Správa a zabezpečení mobilních zařízení v prostředí firmy

Bc. Michal Gadlena

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Michal Gadlena**
Osobní číslo:	**A16267**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Správa a zabezpečení mobilních zařízení v prostředí firmy**
Téma anglicky:	**Managing and Securing Mobile Devices in Company Environments**

Zásady pro vypracování:

1. **Stručně představte aktuálně používané mobilní zařízení a operační systémy – zaměřte se na nejrozšířenější platformy z korporátní sféry.**
2. **Prozkoumejte možnosti zabezpečení mobilních zařízení.**
3. **Vytvořte přehled softwarových nástrojů pro vzdálenou správu mobilních zařízení ve firmě.**
4. **Proveďte výběr adekvátního nástroje pro správu na základě požadavků firmy.**
5. **Předložte návrh nasazení a konfigurace vyhovujícího softwaru do prostředí firmy.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **PIERER, Markus. Mobile Device Management: Mobility Evaluation in Small and Medium-Sized Enterprises, Springer, 2016. ISBN 9783658150464.**
2. **HOLUBCOVÁ, Petra a Edward PLCH. Řešení pro správu firemní mobility. ITSystems [online]. 2016, (9) [cit. 2017-03-28]. ISSN 1802-615X. Dostupné z:https://www.systemonline.cz/sprava-it/reseni-pro-spravu-firemni-mobility.htmEdward PLCH.**
3. **MITCHELL, Robert. Výběr správného nástroje pro správu podnikové mobility.Computerworld [online]. 2014 [cit. 2017-03-29]. ISSN 1210-9924. Dostupné z:http://data.computerworld.cz/file/specialy/BYOD-2014.pdf**
4. **STANČÍK, Martin. Tři způsoby zabezpečení firemní sítě v rámci politiky BOYD.Computerworld [online]. 2012 [cit. 2017-03-25]. ISSN 1210-9924. Dostupné z:http://computerworld.cz/technologie/tri-zpusoby-zabezpeceni-firemni-site-vramci-politiky-boyd-49129**
5. **SPEED, Tim, Darla NYKAMP, Mari HEISER, Joseph ANDERSON a Jaya NAMPALLI. Mobile security: how to secure, privatize, and recover your devices : keep your data secure on the go. Birmingham: Packt Publishing, 2013, vi, 216. Community experience distilled. ISBN 978-1-84969-360-8.**
6. **LIU, Haowei. Facial detection and recognition on mobile devices. Amsterdam: Elsevier, Morgan Kaufmann, 2015, 38 s. ISBN 978-0-12-417045-2.**

Vedoucí diplomové práce: **Ing. Radek Vala, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Ve Zlíně dne 8. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

.....
podpis diplomanta

ABSTRAKT

Diplomová práce se věnuje správě a zabezpečení mobilních zařízení ve firemních prostředích. V práci jsou popsány základní možnosti zabezpečení mobilních telefonů, tabletů a notebooků. Zároveň jsou doporučeny základní principy pro zabezpečení obecně. Následně je vyhotoveno určité srovnání dostupných řešení pro správu mobilních zařízení a jsou nalezeny přidané hodnoty každého srovnávaného softwarového nástroje. Ze srovnání je vybrán nejvýhodnější dodavatel řešení. Následně je vypracován postup nasazení a konfigurace vybraného softwaru do prostředí firmy s důležitým časovým harmonogramem. Postup práce při navrhování lze užít jako návod pro podobná nasazení v budoucnu.

Klíčová slova: mobilní správa, MDM, Microsoft Intune, IBM MaaS 360, VMware AirWatch, postup nasazení MDM, zabezpečení mobilních zařízení, srovnání nástrojů pro správu mobilních zařízení.

ABSTRACT

The diploma thesis deals with the management and security of mobile devices in corporate environment. The thesis describes basic possibilities of security on mobile phones, tablets and laptops. At the same time, basic principles for security are recommended for users. A comparison is made between the available mobile device management solutions, afterwards the added value for each comparable software tool is found. The best solution provider is chosen from the comparison. Subsequently, the procedure of deploying and configuring the selected software into the company environment with an important time schedule is developed. The design process can be used as a guideline for similar deployments in the future.

Keywords: mobile management, MDM, Microsoft Intune, IBM MaaS 360, VMware AirWatch, MDM deployment, mobile device security, mobile device management comparison.

Děkuji panu Ing. Valovi, Ph.D., že se ujal dohledu nad touto diplomovou prací a byl nápomocen při jejím řešení.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Základní myšlenka práce si klade za cíl navrhnout reálný postup a proces nasazování softwarového nástroje pro vzdálenou správu mobilních zařízení v podnikových prostředích. Na začátku jsou vymezeny především základní pojmy, například jaké všechny mobilní zařízení spadají do této kategorie. Dále je blíže specifikován nový moderní trend BYOD, který se v posledních letech těší masivnímu nárůstu oblíbenosti a stále více se rozšiřuje. Firmy jej stále více zavádějí a zpřístupňují pracovníkům ve snaze zvýšení jejich produktivity. Následně je popsán detailnější pohled na základní nejrozšířenější operační systémy v podnikovém prostředí, jaké možnosti správy přinášejí a podporují. Postupně jsou v teoretické části přiblíženy všechny možnosti zabezpečení přenosných zařízení a současná bezpečnostní doporučení, které by se ze strany uživatele neměla podceňovat.

Po prozkoumání všech možností zabezpečení je vytvořen přehled softwarových nástrojů pro vzdálenou správu mobilních zařízení a je vzájemně srovnána jejich jednotlivá funkcionalita a přístup k zabezpečení firemních dat. Srovnání také zahrnuje cenovou politiku softwarových nástrojů a typy licencí.

V praktické části jsou představeny všechny podmínky a funkce, které musí nástroj mobilní správy obsahovat. Tyto požadavky mají základ na reálných podmínkách a funkcích od zadavatelské firmy, nicméně v práci bude vystupovat jako firma fiktivní s názvem GadlenaM s.r.o. Na základě výsledku přehledu srovnání je vybrán nejvhodnější kandidát, který splňuje všechny požadavky a má určitou přidanou hodnotu pro firemní politiku. Následně je navrhnut reálný postup nasazení ve specifickém podnikovém prostředí. Proces jako takový obsahuje nezbytné body k úspěšnému nasazení jako je stanovení časového harmonogramu. Dalším bodem je především neomezení normálního produkčního prostředí, následně nezbytným bodem je také včasná příprava samotných zaměstnanců na nově zavedený přístup firmy právě k jejich přenosným zařízením, aby byli dostatečně efektivně proškoleni v za účelem využít potenciál trendu BYOD.

V práci je také popsán průběh testovacího provozu a jak jej správně dělit do fází, aby se předešlo případným chybám před ostrým nasazením a byl čas na jejich opravu. Dostatečný časový interval by měl eliminovat pravděpodobnost omezení produkce.

I. TEORETICKÁ ČÁST

1 MOBILNÍ ZAŘÍZENÍ

Obecný popis mobilního zařízení je v celku jednoduchý. Do této kategorie patří především všechna zařízení, která nemusí být po dobu své činnosti pevně připojená k elektrické zásuvce, a dokáží vykonávat svůj účel pouze na elektrickou energií poskytovanou z integrovaných baterií bez jakýchkoliv omezení. Další nedílnou charakteristikou je možnost připojení daného záření k internetové síti pomocí moderních technologií Wi-Fi nebo přes mobilní datovou sít. V dnešní době všechny tyto charakteristiky splňuje celá řada zařízení, jako je například mobilní telefon, laptop nebo tablet, které používáme jak pro práci, tak pro osobní účely, jako je zábava a komunikace. Z pohledu správy mobilních zařízeních dnes ani pevně připojené stolní počítače neznamenají žádnou změnu přístupu oproti notebookům. Neboť oba dva typy sjednocuje stejný operační systém. [1]

1.1 Bring your own device

Zkratka BYOD (Bring your own device) v doslovném překladu znamená „přines si své vlastní zařízení“ tento přístup je v dnešní době velice populární, jelikož stálé více se zavádí do firem, jak středních, tak zejména i v těch menších. Pod touto zkratkou si lze představit jakékoliv mobilní zařízení, např. smartphone, tablet nebo notebook. Tento přístup má několik přínosů, které jsou přínosem především pro firmu, ale i pro zaměstnance. Pokud se daná firma rozhodne, že umožní svým zaměstnancům využívat jejich vlastní zařízení, zbavuje se tím v podstatě části svých nákladů na vybavení pracovního místa počítačem nebo notebookem. Zaměstnanec, který se rozhodne a začne využívat svůj vlastní přenosný počítač ke své prací, získá především možnost pracovat odkudkoliv, a tím zvyšovat svoji produktivitu. Následně také nespornou výhodou je, že pracuje ve svém známém prostředí a zbytečně nemusí rozdělovat osobní a pracovní počítač a mít tak své data všude přístupná. Samozřejmě se nesmí opomenout fakt, že tito zaměstnanci mají na svých vlastních zařízeních dokumenty a aktiva, se kterými firma pracuje, a jsou pro ni důležitá. Tímto přístupem vystavují firmu nebezpečí úniku dat při odcizení přenosného zařízení. Proto je nutné zavedení nezbytných bezpečnostních opatření, které povedou ke zvýšení bezpečnosti, jak firemních dokumentu, tak zároveň i soukromých dat uživatelů. [2] [3]

1.1.1 Zásady pro zavedení BYOD

Nejdůležitější zásada pro zavedení BYOD do firmy je především nepodcenění přípravy před nasazením určitých pravidel a povinností pro používání vlastních zařízení pro firemní účely.

