve společnosti je k dispozici dostatečná infrastruktura.*

23. Je Vaše IT oddělení natolik zkušené, aby zvládlo nasazení Mobile Device Managementu?

- ***ANO*** *– Vyplývá z textu.*

24. Víte, jaké operační systémy pracují na mobilních zařízeních ve Vaší společnosti?

- ***ANO*** *– Vyplývá z textu.*

Získáno bodů: 4 z 9

Body získané v jednotlivých částech průvodce			
Vedení společnosti	Zaměstnanci (uživatelé)	IT oddělení	Celkem bodů
6	3	4	13

14.5 Doporučení

Dotazovaná společnost získala 13 bodů z 26 možných. Tím se zařadila do kategorie, kdy není možné jednoznačně doporučit, zda MDM nasadit, či nikoli. Zvláštní pozornost věnuji vyhodnocení průvodce pro IT oddělení, ve kterém bylo získáno méně než 50% možných bodů. Z otázek vyplývá, že IT oddělení je sice způsobilé, aby mohlo MDM spravovat a také má k dispozici dostatečnou infrastrukturu. Ale žádné výhody pro IT oddělení se zavedením MDM neplyne. Správci nemají žádné speciální požadavky, nepřijdou si zbytečně vytíženi dotazy zaměstnanců a prakticky nijak nejeví zájem o pokročilé funkce Mobile Device Managementu.

Zaměstnanci samotní nemají potřebu často kontaktovat IT oddělení, kvůli běžným nastavením (Wi-Fi, VPN, hesla, apod.) a v zásadě by neměli výhrady, pokud by se mělo MDM nasadit. Jsou tedy se svými zařízeními spokojeni a mohou je efektivně využívat.

Vedení společnosti zodpovědělo, že by mělo zájem o omezení určitých webových služeb, které zaměstnanci v pracovní době využívají. Tento problém lze ovšem samostatně řešit i jinak, než nasazením MDM řešení (například omezeními na proxy serveru společnosti). Dále vedení uvedlo, že zaměstnanci využívají několik interních aplikací. IT oddělení ovšem odpovědělo, že necítí potřebu vytvořit interní aplikační obchod a nabídnout tak zaměstnancům všechny aplikace na jednom místě. Tudíž s instalacemi daných aplikací zřejmě nevznikají žádné problémy.

Nejslabšími články jsou v tomto případě vedení společnosti a IT oddělení. Ti odpověděli kladně pouze na malou část otázek, které ve výsledku nesignalizovaly nutnost zavedení MDM řešení. Zaměstnanci s případným zavedením MDM souhlasili.

V tomto případě by ale bylo velmi neplodné nepřiklonit se k jedné z konkrétních variant. Tedy buď k variantě, kdy lze nasazení MDM doporučit, nebo k variantě, kdy doporučit nelze. Z profilu společnosti také vyplývá, že uživatelé jsou dostatečně technicky zdatní, aby své

problémy řešili samostatně. IT oddělení má sice dostatečnou infrastrukturu, naproti tomu ale není vytíženo správou mobilních zařízení. Samotné vedení společnosti by uvítalo spíše klasická firemní nastavení, která lze řešit i jinou metodou než nasazením MDM. Požadavky jsou podrobněji rozepsány výše.

Z tohoto důvodu se přikláním k variantě, kdy nasazení MDM nedoporučuji, ačkoli po vyhodnocení průvodce se tato společnost nacházela v situaci, kdy nešlo jednoznačně doporučit konkrétní řešení. Mohu tedy tvrdit, že má hypotéza byla správná, ovšem při zvážení odpovědí by nebylo nasazení MDM pro společnost významným přínosem.

Výsledné kategorie dle dosažených bodů s doporučeným řešením			
Výsledné hodnocení	Lze doporučit nasazení MDM	Nasazení MDM nelze jednoznačně doporučit	Nasazení MDM není doporučeno
Body	18 - 26	12 - 17	0 - 11

15 Společnost B

Společnost B se zaměřuje na finanční poradenství a vedení účetnictví malých a středně velkých firem. Má mnoho klientů po celé České republice a zaměstnanci jsou často nuceni za nimi cestovat.