Následně vytvoření dokumentu s povinným písemným souhlasem, kterým se dotyčný uživatel zavazuje tato bezpečnostní pravidla a povinnosti dodržovat. [4]

Základními pravidly jsou zejména:

- pravidelná kontrola zabezpečení BYOD zařízení,
- vynucení (bez možnosti obcházení, pokud je to možné) používání komplexnějšího hesla pro odemknutí mobilního zařízení,
- využívání zabezpečených šifrovaných komunikačních kanálů pro komunikaci,
- zašifrovaná všechna data na uložišti dat,
- zálohování dat,
- použití antivirových programů a firewallů,
- včasná aktualizace operačního systému a softwaru. [5]

Další nedílnou součástí je vyhotovení protokolu o BYOD, který bude zaměstnanec podepisovat, a tím souhlasit s uvedenými pravidly užívání. Vlastník mobilního zařízení dává svůj souhlas ke kontrole a zásahu podnikatele do pravidel, které podnikatel může měnit, a reagovat tak na nové trendy či hrozby. Při ztrátě zařízení musí mít správce možnost vzdáleně smazat celé zařízení i za cenu smazání soukromých dat uživatele, s důvodu zabezpečení a zamezení odcizení firemních dat nepovoleným osobám. Souhlas by měl taktéž obsahovat vztah k autorským právům, vytvořeným na zařízení pracovníkem při užívání BYOD. Tyto požadavky a souhlasy nemusí být nutně na protokolu o BYOD, ale může je upravovat také již zavedený vnitřní předpis firmy. [6]

1.2 Operační systémy mobilních zařízení

V minulosti při rozšiřování mobilních telefonů a přenosných zařízení existovalo několik operačních systémů (dále jen „OS“), kde z pravidla každý velký výrobce telefonů si sám vyvíjel vlastní operační systém. To vedlo k velké roztříštěnosti a rozmanitosti z pohledu uživatele, který u každého nového telefonu měl jiný uživatelský zážitek a musel se tak znovu a znovu učit základní operace se systémem. Následně touto nejednotností trpěla i samotná kompatibilita mezi zařízením a příslušenstvím. [7]

Tato minulost je už pryč a v dnešní době trhu mobilních operačních systémů kraluje především Android od Googlu a iOS od společnosti Apple. Dle průzkumů a studií společnosti Gartner dohromady tyto dva zmíněné systémy obsluhují skoro 99 % trhu s mobilními OS. Zároveň se jedná o dva největší konkurenty v dnešní době. Tito dva hráči jsou si navzájem

diametrálně odlišní, ale jen ve specifických odvětvích. Android si díky své otevřenosti a univerzálnosti otevřel cestu k ohromné škále smartphonů, stolních počítačů, chytrých krabiček k TV, ale i miniaturních počítačů označovaných jako SBC (Single Board Computer). [8]

Operační systém Android také pokrývá všechny cenové hladiny u prodeje smartphonů, a tím si udržuje dostatečný náskok nad konkurencí. Konkurent iOS míří úplně odlišnou cestou a razí si svoji vizi drahého zboží. Primárním rozdílem je tedy uzavřenost iOS a uzamknutí vlastního OS jen na produkty vlastní firmy. [7]

Zbylá procenta jsou takové systémy, které se snažily vydobýt svoji pozici na trhu a udržet si stálou pozici. Ale po několika neúspěšných letech pomalu ztrácely na popularitě a ukončovaly pomalu svůj vývoj. Mezi těmito neúspěšnými je nutné vyzdvihnout Windows Phone od společnosti Microsoft, který při době svého největšího zastoupení v řádech několika jednotek procent, přinášel alespoň potencionální šanci v budoucnosti na třetí majoritní mobilní operační systém. [7]

1.2.1 Google Android

Stručná historie nejrozšířenějšího mobilního operačního systému začíná u stejnojmenné společnosti Android Inc. Tento startup vydal svoji první verzi v roce 2003, za kterou stál především Andy Rubin a jeho kolegové. Následně za necelé dva roky upoutali s jejich produktem pozornost právě gigantické společnosti Google, která je v roce 2005 odkoupila a na základě potenciálu tohoto startupu založila svoji dceřinou společnost. Android od Googlu je od začátku založen na otevřenosti zdrojových kódů, tímto krokem poskytuje velkou svobodu v užívání a přizpůsobení si prostředí dle specifických požadavků každého uživatele. [9]

Android, jako takový, je ve své základní podstatě zdarma a open source jako projekt AOSP (Android Open Source Project). Nicméně tato vlastnost je vykoupena tím, že neobsahuje právě centrální obchod aplikací Google Play, a proto tento open source projekt nemá možnost instalovat aplikace právě z tohoto zdroje. Aby byl obchod dostupný i na takovémto zařízení, musí splňovat certifikaci Google Mobile Services (GMS) vydané Googlem. Tuto certifikaci lze získat od autorizovaných firem třetích stran za určitý poplatek. [10]

Obr. 1. Android logo [11]

V roce 2006, tedy pouhý rok od nákupu, Google vydal balíček aplikací, která míří zejména na firemní prostředí pod prvotním názvem Google Apps for Your Domain, dnes známý pod názvem G Suite. G Suite obsahuje základní set aplikací a míří s nimi zejména na menší až střední podniky. Nespornou výhodou tohoto řešení je možnost spolupráce na jednom dokumentu v reálném čase s ostatními pracovníky. Jelikož tento produkt staví na webových technologiích, tak další výhodou je podpora nejrůznějších OS tzn. Cross-Platform Friendly. [12]

Nedílnou součástí je právě i Mobile device management (dále jen „MDM“), který řeší jednoduchým nastavením zabezpečení na všech platformách a udržuje firemní data v bezpečí. Aby telefon mohl splňovat bezpečnostní politiku firmy, nabízí Google možnost v MDM vynucovat komplexitu hesel, mazat vzdáleně obsah telefonu, najít ztracený telefon a zákaz používání předešlých hesel. Dále také poskytovat své vlastní interní firemní aplikace přes soukromý firemní obchod mezi vlastní zaměstnance. [12]

1.2.2 Apple iOS

Apple se vydal cestou operačních systémů směrem, kde v celém jeho ekosystému je vše implementováno s ohledem na provázanost a spojení napříč všemi softwarovými produkty od Applu. Tuto cestu začal tehdy, když hlavní představitel firmy, sám Steve Jobs, představil první iPhone na konci roku 2007, a paralelně s ním byl představen i jeho systém, který ho bude pohánět a ten dostal jednoduchý název iPhone OS. Zajímavostí je, že v době uvedení na trh tento systém neměl žádný centrální obchod pro distribuci a instalaci aplikací i napříč tomu, že konkurence v podobě Androidu již svůj vlastní obchod měla. Pouhý rok nato vedení firmy změnilo svůj názor a připravilo aktualizaci, která nový obchod přidává. [13]

Zásadním rozdílem oproti konkurenčnímu Androidu je uzavřenost celého systému a právě s tím je spojen přísný schvalovací proces v obchodě iTunes App Store při přidávání nové aplikace. S touto vstupní kontrolou každé nové aplikace, která se v nabídce objeví, je i zaručen určitý stupeň zabezpečení telefonu. Tento instalační proces je jediným způsobem, jakým

lze do telefonu aplikace nainstalovat bez obcházení zabezpečení. Systém iOS má také zásadní výhodu v jednotnosti nejpoužívanějších verzí, kde drtivá většina uživatelů používá právě nejnovější verzi OS s nejnovějšími opravami a zabezpečeními platformy. [13]

Obr. 2. Logo společnosti Apple [14]

Společnost Apple poskytuje zaměstnavatelům i velkou škálu programů pro snadnější správu a zabezpečení jejich výrobku ve firmě tak, aby firmy mohly zařízení zaměstnanců i firmy snadněji spravovat a udržovat zabezpečené. Jedním z těchto programů je takzvaný Device Enrollment Program (DEP). Ten umožňuje technikům nebo zodpovědným osobám zaregistrovat nový firemní telefon automaticky hned po vybalení. Při prvním zapnutí lze využít několik možností pro automatické nastavení dle firemních požadavků např. SMS, e-mail, QR kód nebo Apple Configurator. Po registraci zařízení do systému MDM získá společnost možnost vzdálené správy nad nastavením složitosti hesel, vynucení dvou-faktorového ověření, zamknout odcizený telefon, lokace telefonu, reset do továrního nastavení, přístup k firemním datům pouze z dané lokace. [15] [16]

1.3 Možnosti zabezpečení

Ve svých vlastních mobilních telefonech dnes máme a ukládáme velmi osobní citlivé informace, o které nechceme přijít, a ani je s nikým jiným bez našeho vědomí sdílet. Může se jednat o fotky z dovolené, kontakty, zprávy, emaily a naše hesla ke všem službám či účtům. Proto by se neměla dnes podceňovat důležitost mít svůj vlastní mobilní telefon zabezpečený a chránit se tak před vystavením našich informacím neoprávněným osobám, které mohou takto získané informace zneužít k páchání trestné činnosti. [5] [17]

Chytré telefony dnes používáme výhradně pro komunikaci a uchování citlivých dat. Nicméně pokud náš chytrý telefon nabízí širokou škálu možností zabezpečení od jednoduchého nastavení PIN hesla až po komplexní biometrické zabezpečení. Je v nejlepším zájmu

uživatele využít co největší počet možnosti zabezpečení a i možných kombinací bezpečnostních prvků. Když si tento návyk uživatel osvojí, nebude to prospěšné jen pro jeho vlastní ochranu, ale bude to přínosem i v budoucnosti při práci ve společnosti, jelikož tentýž stejný přístup bude vyžadovat i firma. Odpadne tedy složité přejímání bezpečnostních politik, které mohou i ve výsledku pracovníky omezovat a zpomalovat jejich produktivitu, ale když se politika správně nastaví na určitý kompromis komfortu a bezpečnosti, a když uživatel je již na určitou úroveň zabezpečení navyklý ze svého soukromého života, je výsledkem spokojenost na obou stranách. [18]

1.3.1 Čtečka otisků prstů

Novou poměrně rychle rozšiřující se formou ověření identity na mobilních telefonech se v posledních letech stala čtečka otisků prstu, která již nepatří pouze do kategorie top modelů, ale i mezi obyčejné telefony střední třídy, kterých se obecně prodá největší množství. Posledních pár let tato technologie prochází postupným zdokonalováním, kde postarší principy ověření otisků jsou nahrazovány zcela novými, účinnějšími a rychlejšími metodami. Nejnovější metoda pracuje na bázi ultrazvuku, kde snímaný prst lze pouze přiložit na vyznačené místo na dotykovém displeji telefonu a bezkontaktně sejmout otisk. [19]

S postupným trendem rozšíření mezi skoro všechny cenové kategorie telefonů roste i podpora softwaru a aplikací, které tyto hardwarové využívají pro ověření. V kategorii MDM řešení je tato funkce implementována a plně podporována jako plnohodnotné a dostatečné ověření. Možnosti nastavení se liší dle poskytovatele MDM, například u řešení Intune od společnosti Microsoft lze povolit nebo úplně zakázat tuto funkci na telefonu. Při povolení této funkce získá firma možnost dále spravovat již uložený otisk a to tím, že lze potlačit jakoukoliv manipulaci s ním, jako je například smazání, editaci či přidání dalšího otisku. Tato funkce je především užitečná u firemních zařízení. [19] [20]

1.3.2 Zabezpečení PIN heslem

Ochrana zabezpečení PIN heslem, se nenachází pouze na mobilních zařízeních, ale také na široké škále zařízení od seto-boxů, SIM karet, BitLockeru, elektrických zámků, kreditních karet, Wi-Fi sítí a dalších elektronických zařízení. PIN lze použít i na zabezpečení konkrétní aplikace. PIN se skládá z krátké či delší soustavy čísel k jasné identifikaci a ověření. Jedná se o nejzákladnější a nejjednodušší formu zabezpečení, která může být i velice efektivní při správném nastavení. Při použití zabezpečení PINem by systém, který ho vyžaduje, měl mít

nastavený i maximální počet pokusů chybného zadaní, aby nedocházelo k útokům na takto jednoduchý typ zabezpečení. Především se jedná o brute-force útok, který bez nastavení tohoto limitu může zkoušet všechny možné kombinace zámku. [21] [22]

1.3.3 Šifrování zařízení

U mobilních telefonů s operačním systémem Android je tato možnost ve výchozím nastavení bohužel vypnutá, a tedy nenutí uživatele k jejímu využívání. Opačný přístup volí konkurenční operační systém iOS, kde šifrování mobilního zařízení je zapnuté ve výchozím stavu a šifruje celý obsah paměťového uložiště, šifrování lze i aplikovat na přítomnou SD kartu. Pokud se uživatel Android telefonu rozhodne funkci zapnout, bude vyzván k zadání hesla nebo PIN kódu, pro zpětné dešifrování přístroje. K zadání dešifrovacího kódu je uživatel vyzýván po každém vypnutí a zapnutí telefonu. Proces šifrování dat znemožní na krátkou dobu užívání telefonu, ale jakmile je proces dokončen, šifrování probíhá automaticky na pozadí běžícího OS. Při využívání našeho zařízení ve firemní sféře je nezbytnou nutností využívat možnosti zašifrování přístroje. Všechny aktuální systémy pro správu dnes umožnují informovat uživatele a přinutit jej k zašifrování zařízení, jinak mu nebude umožněno přistupovat k firemním aktivům. Tento proces je vhodný způsob ochrany všech dat obsažených v zařízení, tak i na SD kartě v případě odcizení nebo ztráty telefonu. Tato funkce je přímo integrována v operačním systému a nevyžaduje další instalaci jakékoliv aplikace třetí strany. Ekvivalent této funkce lze přirovnat k šifrování BitLockerem na zařízení s operačním systémem Windows. [23]

1.3.4 Virtual Private Network

VPN neboli virtuální soukromá síť spojuje všechny připojené počítače do zabezpečené soukromé sítě právě tehdy, když se nachází na různých místech v internetu. Obchází tedy nutnost mít připojené servery nebo klientské stanice fyzickým kabelem. Aby se tohoto dosáhlo, využívá se cest sítě internetu k propojení všech počítačů do sítě VPN. [24]

Nejčastějším využitím VPN, se kterým se lze běžně setkat, je vzdálené připojení do podnikové sítě, když jsme například na dovolené v zahraničí nebo pouze chceme pracovat z domu. Takto se mezi počítači vytvoří šifrovaný tunel a napojí se na VPN server v podniku. Komunikace proudí z našeho počítače, kde je klientskou aplikací zašifrována a následně odeslána tunelem k serveru. Přijímaná data jsou rozšifrována do čitelné podoby a následně předána cílovému serveru. [24] [25]

Obr. 3. Princip komunikace VPN [25]

Další nespornou výhodou je forma zabezpečení, kterou VPN zprostředkovává při připojování z veřejných Wi-Fi sítí kamkoliv k našim účtům, kde zadáváme naše osobní přihlašovací jména a hesla. Pomocí VPN lze taktéž obcházet různé geoblokace nebo lokální cenzury, kdy například daný obsah je zakazován, ať už je to legislativou nebo jen vůlí poskytovatele internetového připojení. [25]

1.3.5 Rozpoznávání obličeje

Rozpoznávání obličeje analyzuje celkovou charakteristiku snímaného obličeje přes standartní fotoaparát. Pomocí algoritmu změří specifické vlastnosti tváře, jako je vzdálenost očí od sebe, velikost nosu, velikost úst nebo specifické lícní kosti. Takto naměřené míry se uloží, a poté jsou porovnávané při pokusu o odemknutí přístroje. Jedná se o jednoduchý systém ověření, který lze snadno ošálit, například vytisknutou fotografií uživatele. Samotná společnost Samsung potvrzuje, že tento způsob není natolik bezpečný, jako jiné biometrické bezpečnostní prvky, jako jsou čtečky otisku prstů, sken oční duhovky nebo FaceID. Z důvodu toho není tento způsob povolen při využití online plateb. [26]

Firma Apple v nedávné době přišla s vlastní implementací a rozšířením této technologie u nového telefonu iPhone X. Apple tento způsob ověření pojmenoval FaceID, kde se také využívá obličej majitele, ale není k tomu využíván standardní fotoaparát nýbrž speciální s TrueDepth technologií, která je integrovaná do fotoaparátu. Následně vedle této kamery je přítomen i Dot Projector, který vysílá na skenovanou tvář 30 000 neviditelných světelných bodů. Z těchto bodů je následně vytvořena mapa obličeje a snímána infračervenou kamerou. Následně proběhne sloučení všech nasnímaných objektů a zpracování s transformací na matematický model. Pro odemknutí telefonu algoritmus využije uložený matematický model a srovná jej s aktuálně snímanou tváří, pokud nastane shoda, telefon se automaticky odemkne. U této technologie nelze použít jednoduché oklamání fotoaparátu, jak tomu bylo u jednoduchého skenu obličeje, a to z důvodu, že se zde pracuje s 3D rozměrem celého obličeje. Tato technologie tedy pozná, že se jedná o nastraženou fotografii a zamítne přístup. [28]

Apple ve svých tvrzení srovnává novou techniku ověřování obličeje se svoji starší metodikou rozpoznávání uživatele pomocí otisku prstu. Podle samotného výrobce existuje šance 1:50 000, že někdo odemkne váš telefon pomocí otisku prstu. U nového FaceID je pravděpodobnost odemknutí jiným obličejem stanovena na 1:1 000 000, tato šance je mnohem menší než u předchůdce, kterým je TouchID. Je tedy více než 20 krát bezpečnější při výskytu omylu v ověření. [28]

Jako u všech možností ověření pomocí biometrických prvků je i zde nastaven maximální počet neúspěšných ověření biometrických vlastností. Tento limit se liší dle daného výrobce a implementace v zařízení, ale obvykle se tyto limity nastavují v rozmezí 3 – 5 neúspěšných pokusů v řadě. Pokud je tato hodnota překročena, je uživatel vyzván k zadání hesla. FaceID má tento limit nastaven pouze na dvě možnosti, a hned poté je vyžadováno heslo. [28]

1.4 Doporučení pro zabezpečení mobilních zařízení ve firemním prostředí

Nicméně lidé využívají svá příruční Android zařízení i na vyřizování soukromé agendy, jako je vyřizování telefonátů, komunikace s přáteli a hraní mobilních her. Uživatelé běžně využívají své přenosné zařízení i k vyřizování firemních povinností a záležitostí, jež jsou běžnou součástí pracovní náplně. Proto je dobré dbát na to, že v malém přenosném zařízení ukládáme nejenom naše soukromé informace, ale i ta firemní. Firmy proto dnes zajímá, jaké mají možnosti správy těchto telefonů, a jak chránit své aktiva. Tato forma správy je nicméně i přínosem pro ochranu dat samotného uživatele. [29]

Prvním odvětvím představující zabezpečení ve firmách by měl být vhodný výběr mobilního telefonu, který bude IT oddělení přidělovat zaměstnancům. Je důležité dbát na to, který telefon vybereme a zjistit zda výrobce telefonu bude podporovat minimálně dvouletý časový interval bezpečnostními aktualizacemi, a zdali nabízí i formu lepší správy telefonu, například jako firma Samsung se svým produktem KNOX.

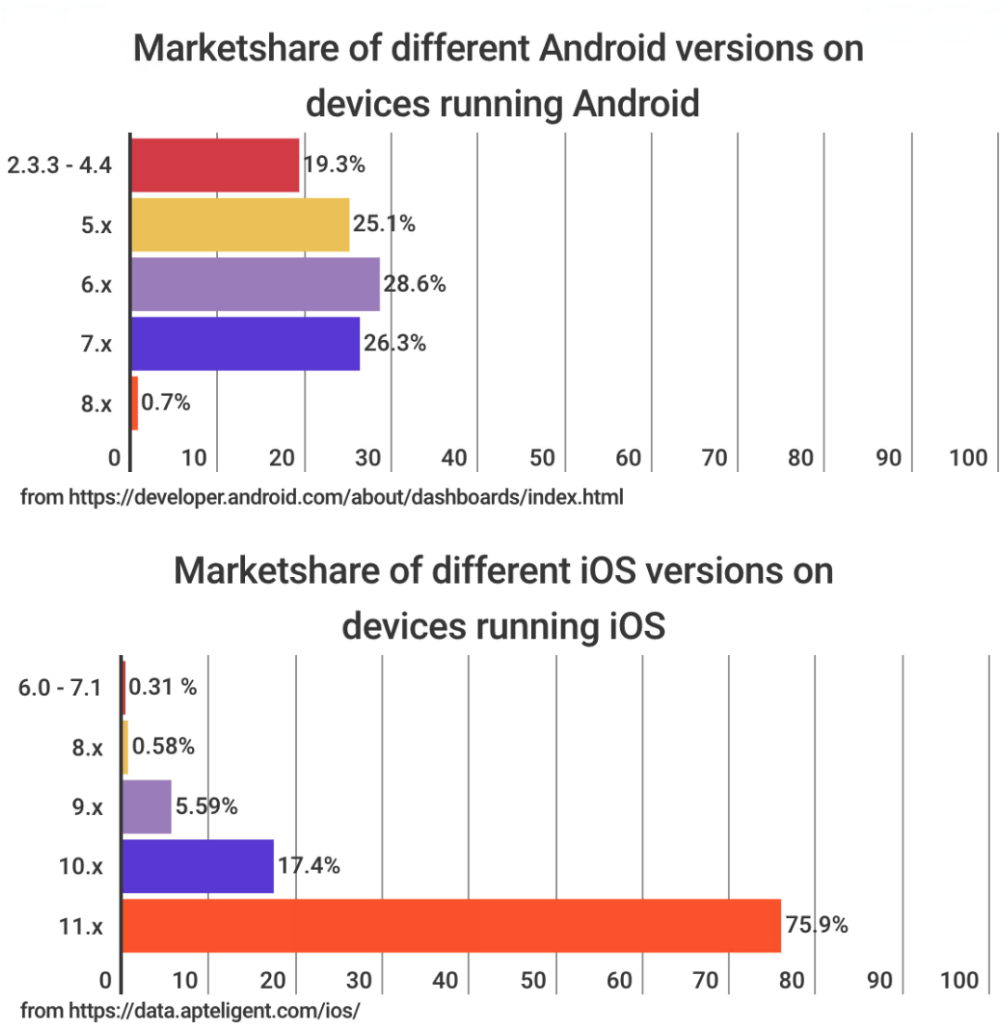
Druhé doporučení se zabývá myšlenkou jednoduchosti prostředí, kterou chceme jako IT oddělení spravovat. Tohle prostředí by mělo být co nejvíce jednotvárné, co se týče počtů různých typů mobilní telefonů. A to sestavením si katalogu zařízení, které budeme poskytovat zaměstnancům k vykonávání jejich práce. Tento katalog by měl obsahovat co nejméně různých typů zařízení, aby se v prostředí dalo jednoduše identifikovat, jaké zařízení pracovník využívá a určit jeho stáří, například hned z názvu zařízení.