Společnost zaměstnává 50 zaměstnanců, z nichž každý využívá firemní chytrý telefon, či tablet. Společnost ovšem zaměstnancům umožňuje využívat také vlastní mobilní zařízení. V posledním roce ovšem došlo k odcizení, či ztrátě 8 mobilních zařízení.

Vedení společnosti by ocenilo možnost lépe monitorovat služby využívané na firemních zařízeních. Zaměstnanci totiž využívají především chytré telefony ke kontaktování klientů. Vedení by tedy ocenilo lepší přehled o počtu provolaných minut, poslaných SMS a objemu přenesených dat.

Ze strany zaměstnanců tedy není vyvíjen tlak na využívání mobilních zařízení ve větší míře, protože aktuální situace ve firmě je nijak neomezuje. Samotní zaměstnanci nemají potřebné znalosti, aby si při komplikovanějších problémech s nastavením zařízení poradili sami. Je ale ovšem časté, že potřebují odbornou pomoc při problémy s přístupem k datům za využití VPN.

Společnost využívá 2 interní aplikace a další 4 aplikace jsou doporučeny využívat z veřejného aplikačního obchodu. Uživatelé by uvítali, kdyby byli všechny aplikace dostupné z jednoho zdroje.

Zaměstnanci na mobilních zařízeních často ukládají citlivá data. Jedná se především o osobní informace a telefonní čísla o klientech. Dále využívají sdílené kalendáře a pomocí VPN mají přístup k datům, která se fyzicky nacházejí v sídle společnosti. Tedy citlivá data o finanční situaci klientů. Je to jeden z důvodu, proč by se nebránili nasazení MDM i za cenu ztráty určité svobody při využívání zařízení, jelikož jsou si plně vědomi důležitosti zabezpečení těchto dat.

IT oddělení má finanční zdroje na pořízení dostačující infrastruktury v případě nutnosti nasazení MDM, ale nemá prakticky žádné zkušenosti se správou tohoto softwaru. IT oddělení je ovšem dobře obeznámeno s Cloudovým řešením.

15.1 Očekávané výsledky

Očekávám, že společnost B by se po vyhodnocení průvodce měla jevit jako vhodný kandidát pro nasazení MDM. Předpokládám tedy, že bodový součet mi dle tabulky naznačení, že nasazení MDM je vhodné.

Již při definici profilu společnosti, jsem tedy dbal na to, aby byla vhodným kandidátem pro nasazení MDM. Protože počet zaměstnanců jsem stanovil jako menší než 70, je jasné že se jedná spíše o firmu menší. Ta by skutečně mohla mít problémy s nasazením MDM On-Premise, protože neinvestuje zdaleka tolik financí do IT oddělení. Ve výsledku se nejedná ani o problém, ale spíše o nutnost vybrat vhodné řešení, které bude společnosti vyhovovat.

Předpokládám tedy, že po sečtení bodů z průvodce a bližším prozkoumáním odpovědí, ve kterých bylo odpovězeno záporně, dospěji k výsledku, že společnost je vhodným kandidátem pro nasazení Mobile Device Managementu.

15.2 Vedení společnosti

1. Má Vaše společnost více než 70 zaměstnanců?

- ***NE*** *– Vyplývá z textu.*

2. Využívá Vaše společnost více než 50 mobilních zařízení?

- ***NE*** *- Vyplývá z textu.*

3. Umožňujete zaměstnancům používat soukromá zařízení pro pracovní účely (BYOD)?

- ***ANO*** *- Vyplývá z textu.*

4. Plánujete v blízké budoucnosti (do 3 let) ve Vaší společnosti využívat více mobilních zařízení?

- ***NE*** *– Není výslovně zmíněno.*

5. Potýkáte se s častými ztrátami firemních mobilních zařízení?

- ***ANO*** *- Bylo ztraceno 8 zařízení během posledního roku.*

6. Máte ve Vaší společnosti nezanedbatelnou (dle vlastního uvážení) skupinu zaměstnanců, kteří pracují převážně na cestách a v zahraničí?