1.4.1 Pravidelná aktualizace operačního systému

Svůj postoj a přístup k aktualizacím telefonů zastává každý výrobce telefonu sám dle svého uvážení. V dnešní době není navržený žádný systém jednotné distribuce aktualizací pro telefony s operačním systémem Android. Tento fakt vede k velké roztříštěnosti platformy a pravidelné aktualizace musí zajišťovat samotní výrobci chytrých telefonů.

Jedinou výjimkou je značka Pixel a projekt Android One. Tato značka a projekt mají přímou podporu od Googlu a tím dostávají pravidelné aktualizace v den vydání.[30]

U druhého nejrozšířenějšího mobilního operačního systému, a to u iOS, je situace zcela odlišná a problémy s pravidelnými aktualizacemi jsou tu spíše ojedinělé, neboť všechny telefony mladší pěti let dostávají aktualizace. Tato podpora i pět let starých telefonů je přímo špičková a měla by být vzorem pro další výrobce. [30] [31]



Obr. 4. Srovnání zastoupení jednotlivých verzí operačního systému

Obrázek zobrazuje aktuální stav nainstalovaných jednotlivých verzí operačního systému napříč celou platformou. Z obrázku je patrné, že platforma Androidu trpí poměrně velkou roztříštěností dílčích verzí, kde každá majoritní verze zastupuje čtvrtinu aktivních mobilních telefonů. Tento stav mají právě na svědomí jednotlivý výrobci hardwaru, kteří často u svých nejlevnějších zařízeních neposkytují žádný další nový velký update OS na novou verzi. A uživatelům nezbývá nic jiného, než nakoupit nejnovější modely telefonů s nejaktuálnějším OS. Na druhé platformě (iOS), více než 75% uživatelů, v době vydání nové verze přechází bez problémů na nejnovější verzi. Zbylí uživatelé, kteří nepřechází na nejnovější verzi, dosáhli ve většině případů na konec podpory zařízení, na kterém pracují a již nemají v nabídce přechod na nový. Toto procento je ale stále nižší než u většiny Android telefonů.

1.4.2 Instalace aplikací jen z oficiálních zdrojů

Do mobilních zařízení lze instalovat aplikace různými způsoby. Od té nejzákladnější jako jsou vestavěné obchody aplikací, až po zapnutí vývojářského režimu a ruční instalace aplikace. S těmito možnostmi vzniká problém s ověřením instalované aplikace, zdali neobsahuje škodlivý software. Ve firmách se tedy přistupuje k zakazování instalace aplikací z neznámých zdrojů či vlastnoruční instalace z počítače do mobilního telefonu. Aby se tyto pravidla opravdu dodržovala, lze na spravovaných mobilních zařízeních nastavit pouze možnosti, odkud lze aplikace instalovat. [18]

U prostředí iOS lze povolit instalace pouze z App Store, kde je poměrně hodně striktní kontrola prováděna zaměstnanci při přidávání aplikací od vývojářů. Takže by aplikace vystavené v App Store neměly nikterak ohrožovat zabezpečení uživatelů. V případě Android zařízení je také určitá kontrola vstupních aplikací, které jsou publikovány v Google Play obchodě, ale tato kontrola již zde probíhá automatizovaně pomocí počítače. U počítačů běžících s operačním systémem Windows, který do příchodu Windows 10 neobsahoval jednotný systém distribuce aplikací, je zatím zamezení instalace prováděno přes neposkytování administrátorského práva k instalaci aplikací a nadále i pomocí dalších omezujících nastavení. Firma má také možnost využití například produktu SCCM, který integruje svoji vlastní verzi firemního centra pro správu a instalaci aplikací firemním pracovníkům, kde tento software je přidáván právě IT oddělením a je bezpečný k instalaci na koncových zařízeních bez nutnosti administrátorského oprávnění. [18]

1.4.3 Omezení nadbytečných práv aplikací

Bohužel i instalace aplikací z oficiálních zdrojů neposkytují stoprocentní ochranu před nevhodným chováním aplikací či možnosti stáhnout si nebezpečný software. Uživatel musí věnovat pozornost právům, které se při instalaci aplikace vyžadují. Zde se sází především na uživatelský rozum a schopnost dedukce. [31]

Jako příklad může posloužit obyčejná aplikace na Android, která má jednoduchou funkci na úpravu textového dokumentu a následné uložení do zařízení. Může být podezřelé, že právě tato aplikace při instalaci vyžaduje oprávnění na volání, SMS, fotoaparát nebo GPS lokaci, když naopak vyžaduje jen a pouze oprávnění místního uložiště, což je pochopitelné, aby mohla provést trvalé uložení do telefonu. [31]

S příchodem verze Androidu 6.0 se změnila politika k přístupu udělování práv mobilním aplikacím. Nově nyní instalace aplikace nevyžaduje všechny oprávnění při instalaci, ale až když je spuštěna a vykonávaná určité akce, které vyžadují oprávnění k přístupu, například u ukládání do místního uložiště, je uživatel vyzván k povolení či zamítnutí udělení práva aplikace k uložení. Ve firmě Apple tento přístup k udělování práv aplikacím implementovaly již od raného vývoje iOS. [31]

2 SOFTWARE PRO VZDÁLENOU SPRÁVU MOBILNÍCH ZAŘÍZENÍ

Mobile device management (MDM) je termín pro software k administraci a správu všech mobilních zařízení, jako jsou především smartphony, tablety, laptopy, ale lze s těmito softwary spravovat i desktop počítače. Nicméně pro správu těchto desktopů a serverů jsou určené jiné softwary, které mají mnohem více možností ovládání a nastavení, než jakékoliv MDM řešení, které primárně míří právě na přenosná zařízení. S příchodem masivního rozšíření trendu BYOD mezi zaměstnance, se vyskytla také otázka, jak vyhovět pracovníkům, aby mohli pracovat ze svých zařízení, a jak tyto zařízení spravovat. [32] [33]

Všechny MDM řešení si kladou za jeden z primárních a nejdůležitějších cílů to, aby pracovník zůstal produktivní na cestách, a aby přitom neporušoval bezpečnostní politiky nastavené firmou. Implementací firma neztratí jen finanční prostředky na pořízení a provoz MDM, nýbrž na druhou stranu získá velké úspory v podobě ušetření nákladu na nákup IT vybavení. Následně u jednotlivých zařízeních razantně sníží rizika na neoprávněné odcizení klíčových dat firmy. Tuto myšlenku se snaží implementovat jednotliví výrobci již do svých produktů a snaží se nabídnout jednoduší formu správy a rozšířit tím omezené možnosti vzdáleného ovládání. Příkladem může být firma Samsung se svým standardem KNOX, která běží na platformě SE Android (Security Enhanced Android). [34]

2.1 Software pro správu

Systémy pro mobilní správu zařízení staví na shodné myšlence kontejnerování aplikací a procesů, aby bylo možné rozlišit proces a aplikaci jako firemní nebo soukromou. Kontejner je izolovaný proces, ve kterém jsou pouze firemní data. To zajišťuje, že korporátní data jsou oddělená od soukromých. Pokud firma vlastní a vyvíjí si svoji aplikaci pro mobilní OS, většina MDM řešení nabízí tzv. Wrapping, ke kterému poskytuje dokumentaci a návody, jak tento wrap přibalit k firemní aplikaci. Po wrapování firemní aplikace získají větší možnosti správy a hlavně bude aplikace schopná běžet v zabezpečeném kontejneru s ostatními podnikovými aplikacemi. Poskytovatelé MDM v základu poskytují základní baliček aplikací, které již pracují v režimu kontejneru. Mezi základní aplikace patří například:

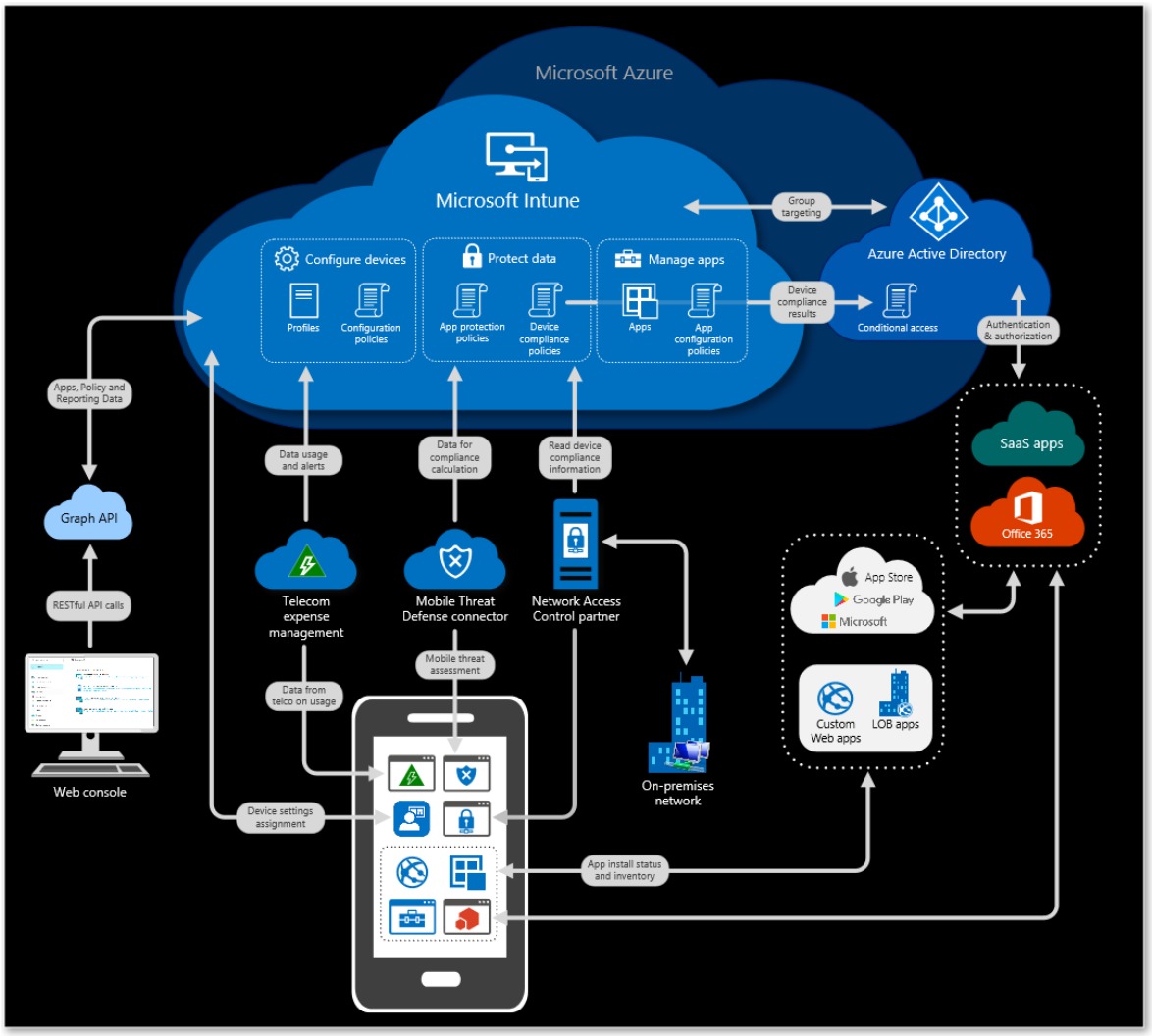
- zabezpečený email,
- zabezpečený prohlížeč dokumentů,
- zabezpečený internetový prohlížeč,

- zabezpečený aplikační katalog. [33] [35]

Tyto aplikace se specializují především na prohlížení dat, ale umožnují i základní úpravy dokumentů. Nicméně oproti primárně určeným aplikacím pro editaci, nabízí opravdu jen nezbytně nutné funkce. Zabezpečený email umožňuje integraci a spojení s firemním Exchange serverem a vzdálené nastavení připojení, aby uživatel nemusel ručně nastavovat cílový server, ke kterému chce přistupovat. Důležitou součástí je zabezpečení dokumentů otevíraných na mobilních zařízeních. Zde lze nastavit například zákaz kopírování a vkládání textu mimo spravovaný kontejner. Nedílnou součástí je omezení přikládání firemních dokumentů jako přílohu k soukromým emailům. Zabezpečený prohlížeč může zamezit potenciálním rizikům, na které uživatelé naráží při prohlížení internetu. A tím dostat do zařízení nechtěný a nebezpečný software. Administrátor může vynutit užívání pouze zabezpečeného prohlížeče a tím používání před-instalovaných prohlížečů zcela zamezit. Aplikační katalog plní roli „firemního obchodu“, kde zaměstnanec najde všechny potřebné aplikace k práci. Další roli, kterou zastává tahle aplikace, je možnost registrace našich vlastních zařízení do podnikového MDM a forma samosprávy zařízení, kde může i sám uživatel lokalizovat nebo vyresetovat svůj vlastní telefon bez zásahu IT oddělení firmy. [32]

2.2 Způsob komunikace zařízení se serverem správy

Komunikace mezi koncovým zařízením a serverem pro správu je realizována dle modelu klient/server, kde na koncovém zařízení běží agent zajištující komunikaci se serverem MDM. Řeší všechny potřebné informace a provádí všechny příchozí příkazy na nastavení. Agent je ve většině případů součástí aplikačního katalogu nebo může být od výrobce přímo integrován do mobilního telefonu, tabletu nebo přenosného počítače. Agent pomocí všech dostupných kanálů přijímá požadavky ze serveru a odesílá zpět aktuální informace o stavu. Následně může taktéž hlídat v určitých intervalech, zda nedošlo ke změně z nadefinovaných stavů, dle kterých je potom potřeba náležitě reagovat a sjednat nápravu odchylky od bezpečnostní politiky. Nevýhodou tohoto způsobu komunikace je zpoždění mezi reálným stavem a jeho reportu zpět na server, že nekoresponduje s nastavením bezpečnostní politiky. Případný požadavek na restart nebo uzamknutí telefonu má řádově zpoždění několik jednotek minut, kde se ještě tato doba může libovolně měnit dle konkrétního nastavení intervalu, kdy se odesílají informace zpět. Ojediněle různé programy pro zvýšení výdrže baterie mohou negativně ovlivňovat tento interval synchronizace. [33]



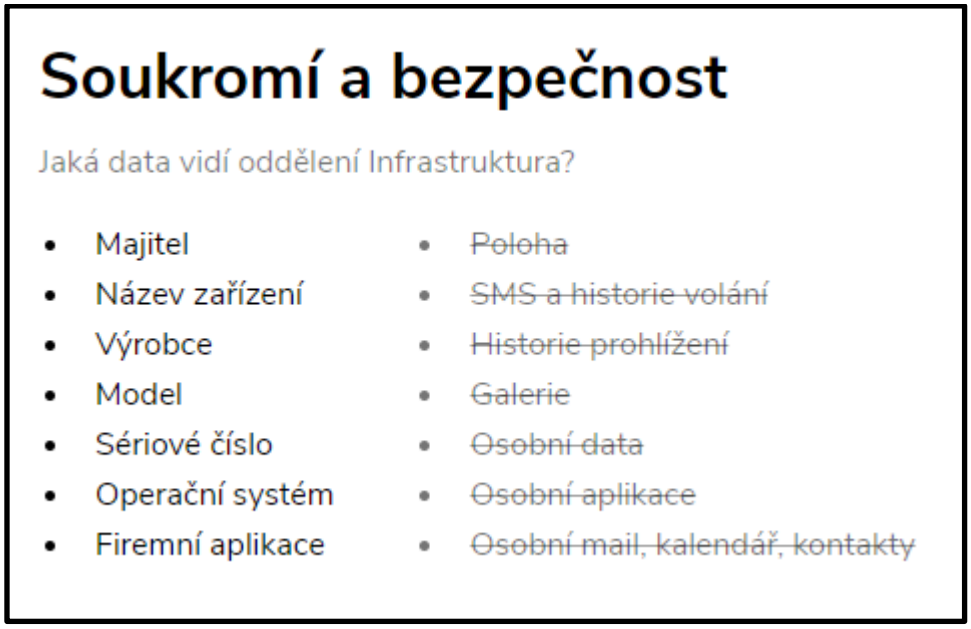
Obr. 5. Princip fungování a komunikace Microsoft Intune

2.3 Úskalí systémů MDM

Společnost Gartner v tiskové zprávě varuje správce, kteří přemýšlí o nasazení MDM systému do jejich podniku. Před některými úskalími nabízených systémů, se kterými by chtěli pracovat. Každá platforma z kategorie mobilních operačních systému má své specifické limity a možnosti správy, z tohoto důvodu nelze aplikovat stejné nastavení na celé portfolio mobilních zařízení, protože pracují na různých operačních systémech. Pokud tedy firma chce nabídnout BYOD pro zvýšení produktivity v rámci své firmy, musí se předem připravit plán do budoucna, kde bude IT oddělení pečlivě zkoumat mobilní zařízení a jejich možnosti správy, než budou nabídnuty zaměstnancům. A pokusit se tak mít svoji interní síť mobilních zařízení co nejvíc homogenní, alespoň u těch zařízení, které firma poskytuje pracovníkům. Nicméně je tento stav po nasazení BYOD více než nereálný, protože pracovníci mají své vlastní zařízení. Tím pádem se stane spravované prostředí heterogenním a takové prostředí

je obtížné spravovat. A je nutné i kvůli jednomu nebo dvěma zařízení nasadit specifickou novou bezpečnostní politiku pouze na dvě zařízení, protože například tyto dvě zařízení mají postarší verzi OS nebo konkrétní specifický přístup ke správě. [33]

Dalším úskalím může být obava zaměstnanců, že zaměstnavatel sleduje, co kdo dělá na svém vlastním zařízení, které si musel kvůli práci zaregistrovat do systému MDM a uvést ho pod správu firemních administrátorů. Obava je to určitě oprávněná, proto je nesmírně důležité pracovníky náležitě informovat k čemu vlastně IT oddělení má přístup, a k jakým datům nikoliv. [32] [33]



Obr. 6. Informace, které vidí IT oddělení [vlastní zpracování]

Soukromí a bezpečí je vlastně alfa a omega, proč jakékoliv řešení, které má na starost správu zařízení nasazovat a provozovat. Nicméně by řešení nastavené firmou na soukromá zařízení neměly vyvolávat mezi uživateli žádné pochybnosti o tom, zda jsou sledováni či nikoliv. Proto je nezbytně nutné pravidelně informovat pracovníky, co IT vidí a co nevidí. Na obrázku lze pozorovat, že jakákoliv soukromá data jsou před IT schovaná, a že IT má přístup pouze k obecným informacím k identifikaci zařízení, jako je například vlastník zařízení, model telefonu, výrobce, sériové číslo a verzi operačního systému. Nastolení určitých pravidel používání není jen jednostranná ochrana firemních dat, ale je to přínosem i pro ochranu soukromých dat uživatele. Důraz na jednoduchost a co nejmenší zatížení jednotlivých pracovníků s vynucením bezpečnostních pravidel by neměla přesáhnout určitou komfortní hranici, která může představovat rovnováhu mezi tím, co uživatele omezuje a co jej naopak podporuje. [32]

II. PRAKTICKÁ ČÁST

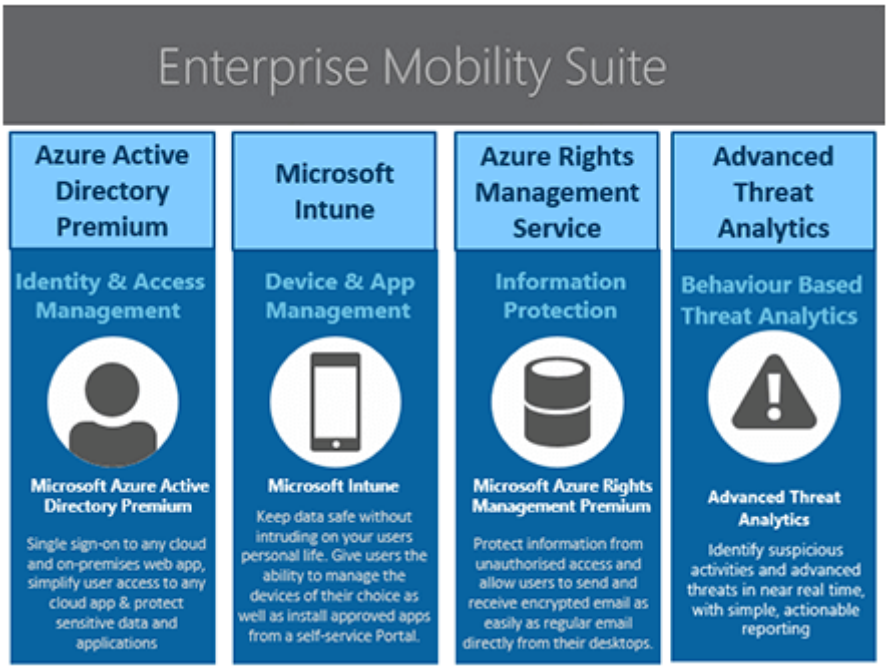
3 PŘEHLED SW NÁSTORJŮ PRO VZÁDLENOU SPRÁVU