- ***ANO*** *– Téměř všichni zaměstnanci jsou nuceni více, či méně cestovat.*

7. Potřebujete ve Vaší společnosti hromadně upravovat tarifní plány na mobilních zařízeních?

- ***ANO*** *– Vzhledem k častému využívání zpoplatněných služeb, by to bylo vhodné.*

8. Potřebujete ve Vaší společnosti umožnit nezanedbatelné (dle vlastního uvážení) skupině zaměstnanců přístup k firemním datům pomocí Virtual Private Network (VPN)?

- ***ANO*** *- Vyplývá z textu.*

9. Chtěli byste Vašim zaměstnancům omezit určité internetové služby v rámci zvýšení efektivity práce na firemních zařízeních?

- ***NE*** *– Není zmíněno.*

10. Využívá většina zaměstnanců aplikace, které byly navrženy speciálně pro Vaši společnost, nebo aplikace, které nejsou veřejně dostupné?

- ***ANO*** *– Vyplývá z textu.*

Získáno bodů: 10 z 12

15.3 Zaměstnanci (uživatelé)

11. Jsou zaměstnanci schopni učinit ústupky, které se budou týkat jejich soukromí v případě, že zařízení budou spravována pomocí MDM softwaru?

- ***ANO*** *– Vyplývá z textu.*

12. Jsou zaměstnanci spokojeni s přidělenými firemními zařízeními?

- ***ANO*** *- Vyplývá z textu.*

13. Vzrůstá zájem zaměstnanců využívat mobilních zařízení (vlastních i firemních)?

- ***ANO*** *– Vyplývá z textu.*

14. Jsou zaměstnanci často nuceni kontaktovat IT oddělení kvůli nastavením Wi-Fi sítí, přístupu k e-mailu, kalendáři a firemním datům?

- ***ANO*** *- Především kvůli nastavení VPN.*

15. Využívají zaměstnanci firemní zařízení často také k osobním účelům?

- ***ANO*** *– Vyplývá z textu.*

Získáno bodů: 5 z 5

15.4 IT oddělení

16. Chtěli byste nově zakoupená zařízení snadno konfigurovat podle předem definovaných bezpečnostních politik?

- ***ANO*** *– IT oddělení by uvítalo vzdáleně mazat a konfigurovat zařízení.*

17. Chtěli byste zjednodušit proces vymazání firemních dat ze zařízení, které patřilo zaměstnanci, jenž nyní z firmy odchází?

- ***ANO*** *– Vyplývá z textu a zároveň z odpovědi na otázku č. 16.*

18. Chcete zvýšit kontrolu nad tím, jak zaměstnanci využívají svá mobilní zařízení?

- ***ANO*** *– Vyplývá z textu.*

19. Jsou citlivá data Vaší společnosti často uchovávána právě na mobilních zařízeních zaměstnanců?

- ***ANO*** *– Vyplývá z textu.*

20. Chcete mít větší kontrolu nad tím, jaké aplikace budou moci zaměstnanci instalovat?

- ***NE*** *– IT oddělení nevyžaduje zvýšenou kontrolu při instalaci aplikací.*

21. Chtěli byste zaměstnancům vytvořit firemní aplikační obchod a usnadnit jim tak instalování důležitých aplikací?

- ***ANO*** *– Vyplývá z textu.*

22. Má Vaše společnost potřebnou infrastrukturu pro nasazení MDM na Vaše servery?

    - Pokud ne, jste obeznámeni s variantou nasazení MDM v Cloudu?