Na trhu s nástroji pro vzdálenou správu mobilních zařízení je hned několik poskytovatelů této služby. Mezi hlavní poskytovatele patří: Microsoft, IBM, VMware a další menší poskytovatelé, jako je například MobileIron nebo SOTI. Jelikož v principu je každý tento nástroj omezen možnostmi správy, které jsou implementovány do mobilního operačního systému, nabízí poskytovatelé v podstatě stejné možnosti vzdálené správy. Případnou přidanou hodnotou, a tím pádem výhodou nad konkurencí, je vytvoření kompletní služby, která jen necílí na MDM, ale i na kompletní zabezpečení a monitoring firemní sítě a detekci abnormálních jevů v síti. Všechna řešení pracují na konceptu, kde se stáhne klientská aplikace do smartphonu, který chceme spravovat. Tato aplikace může následně sbírat, reportovat a hlídat určité stavy a posílat zpět do administrátorské konzoly, kde s nimi můžeme dál nakládat. [36]

Všechny nástroje pro správu nabízí také především bezplatnou dočasnou verzi na vyzkoušení produktu bez žádných funkčních omezení. U některých poskytovatelů se může objevit jeden negativní trend v podobě, kde je možnost stáhnutí či zpřístupnění do zkušební verze produktu, vykoupena zadáním platné platební karty. [36]

3.1 Microsoft Intune

Jedná se o produkt jedné z největších softwarových firem, kterou představuje společnost Microsoft, který v posledních dobách soustředí svoji firemní politiku na cestu cloudových služeb a pomalu transformuje svoje produktové portfolio na jednotnou platformu Azure. Na této platformě se nachází nespočet služeb od zálohování celých prostředí až po monitoring on-premise. V rámci nabízení služeb Microsoft integruje a seskupuje své jednotlivé dílčí produkty do balíčků, aby tvořili jednotnou ucelenou nabídku, která pokrývá všechny odvětví dané problematiky. Jedna taková dílčí služba je právě Intune, který zajišťuje a obsahuje správu mobilních zařízení a firemní aplikaci na těchto zařízeních. Aby se dala tato služba plnohodnotně používat, vyžaduje i produkt na správu identit v Azure prostředí, a to Azure Active Directory (AAD). Ta je se svou funkcí srovnatelná s Active Directory řešení ve firmě on-premise. Balík obsahuje taktéž funkci pro účely ochrany konkrétních dat a jednotlivých souborů. To vše za účelem zvýšení bezpečnosti, produktivity a zpřístupnění firemních dat na všech zařízeních s využitím kancelářského balíku Office 365. [37]



Obr. 7. Enterprise Mobility Suite

3.2 IBM MaaS 360

IBM MaaS 360 představuje jednu z nejlepších možností správy firemním mobilních zařízení. Tato možnost taktéž spadá pod určitý kompletní balík služeb od IBM pod názvem IBM's enterprise mobility management (EMM). Tato služba je taktéž nabízena jako hostovaná služba v cloudu stejně jak ostatní konkurenční řešení. Zároveň také nabízí i možnost plné instalace do On-Premise uzavřeného prostředí, aby se firma nemusela obávat o nějakou formu zneužívání dat třetí stranou, která jim zajištuje správu právě těchto citlivých zařízeních a jejich dat. Mezi základní klíčové funkce patří především zabezpečení, tak i různé formy sestavování jednotlivých reportů a analýz o využívání spravovaných prostředků pro správce a pro management firmy. Podpora operačních systému běžících na mobilních zařízení je přímo ukázková. Patří mezi ně samozřejmě základní trojice operačních systému jako je Android, iOS a Windows Phone. Tak i jejich ekvivalenty v podobě Android Wear, watchOS a Apple TV, které můžeme najít na malé nositelné elektronice tzv. wearebles příslušenství. Další podpora je zaměřena na sdílené tablety nebo na jednoúčelové kiosky. Součástí MDM je určitě taktéž forma zabezpečení aplikací MAM, zde IBM nabízí několik vlastních aplikací, jako je aplikace Mail, Docs, Browser, VPN, a to vše pro jednodušší komunikaci a práci se zabezpečeným přenosem dat. [38]

3.3 VMware AirWatch

VMware jako velký hráč na poli virtualizace má ve firmách zvučné a silné jméno. Na základě trendu, kde se mobilní zařízení globálně rozšířily a začaly se vyvíjet, společnost rozhodla o založení platformy AirWatch. Tato platforma byla sestavena od nuly se záměrem hladce a jednoduše se přizpůsobovat trendům a prostředím, ve kterém je nasazována. Při návrhu byl kladen také důraz na jednoduchost používání pro uživatele. AirWatch není žádnou výjimkou mezi konkurencí a staví taktéž na osvědčeném principu cloudového řešení i s možností on-premise, ale ta je nabízena až jako druhotné řešení. Samozřejmostí je podpora všech mobilních operačních systémů, kde je zase kladen důraz na jednoduchost registrace zařízení do systému, a tím nabídnutí BYOD bez sebemenších problémů. Výhodou řešení je smlouva se společností Samsung, která má svůj vlastní standard zabezpečení jejich telefonů nazvaný Samsung KNOX, který správu MDM ještě více rozšiřuje a poskytuje daleko víc možnosti správy a nastavení na podporovaných telefonech. [39] [40]

4 VÝBĚRH VHODNÉHO MDM

Výběr správného MDM řešení by se určitě neměl žádným způsobem uspěchat. Ale naopak projít důkladným prozkoumáním jednotlivých možností, které trh s MDM produkty nabízí. Je důležité také při rozhodování mít na vědomí, že volba ovlivní určitým způsobem drtivou většinu pracovníků v jejich každodenní pracovní činnosti. Proto by se měl i zohlednit názor cílové skupiny a případně najít určitý kompromis ve finální podobě nastavení bezpečnostní politiky. Potencionální řešení, které bude vybráno, by zajisté mělo mít i určitou perspektivu budoucího růstu či navázání na další služby, aby zbytečně za několik let nedošlo ke změně dodavatele MDM řešení, například kvůli jeho zániku či neforemnosti produktu přizpůsobovat se požadavkům zákazníka. [41]

4.1 Podmínky a funkce zadané od zadavatele

Zadavatelská firma má poměrně jednoduché nároky na požadované funkce, které by mělo řešení MDM mít. Jako celkový primární cíl je samozřejmě zvoleno zvýšení zabezpečení mobilních zařízení. Pod správou by právě měly být všechny telefony a tablety přistupující k firemním aktivům, jako je firemní pošta nebo dokumenty. Nedílnou podmínkou nasazení je, aby co nejméně nebo vůbec proces nasazování neomezil provoz firmy. Následně nové řešení, které bude vybráno, musí splňovat určitou kompatibilitu s firemní infrastrukturou, aby nedošlo k velkým a razantním změnám ve stylu fungování infrastruktury, např. pořízení specifického hardware nebo podobné specifické komponenty, bez kterých by vybrané řešení nemohlo správně pracovat. Mezi konkrétní požadavky na řešení MDM patří následující funkce:

- šifrování přístroje,
- vzdálený restart,
- vzdálené uvedení telefonu do továrního nastavení (factory reset),
- vzdálené vymazání všech firemních dat (selective wipe),
- vzdálené uzamknutí telefonu,
- lokalizace polohy telefonu,
- vy-resetování hesla,
- přihlašování pomocí PIN,
- přihlašovaní pomocí biometrických bezpečnostních prvků,
- omezení zdrojů, odkud lze aplikace instalovat,

- povolení/zakázání přístupu k firemní poště.

Všechny tyto požadavky by mělo řešení být schopno vynutit a následně hlásit zpět pověřeným pracovníkům jednotlivé aktuální stavy dílčích nastavení na daném zařízení, a to v podobě souhrnného reportu. A zdali je konkrétní zařízení v souladu s bezpečnostní politikou či nikoliv. Při situaci, kdy spravované zařízení není v souladu s politikou, musí řešení jasně zobrazit, v jakém konkrétním nastavení je nutno sjednat nápravu a informovat uživatele k nápravě prostřednictvím emailu nebo notifikace zobrazené na displeji zařízení.

4.2 Srovnání software pro správu mobilních zařízení

Srovnání vychází z požadavků zadavatelské firmy, kde byly provedeny jednotlivé srovnání, napříč jednotlivými nabízenými řešeními potencionálních dodavatelů. Nad rámec požadavků bylo vytvořeno jednoduché doporučení s přidanými hodnotami, které dané řešení přináší. Určitou váhu v hodnocení jednotlivých MDM řešení měla i designová stránka a jednoduchost řešení, jak pro administrátorskou správu, tak i pro uživatele. Výsledné řešení by mělo být jednoduché a přehledné. Nicméně tohle hodnocení nespadá do funkčních kritérií, ale jen do osobního názoru zpracovatele.

Tab. 1. Srovnání funkcionalit mobilních nástrojů pro správu

Požadavek:	Intune	MaaS 360	AirWatch
Šifrování přístroje	Ano	Ano	Ano
Vzdálený restart	Ano	Ano	Ano
Vzdálený reset do továrního nastavení	Ano	Ano	Ano
Vzdálené vymazání všech firemních dat	Ano	Ano	Ano
Vzdálené uzamknutí telefonu	Ano	Ano	Ano
Lokalizace polohy telefonu	Ano	Ano	Ano
Vyresetování hesla	Ano	Ano	Ano
Přihlašování pomocí PIN	Ano	Ano	Ano
Přihlašovaní pomocí biometrických prvků	Ano	Ano	Ano
Omezení zdrojů, odkud lze aplikace instalovat	Ano	Ano	Ano
Povolení/zákaz přístupu k firemní poště	Ano	Ano	Ano
Přidaná hodnota:	jednoduchost	reporty	dvě licence
	integrace	úrovně baterie	dozor dokumentů
	žádné app navíc	extra app	extra app

Z tabulky lze vyčíst, že všechny srovnávané řešení nabízí stejnou funkčnost dle požadavků firmy. Na základě těchto poznatků by bylo možné vybrat jakékoliv nabízené řešení, protože všechny splňují stanovené požadavky zadavatele. Aby byl pohled na celkové srovnání kom-

pletní, nesmí se opomenout i ekonomická výhodnost každého řešení, a musí být také přihlédnuto k celkové ceně a typu licence, která se s produktem spojuje. Licence se mohou vázat na dva typy objektů, a to na uživatele, který produkt využívá, nebo na každé jednotlivé zařízení spravované firmou. Možnost volby typu licence nabízí pouze AirWatch, kde lze vybrat mezi licencováním uživatele, zařízení nebo kombinací obou variant.