- ***NE*** *- Vyplývá z textu.*
    - ***ANO*** *– Vyplývá z textu.*

23. Je Vaše IT oddělení natolik zkušené, aby zvládlo nasazení Mobile Device Managementu?

- ***NE*** *– Vyplývá z textu.*

24. Víte, jaké operační systémy pracují na mobilních zařízeních ve Vaší společnosti?

- ***ANO*** *- Vyplývá z textu.*

Získáno bodů: 7 z 9

Body získané v jednotlivých částech průvodce a jejich součet			
Vedení společnosti	Zaměstnanci (uživatelé)	IT oddělení	Celkem bodů
10	5	7	22

15.5 Doporučení

Dotazovaná společnost získala 22 bodů z 26 možných. Tím se řadí do kategorie, kdy můžu předběžně říci, že nasazení MDM je vhodné. V tomto případě je spíše nutné blíže prozkoumat otázky, ve kterých bylo odpovězeno záporně.

IT oddělení pouze nechce zvyšovat kontrolu nad tím, jaké aplikace uživatelé instalují. Zde se jedná pouze o jednu z mnoha důležitých funkcí, kterou by IT oddělení v tomto případě nevyužilo, což neklade žádné překážky nasazení MDM. Dalším problémem může být nezkušenost správců. Ti jsou však dobře informováni o způsobu nasazení MDM v Cloudu. V dnešní době všechny mnou zkoumaná MDM řešení nabízejí jak nasazení On-Premise, tak v Cloudu. Tato řešení jsou dle specifikace dodavatele naprosto totožná a nabízí stejné funkce.

Zaměstnanci nasazení MDM nekladou žádné překážky. Na všech 5 položek průvodce odpověděli kladně a můžu se tak přesunout k vyhodnocení třetí části.

Vedení společnost neplánuje nákup nových zařízení v následujících letech, což ovšem neznamená, že nasazení MDM, by v nynější situaci této společnosti nebylo nijak prospěšné. K zamyšlení vede pouze to, že zaměstnanců má společnost méně než 70 a mobilních zařízení je využíváno a spravováno méně než 50. Vzhledem k tomu, že nasazení MDM má smysl i pro menší společnosti, domnívám se, že to není až tak podstatný problém.

Pro menší společnosti je samozřejmě výhodnější využívat hostované služby, které jsou následně dostupné přes webové rozhraní. V tomto případě společnost platí pouze za zařízení,

která jsou přihlášena ke správě, což je v mnohých případech výhodnější, než investovat do hardwarové výbavy pro nasazení On-Premise.

V případě společnosti B, bych tedy dle celkového bodového součtu skutečně doporučil nasazení MDM. Na základě skutečnosti, že IT oddělení nemá dostatečnou infrastrukturu a firma má méně než 70 zaměstnanců, doporučuji nasazení v Cloudu.

Výsledné kategorie dle dosažených bodů s doporučeným řešením			
Výsledné hodnocení	Lze doporučit nasazení MDM	Nasazení MDM nelze jednoznačně doporučit	Nasazení MDM není doporučeno
Body	18 - 26	12 - 17	0 - 11

16 Společnost C

Společností C je městský archiv, ve kterém pracuje 40 zaměstnanců, jejichž hlavní náplní práce je zpracovávání a organizace historických dokumentů. Dále archiv poskytuje informace osobám, které si o ně zažádají. K těmto úkonům využívají především stolní počítače a notebooky poskytnuté archivem. V archivu je celkem 10 firemních chytrých telefonů. Ze strany zaměstnanců není kladen prakticky žádný tlak na větší využívání mobilních zařízení, protože téměř veškerá komunikace probíhá pomocí e-mailu. Ostatní záležitosti se řeší telefonicky přes zavedenou pevnou linku.

V rámci zvýšení efektivity práce má zaměstnavatel zájem na tom, aby bylo možné omezit určité webové služby. Většinou by se ale jednalo nanejvýš o přenosné počítače. Archiv ani v budoucnu neuvažuje o pořízení mobilních zařízení, jako jsou chytré telefony, nebo tablety. Zaměstnanci mohou pro pracovní účely, jako jsou čtení e-mailů a vyřizování služebních hovorů, využívat vlastní zařízení. Ty ale nijak nepodléhají speciální bezpečnostní politice archivu.