Tab. 2. Srovnání cen poskytovatelů MDM

Intune		MaaS 360		AirWatch		
Licence	USD/user	licence	USD/device	licence	USD/user	USD/device
InTune	6	Deluxe	5	Standard	6,52	3,78
EMS E3	8	Premier	6,52	Advanced	10,9	6
EMS E5	14,8	Enterprise	9	Enterprise	15	10

Pro srovnání licencí, byly vybrány takové licence, které nejenom obsahují základní funkcionalitu požadovanou zadavatelem, ale především i určitou přidanou hodnotu nad požadavky. Všechny tyto licence obsahují balíček funkcí se srovnatelnou funkční hodnotou mezi jednotlivými MDM řešeními, aby byla srovnávána stejná úroveň poskytovaných služeb. Nicméně pro úspěšné splnění požadavků by stačilo vybrat od každého řešení tu nejlevnější variantu. Ale jelikož firma využívá především služeb Microsoftu pro licencování vlastní serverovou infrastrukturu, tak také poskytuje licence partnerským firmám ve velkém objemu. Microsoft poskytuje zadavatelské firmě určité benefity, kde jedním z těchto benefitů je právě několik desítek licencí EMS E3, které obsahují Intune.

Mezi přidanou hodnotu Intune patří především jednoduchost administrátorského prostředí, tak i uživatelské, ve kterém se pracovníci pohybují. V souvislosti s uživatelským přívětivým prostředím koresponduje i fakt, že Intune nevyžaduje žádné další aplikace navíc, až na Microsoft Browser, a integruje všechny nástroje, které zajišťují bezpečnost dokumentů a firemních aktiv do výchozích aplikací od Microsoftu, jako jsou Microsoft Word, Microsoft Excel a Microsoft Outlook. Uživatelům tím odpadá nutnost vlastnit několik různých aplikací pro jednu konkrétní činnost. V možnostech správy mobilních zařízení plní Intune pouze jen základní předpoklady a funkce, které se od MDM očekávají. [42]

Produkt MaaS 360, jako jediný, přináší výhody v podobě rozmanitého nastavení reportů, který si může administrátor nastavit, pokud sledovaná hodnota například poklesne pod stanovenou hodnotu, nebo jestli počet neúspěšných instalací překročí horní hranici limitu. IBM také nabízí sledování aktuálního stavu nabití baterie, využití paměti RAM v zařízení, výpis

aktuálně běžících procesů s možností jejich ukončení. Negativem řešení je absence volby typu licence. Při využití možností nejenom správy zařízení ale i aplikační správy dokumentů je nutné instalovat aplikace přímo od IBM, aby se dosáhlo požadovaného zabezpečení. Produkt je více orientovaný do prostředí, kde jedno konkrétní zařízení je využíváno několika zaměstnanci. [43]

Třetí řešení AirWatch podporuje širokou škálu operačních systémů. Jako jediné řešení nabízí možnosti volby typu licence, tím se lehce může přizpůsobit stylu Vaší společnosti při návrhu a provozu MDM. Administrátorské prostředí je přívětivé a poskytuje všechny potřebné informace o zařízení, jestli vyhovují nastaveným bezpečnostním politikám, ihned na domovské stránce. Administrátor může procházet nainstalované firemní aplikace a vzdáleně je spravovat. To platí i pro firemní dokumenty, kde administrátor má přehled jaké dokumenty v zařízení jsou uložena, a jak s nimi pracovník nakládá. AirWatch také poskytuje několik desítek vlastních aplikací pro jednotlivou správu a rozdělení soukromého prostředí od firemního. [39] [40]

4.3 Výčet nejdůležitějších funkcí MS Intune

Vedení firmy rozhodlo, že pro správu mobilních zařízení bude využit produkt Microsoft Intune. I když tento produkt zaostává v počtu funkcí ve srovnání s konkurencí a není zdaleka tím nejlepším řešením pro MDM, obsahuje nicméně všechny požadované funkce, které byly zadány zadavatelem. A především koresponduje s firemní politikou v oblasti budoucího rozvoje společnosti, které se chce společnost věnovat, a to právě poskytováním cloudových služeb od Microsoftu. Na dále tu je faktor výhod, které jsou již poskytovány v rámci partnerského programu s Microsoftem v podobě volných licencí k EMS E3. Pokud pomineme, tento fakt levnějšího pořízení, vedení uvedlo, že ostatní provozovatelé MDM řeší zabezpečení dokumentů a aplikací pomocí svých vlastních aplikačních řešení, kde by zbytečně docházelo k duplikaci aplikací. U řešení v podobě Intune tato nevýhoda odpadá a stupeň zabezpečení je již chytře integrován do balíčků Office, jak pro mobilní zařízení, tak i do desktopových ekvivalentů. [44]

4.4 Enterprise Mobility + Security (EMS)

Jak už bylo zmíněno v kapitole 3.1 Intune je jen dílčí službou celého kompletního řešení Enterprise Mobility + Security (EMS), které slouží ke spravování mobilních zařízení a aplikací. Kompletní portfolio nabídky EMS obsahuje tyto následující komponenty:

- Identity Management,
- Device Management,
- Information Protection,
- Advanced Threat Analytics. [42] [45]

Tyto komponenty nadále rozšiřují možnosti spolupráce Intune i s dalšími službami od Microsoftu, ke kterým mohou být využívány. Není zde tedy žádné omezení, jen a pouze na konkrétní využití jen s jednou službou. Identity Management pracuje a využívá možnosti ověření identity přes Azure Active Directory (AAD) k řízení přístupu a práv. Další hlavní součástí je služba Azure Information Protection (AIP) pro účely ochrany dat jejich označení, jaká data obsahují, a zabezpečení šifrováním při posílání mimo hranice firemní sítě například na zařízeních firemních partnerů. Poslední částí je analytický nástroj Microsoft Advanced Threat Analytics (ATA), k identifikaci hrozeb a neobvyklého chování uživatelů, kde sleduje neobvyklou činnost jako počet neúspěšných přihlášení či místo přihlášení. [45]

4.4.1 Identity Management

Tento produkt zajišťuje několik možností ověření Vaší identity vůči doménovému řadiči. Princip ověření pracuje s provázaností lokálního doménového řadiče s druhým řadičem v cloudovém řešení, pomocí AAD konektoru, který zajišťuje synchronizaci mezi těmito servery. Základní způsoby ověření, které jsou v rámci této služby poskytovány:

- Single Sign-On,
- Multi-Factor Authencation,
- Risk-Based Canditional Access,
- Privileged Access Management,
- Secure Remote Access.

Identity Management nabízí pracovníkům využití Single Sign-On (SSO) pro nespočet různých aplikací. Tato metoda je velice rozšířená v on-premise, kde se stačí jednou přihlásit k počítači a tohle ověření si potom přebere daná aplikace. Takto ověřenou osobu tak rázem může připojit i na Váš firemním Outlook, bez nutnosti znovu vyplňovat přihlašovací jméno a heslo. Zde tato služba umožňuje využití SSO v cloudovém prostředí především pro služby od Microsoftu, ale i několik tisíc partnerských aplikací. Více-faktorové ověření se pomalu v dnešní době stává standardem a klíčovým prvkem při ověření identit k nejcitlivějším údajům. Uživateli je po správném vyplnění přihlašovacího jména a hesla ještě navíc zaslán kód

do mobilního telefonu, kterým dokončí celý proces přihlášení. Risk-Based Conditional Access poskytuje funkci k zablokování či povolení přístupu na základě nadefinovaných podmínek, lze vynutit například použití více-faktorového ověření na základě vaší polohy jen mimo firmu a naopak použití potlačit při nacházení se uvnitř podnikové sítě. [45]

4.4.2 Device Management

Intune je převážně cloudová služba, ale nabízí i možnosti integrace do on-premise k současnému nasazení System Center Configuration Manager (SCCM), kde lze potom z jednoho místa spravovat firemní PC, tak i mobilní zařízení přes rozšíření o funkcionalitu Intune. Tato integrace přímo do SCCM, ale kromě jednotného místa ke správě, žádné další razantní výhody oproti užívání čistě cloudového řešení nenabízí. [45]

Funkci správy mobilních zařízení zde zastupuje právě Intune jako MDM řešení. Jeho další hlavní součástí je také Mobile Application management (MAM), takže se spíše jedná o produkt dva v jednom. Lze v něm nejenom spravovat mobilní zařízení ale i aplikace, které se na zařízení provozují. Intune je založen na čtyřech základních pilířích:

- Mobile Application Management,
- Multi-Identity Management,
- Selective Wipe of Corporate Data,
- Unified Endpoint Management Solution. [45]

Multi-Identity Management umožnuje uživatelům přistupovat jak k firemním, tak i osobním účtům skrze jednu aplikaci Office i právě tehdy, když je na pracovní účet aplikovaná MAM politika spravující chování aplikace a její možnosti používání. Dokáže tedy bezchybně rozlišovat, zda se jedná o firemní nebo soukromá data bez nutnosti zdvojování aplikací pro různé činnosti. Následně umožnuje vzdálené smazání jen a pouze právě firemních dat, kdy soukromá zůstanou beze změny. [45]

4.4.3 Information Protection

Tato funkce spravuje jednotlivé přístupu k vytvořeným dokumentům. Kdo a jaké práva má k danému dokumentu, jestli lze jenom číst nebo editovat obdržený dokument či nikoliv. Dokumenty jsou již chráněné při vytvoření dokumentu, a poté jsou úzce spjaty s dokumentem a cestují spolu s ním. Při tvorbě se daný dokument označí titulkem a zařadí do příslušné kategorie dle obsahu. Tvůrce dokumentu následně může sledovat aktivitu dokumentu a při-

řazovat nebo odebírat přístupy vzdáleně. Tento systém samozřejmě využívá připojení k internetu k aktualizaci tabulky přístupů, ale není to podmínka. Lze k dokumentům přistupovat i offline, kde si dokument uchovává offline verzi tabulky přístupů, následně se po opětovném spojení se serverem správy svoji tabulku aktualizuje. [46]

4.4.4 Advanced Threat Analytics

Představuje analytický nástroj, který v reálném čase sleduje bezpečnost prostředí k následné detekci hrozeb. Nástroj je založený na strojovém učení, proto je stále on-line a neustále se v detekci zdokonaluje. Zaznamenává všechny přístupové požadavky, všechny vytvořené dokumenty, všechny lokace odkud se přistupuje, všechny zařízení prostě všechny dostupné informace. Pokud detekuje potencionální hrozbu, okamžitě poskytuje nezbytné informace IT pracovníkům, jak hrozbu potlačit a snaží se určit důvody, proč k dané situaci mohlo dojit. [46]

5 POSTUP A DULEŽITÉ BODY PŘI NASAZENÍ

Postup nasazení vybraného řešení pro správu mobilních zařízení Microsoft Intune, které vedení firmy „GadlenaM, s. r. o. vybralo“, představuje nejvhodnější variantu, která současně koresponduje s budoucím rozvojem a zaměřením firmy. Vybrané řešení Microsoft Intune následně splňuje všechny funkční požadavky na správu mobilních zařízení i koncovou cenu za zpravování jednoho uživatele využívající plnou licenci Enterprise Managament Securitry (EMS).