Pokud se jedná o notebooky a chytré telefony, zaměstnanci je běžně využívají i pro osobní účely. IT oddělení, má v tomto případě 3 zaměstnance, kteří se starají o bezpečný chod specializovaných programů a správu serverů. Správci mají dostatečný přehled o tom, jaké operační systémy pracují na zařízeních v archivu. IT oddělení nemá potřebnou infrastrukturu pro nasazení MDM přímo v archivu a správci nemají žádné zkušenosti s nasazením MDM.

Zároveň nejsou obeznámeni s nasazením MDM v Cloudu. IT oddělení by navíc uvítalo, kdyby mohlo mít větší přehled o využití všech využívaných zařízení.

16.1 Očekávané výsledky

Společnost C byla definována s cílem, aby se již od počátku profilovala jako společnost, která není vhodná pro nasazení MDM. Je to tedy typ společnosti, v tomto případě patřící do státního sektoru, která by potencionálu MDM jen stěží využila a již nyní v ní mobilní zařízení nabývají pouze podružné důležitosti.

V podrobnější definici společnosti je zřejmé, že nesplňuje většinu klíčových požadavků pro nasazení MDM. Je to zřejmé již z oboru, ve kterém daná společnost existuje. Činnost zaměstnanců prakticky nevyžaduje žádnou pokročilou správu mobilních zařízení a ani vedení společnosti nemá potřebu zařízení, která v naprosté většině patří zaměstnancům, nějakým způsobem kontrolovat, zabezpečovat, či omezovat.

Předpokládám tedy, že společnost nebude vhodným kandidátem pro nasazení MDM.

16.2 Vedení společnosti

1. Má Vaše společnost více než 70 zaměstnanců?

- ***ANO*** – *Vyplývá z textu.*

2. Využívá Vaše společnost více než 50 mobilních zařízení?

- ***ANO*** - *Vyplývá z textu.*

3. Umožňujete zaměstnancům používat soukromá zařízení pro pracovní účely (BYOD)?

- ***NE*** -

4. Plánujete v blízké budoucnosti (do 3 let) ve Vaší společnosti využívat více mobilních zařízení?

- ***NE*** – *Archiv ani nepodporuje koupě služebních mobilních zařízení.*

5. Potýkáte se s častými ztrátami firemních mobilních zařízení?

- ***NE*** – *Vyplývá z odpovědi na otázku č. 4.*

6. Máte ve Vaší společnosti nezanedbatelnou (dle vlastního uvážení) skupinu zaměstnanců, kteří pracují převážně na cestách a v zahraničí?

- ***NE*** *- Zaměstnanci pracují pouze z místa společnosti. Pro hovory využívají pevné linky.*

7. Potřebujete ve Vaší společnosti hromadně upravovat tarifní plány na mobilních zařízeních?

- ***NE*** *– Vyplývá z odpovědi na otázku č. 6.*

8. Potřebujete ve Vaší společnosti umožnit nezanedbatelné (dle vlastního uvážení) skupině zaměstnanců přístup k firemním datům pomocí Virtual Private Network (VPN)?

- ***NE*** *– Vyplývá z textu.*

9. Chtěli byste Vašim zaměstnancům omezit určité internetové služby v rámci zvýšení efektivity práce na firemních zařízeních?

- ***ANO*** *- Na konkrétně deseti firemních telefonech by vedení uvítalo omezení určitých webových služeb.*

10. Využívá většina zaměstnanců aplikace, které byly navrženy speciálně pro Vaši společnost, nebo aplikace, které nejsou veřejně dostupné?

- ***NE*** *– Společnost nemá speciálně navržené aplikace pro mobilní zařízení.*

Získáno bodů: 3 z 12

16.3 Zaměstnanci (uživatelé)

11. Jsou zaměstnanci schopni učinit ústupky, které se budou týkat jejich soukromí v případě, že zařízení budou spravována pomocí MDM softwaru?

- ***NE*** *– Vyplývá z textu.*

12. Jsou zaměstnanci spokojeni s přidělenými firemními zařízeními?

- ***ANO*** *– Nepatrná skupina, která tato zařízení využívá, ano.*

13. Vzrůstá zájem zaměstnanců využívat mobilních zařízení (vlastních i firemních)?

- ***NE*** *- Vyplývá z textu.*

14. Jsou zaměstnanci často nuceni kontaktovat IT oddělení kvůli nastavením Wi-Fi sítí, přístupu k e-mailu, kalendáři a firemním datům?

- ***NE*** *– Vyplývá z textu.*

15. Využívají zaměstnanci firemní zařízení často také k osobním účelům?

- ***ANO*** *– Pokud se jedná o firmou zakoupená mobilní zařízení, ano.*

Získáno bodů: 2 z 5

16.4 IT oddělení

16. Chtěli byste nově zakoupená zařízení snadno konfigurovat podle předem definovaných bezpečnostních politik?

- ***NE*** *- Vyplývá z textu. Navíc zde není žádný významný počet těchto zařízení.*

17. Chtěli byste zjednodušit proces vymazání firemních dat ze zařízení, které patřilo zaměstnanci, jenž nyní z firmy odchází?

- ***NE*** *– Pokud je takové zařízení při odchodu odevzdáváno, nemělo by obsahovat žádná citlivá firemní data.*

18. Chcete zvýšit kontrolu nad tím, jak zaměstnanci využívají svá mobilní zařízení?

- ***ANO*** *– Vyplývá z textu.*

19. Jsou citlivá data Vaší společnosti často uchovávána právě na mobilních zařízeních zaměstnanců?

- ***NE*** *- Vyplývá z textu.*

20. Chcete mít větší kontrolu nad tím, jaké aplikace budou moci zaměstnanci instalovat?

- ***NE*** *- Vyplývá z textu.*

21. Chtěli byste zaměstnancům vytvořit firemní aplikační obchod a usnadnit jim tak instalování důležitých aplikací?

- ***NE*** *– Archiv nemá žádné aplikace pro mobilní zařízení.*

22. Má Vaše společnost potřebnou infrastrukturu pro nasazení MDM na Vaše servery?

    - Pokud ne, jste obeznámeni s variantou nasazení MDM v Cloudu?

- ***NE*** *- IT oddělení nesplňuje požadavky pro nasazení MDM.*
    - ***NE*** *– Nemá dostatečné informace.*

23. Je Vaše IT oddělení natolik zkušené, aby zvládlo nasazení Mobile Device Managementu?

- ***NE*** *- Vyplývá z textu.*

24. Víte, jaké operační systémy pracují na mobilních zařízeních ve Vaší společnosti?

- ***ANO*** *– Správci mají o operačních systémech přehled.*

Získáno bodů: 2 z 9

Body získané v jednotlivých částech průvodce a jejich součet			
Vedení společnosti	Zaměstnanci (uživatelé)	IT oddělení	Celkem bodů
3	2	3	8

16.5 Doporučení

Dotazovaná společnost získala 8 bodů z 26 možných. Tím se řadí do kategorie, kdy je možné říci, že nasazení MDM je určitě nevhodné. V tomto případě je spíše vhodné se zaměřit na odpovědi v průvodci, které byly kladné a následně se pokusit společnosti alternativními cestami pomoci řešit problémy, které ji zřejmě přivedly k myšlence, že MDM by mohlo být vhodné řešení.

IT oddělení v této společnosti prakticky neexistuje. Nemá dostatečnou infrastrukturu ani zkušenosti a především nemá potřebu zavádět sofistikovaný software na řízení mobilních zařízení.

Zaměstnanci využívají svá mobilní zařízení a nikterak nevyvíjí tlak na vedení, aby byla nová zařízení kupována a přidělována zaměstnancům. Vedení společnosti nechce zaměstnance nijak omezovat ani zabezpečovat jejich zařízení.

Ani jedna ze tří dotazovaných skupin neodpověděla v průvodce uspokojivě a v případě společnosti C nedoporučuji nasazení MDM řešení. Z původního výsledku, kde se nasazení MDM nedalo jednoznačně určit, se tedy po zvážení důležitých aspektů přikláním k variantě, kdy nasazení MDM není doporučeno.

Výsledné kategorie dle dosažených bodů s doporučeným řešením			
Výsledné hodnocení	Lze doporučit nasazení MDM	Nasazení MDM nelze jednoznačně doporučit	Nasazení MDM není doporučeno
Body	18 - 26	12 - 17	0 - 11

17 Shrnutí

V praktické části této práce jsem sestavil průvodce, které byl realizován pomocí dotazníku. Ten měl za úkol pomoci při rozhodování, zda je vhodné nasadit do společnosti MDM řešení. Průvodce se řídí přesně stanovenými bodovými hranicemi. Je ovšem důležité jaká společnost tohoto průvodce vyhodnocuje, protože každá z dotazovaných firem může mít jiné preference na cílové dotazované skupiny. Nelze tedy obecně tvrdit, že pokud například IT oddělení a uživatelé nejsou připravení na tuto změnu, bude MDM zavedeno. Priority dané společnosti mohou být právě v potřebách vedení společnosti a to bude nakonec klíčovým ukazatelem pro zavedení MDM.

Mohu tedy konstatovat, že průvodce zohledňuje všechny dotazované skupiny ve stejné míře a pro prvotní vyhodnocení přínosu MDM do společnosti je určitě užitečný. Průvodce pomůže potencionálnímu zájemci o MDM uvědomit si, jaké důležité aspekty je třeba zohlednit, aby bylo nasazení výhodné.

MDM řešení jsou v současnosti prakticky jedinou možností, jak efektivně řídit velká množství mobilních zařízení. Využití nalezne MDM i v menších společnostech, jelikož cena za provozované služby klesá a je pravděpodobné, že i společnost, která má 20 zaměstnanců, by se zavedením MDM vyřešila mnohé problémy týkající se zabezpečení a vzdálené správy.

Další vývoj MDM produktů úzce souvisí s tím, jaké funkce přinesou nové verze operačních systému. A to především Android, iOS a Windows Phone, které jsou v současnosti nejrozšířenějšími operačními systémy využívanými na mobilních zařízeních. Na nové možnosti nastavení tak budou muset společnosti vyvíjející MDM software rychle reagovat, aby bylo možné mobilní zařízení dále efektivně spravovat.

18 Závěr

Hlavním cílem mé práce bylo vytvořit průvodce v podobě dotazníku, který by umožňoval zjednodušit rozhodování společnostem, které váhají nad zavedením MDM. Abych byl schopen tohoto průvodce sestavit, musel jsem nejprve zjistit důležitá fakta o Mobile Device Managementu a zmapovat, které funkce jsou nezbytné pro to, aby dané MDM řešení bylo efektivní a dobře využitelné. Z tohoto důvodu jsem se v teoretické části zabýval důležitými vlastnostmi MDM, abych si ujasnil, jaké vlastnosti MDM softwaru jsou nejpodstatnější.

Mohu konstatovat, že vytvořený průvodce prošel třemi testovacími společnostmi a výsledky, kterých jsem dosáhl, se shodovaly s mými očekáváními. Je ovšem důležité zdůraznit, že ne každá společnost bude klást stejné priority mezi dotazované skupiny zaměstnanců. Výsledky se tak v různých společnostech, dle upřednostňovaných dotazovaných skupin, mohou lišit.

Přínos této práce je především pro společnosti, které tápají v oblasti správy mobilních zařízení a uvažují o nasazení MDM. Dále má jistě podstatnou informační hodnotu pro každého člověka, který by se chtěl dozvědět více informací o správě mobilních zařízení. Všechny potřebné pojmy jsou srozumitelně vysvětleny a tak je práce vhodná i pro čtenáře, který s tématem nemá žádné zkušenosti.

Osobně jsem se při zpracovávání tématu dozvěděl nové informace o trendech ve správě mobilních zařízení, o výrobcích MDM softwaru a problémech při nasazování MDM řešení. Práce mi umožnila vytvořit si obraz toho, co bych měl od MDM očekávat a v jakých případech se vyplatí jej nasadit.

19 Zdroje

Elektronické Zdroje

[1] Computerworld. *Mobilní bezpečnost a mobile device management* [online]. [cit. 15. 5. 2015]. Dostupné z: http://computerworld.cz/internet-a-komunikace/mobilni-bezpecnost-a-mobile-device-management-51315

[2] Networkworld. *How does mobile device management work.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://computerworld.cz/internet-a-komunikace/mobilni-bezpecnost-a-mobile-device-management-51315

[3] Networkworld. *How get a handle on MDM.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://www.networkworld.com/article/2178633/wireless/gartner--how-to-get-a-handle-on-mobile-device-management.html

[4] Esecurityplanet. *10 Criteria for an Enterprise MDM Solution.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://www.esecurityplanet.com/mobile-security/10-criteria-for-an-enterprise-mdm-solution.html

[5] BusinessIT. *BYOD a MDM: Mobilní zařízení v podnikové praxi.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://computerworld.cz/internet-a-komunikace/mobilni-bezpecnost-a-mobile-device-management-51315

[6] MobilMania. *Firemní smartphony na uzdě.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://www.mobilmania.cz/clanky/firemni-smartphony-na-uzde/sc-3-a-1125103/default.aspx

[7] Wikipedia. *Mobile Device Management.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://en.wikipedia.org/wiki/Mobile_device_management

[8] ITservices. *Mobile Device Management.* [online]. [cit. 15. 5. 2015]. Dostupné z: https://itservices.stanford.edu/service/mobiledevice/management

[9] Gartner. *Mobile Device Management Prognose.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://computerworld.cz/internet-a-komunikace/mobilni-bezpecnost-a-mobile-device-management-51315

[10] Systemonline. *Mobile Device Management.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://www.systemonline.cz/sprava-it/mobile-device-management.htm

[11] Tom's IT Pro. *Vendors and Comparsion Guide.* [online]. [cit. 15. 5. 2015]. Dostupné z: https://itservices.stanford.edu/service/mobiledevice/management

[12] MotivityLabs. *How to choose a best MDM solution.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://www.motivitylabs.com/how-to-choose-a-best-mdm-solution

[13] Field Technologies Online. *Questions To Ask.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://www.fieldtechnologiesonline.com/doc/essential-questions-to-ask-before-deploying-enterprise-apps-0001

[14] Solutions Review. *Buyers Guide and Best Practise.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://solutions-review.com/mobile-device-management/mdm-buyers-guide-directory/

[15] Good Technology. *MDM Solutions Comparsion.* [online]. [cit. 15. 5. 2015]. Dostupné z: https://www1.good.com/about/comparison-chart.html

[16] Air Watch. [online]. [cit. 15. 5. 2015]. Dostupné z: http://www.air-watch.com/cz

[17] MaaS360. *IBM Company MDM solution.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://www.maas360.com/

[18] Springer. *Efficient Mobile Device Management.* [online]. [cit. 15. 5. 2015]. Dostupné z: http://link.springer.com/chapter/10.1007/978-94-007-5857-5_88

Odborná literatura

[1] **SCHLAGER** Ronald: Selecting Mobile Device Management Systems: Practical Functions, Tips and Checklist, CreateSpace Independent Publishing Platform; 1.0 edition, January 17, 2013. ISBN-13: 978-1482003703

[2] **JOHNSON** Michael: Mobile Device Management: What You Need to Know For It Operations Management, Tebbo, 2011. ISBN-13: 978-1743042151