Implementace nově vybraného řešení do podniku bude probíhat za normálního provozu a produkce firmy, proto musí zvolit takový postup, aby se neomezila a ani výrazně nezpomalila funkce celé firmy. Proto se pro úspěšné nasazení vypracuje přesný harmonogram, kde budou zaznamenána časová okna jednotlivých částí nasazení. Současně s nasazením na pozadí bude probíhat školení uživatelů a rozšíření povědomí o nových možnostech práce pro zaměstnance. I když byl vybrán produkt, který staví na cloudovém prostředí, je nutné propojení služeb v on-premise do prostředí Azure, jako jsou Active Directory (AD) nebo Active Directory Federation Service (ADFS). Po úspěšné konfiguraci, bude spuštěn provoz na testování vzorků vybraných pracovníků, aby se odhalily nedostatky či případné problémy, a aby byl dostatek času na jejich vyřešení před uvedením do ostrého provozu.

5.1 Harmonogram nasazovaní

Celkový proces nasazování do prostředí firmy je poněkud zdlouhavý proces. V aktuálním příkladu nasazení je celková doba zakomponování nové správy pro mobilní zařízení v řádu jednotek měsíců. Největší důraz je zde kladen na délku testování. Tato skutečnost vyžaduje necelé dva měsíce, aby byly eliminovány všechny problémové scénáře před uvedením do ostrého provozu. Konfigurace vybraného řešení zabírá z celkového času pouze jednu třetinu, která odpovídá jednomu měsíci, nicméně ji lze provést i daleko rychleji.

Časové rozvržení bylo rozděleno do jednotlivých etap nasazování. V první etapě probíhalo především plánování, které se skládalo z vypracování srovnání MDM, vypracování kompletního seznamu všech mobilních zařízení, které přistupují v aktuální době k firemní poště a následně i výběr vhodného řešení pro nasazení.

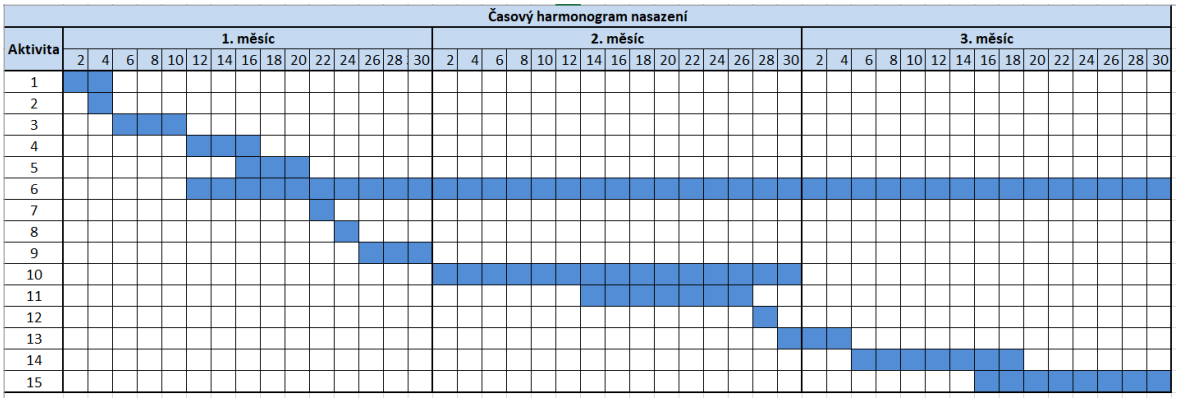
Tab. 3. Aktivity v harmonogramu

	Aktivita	Název aktivity	Doba trvání (dny)
Plánování	1	Vypracování srovnání MDM - Intune, MaaS 360, AirWatch	6
	2	Vypracování seznamu všech mobilních zařízení	2
	3	Výběr vhodného MDM	6
Přípravy	4	Konfigurace dle požadavků	6
	5	1. fáze - Testování – interní provoz	6
	6	Seznamování uživatelů s BYOD a MDM	80
	7	Propojení cloudu k on-premise službám	2
	8	Migrace uživatelů do prostředí cloudu Azure	2
	9	Příprava interního webu s registrací do Intune	6
Realizace	10	2. fáze - Testování - testovací skupina	30
	11	Řešení nalezení problémů	14
	12	Ukončení konfigurace	2
	13	Vyhotovení protokolu	6
	14	3. fáze - Testování - celé IT oddělení	14
	15	Nasazení do provozního prostředí	14

V druhé etapě byly realizované všechny přípravné operace nezbytné k uvedení služby správy do provozu. Jednalo se především o samotnou konfiguraci dle zadaných požadavků, interní testovací provoz, migrace uživatelů a spojení s prostředím cloudu Azure. Paralelně s těmito kroky, kdy už je vedením firmy odsouhlasen konkrétní produkt, se začínají vypracovávat předměty a obsahy školení, které budou postupně všichni zaměstnanci absolvovat, aby byly dostatečně a s předstihem seznámeni s možnostmi a funkcemi vybraného řešení. Zde je také vypracován interní web se všemi náležitými informacemi ohledně Intune, který dále obsahuje podrobné návody na registraci zařízení do Intune, dle konkrétního mobilního operačního systému.

V poslední třetí etapě je kladen důraz na testování a realizaci celého procesu s dostatečnou časovou rezervou, aby byly v tomto čase objeveny a vyřešeny všechny nalezené problémy. A postupně, aby se začal překlápět provoz z testovacího režimu do ostrého provozu s minimem dopadu na funkčnost celé firmy. Současně s těmito všemi kroky probíhalo zaškolování pracovníků, které bylo ukončeno zároveň s nasazením do ostrého provozu. Obsah tohoto

školení v menším měřítku bude zařazen do obsahu zaškolení nových pracovníků při nástupu do firmy.



Obr. 8. Časový harmonogram

Průběh časového harmonogramu zobrazuje průběh postupného nasazování v časovém intervalu tří měsíců včetně testování, realizace a samotného plánování. Každý měsíc je rozdělen do patnácti dílků, kde každý jeden dílek odpovídá času dvou dní. Dílčí jednotlivé kroky potřebné k nasazení jsou zaneseny do sloupce Aktivita, kde jejich číselné vyjádření odpovídá číslům obsažených v tabulce č. 3 Aktivity. Do harmonogramu je vyznačena časová náročnost každého kroku s přehledným vyobrazením paralelním kroků. Především tohle grafické znázornění zobrazuje, kdy a jak dlouho se s řešením dané aktivity začíná a končí.

5.2 Seznámení uživatelů ohledně BYOD

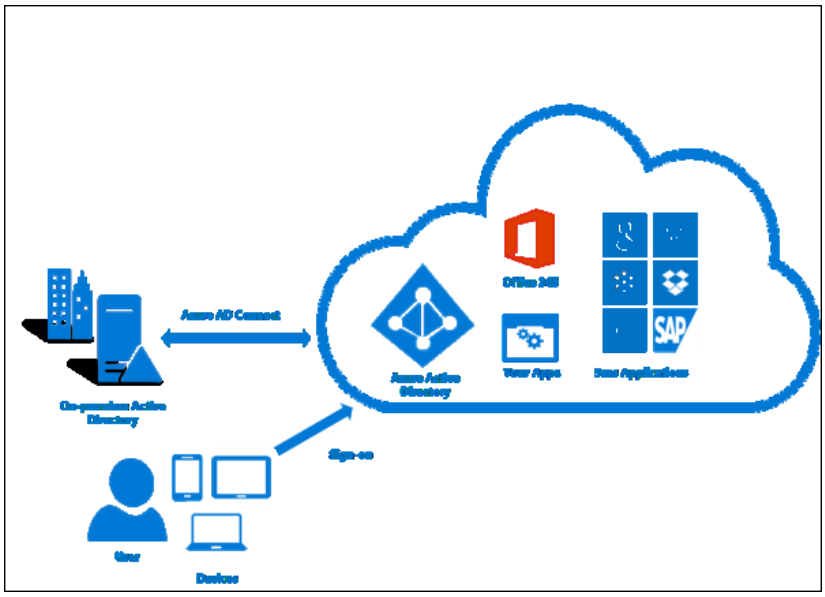
Předání informace pracovníkům ohledně plánu nasazení nového trendu do produkčního nasazení ve firmě by nemělo být podceněno a mělo by informovat všechny zaměstnance s předstihem. Následně pro seznámení uživatelů bude využito několik forem informačních kanálů. V rámci těchto informačních kanálů bude postupně pracovníkům vysvětleno, jakým způsobem a kde o využívání BYOD zažádat. Dále budou také dostupné informace, jaké výhody to přináší zúčastněným pracovníkům i společnosti. Na zaregistrovaném zařízení budou mít zaměstnanci možnosti jednoduché správy a kdykoliv mohou využít služeb odebrání z programu nebo i vlastní lokalizace telefonu, třeba v případě jen krátké ztráty bez nutnosti informovat správce.

Prvotním informačním kanálem bude představení možnosti začátku využívání BYOD na celopodnikové poradě, která se koná každým rokem, kde je probíráno, jaké cíle se splnily a o jaké cíle se bude v následujícím roce usilovat. Jako druhý kanál k přístupu informací

bude zřízen interní web portál pro administraci zařízení s přehlednými a jasnými informacemi o trendu, spolu s návody na registraci a odebrání zařízení, aby byl proces, co nejjednoduší a automatizován bez nutnosti zásahu administrátorů. Třetí místo k nalezení informací bude probíhat prostřednictvím interní směrnice, pojednávající o zavedení MDM řešení, která bude vyvěšena na lokálním centrálním sharepointu, který funguje jako jednotné informační místo pro každého pracovníka. V závislosti s každou výše zmíněnou formou zprostředkování informace bude rozeslán informační email s pozvánkou na hromadné školení nebo odkazy na informační portály k získání bližších informací a kontaktů, v případě problému s nastavením či s funkčností zařízení.

5.3 Migrace uživatelů z On-Premise do cloudu

Migrace uživatelů z on-premise řešení do cloudového řešení není hlavní podmínkou pro úspěšné zprovoznění Intune, ale bez tohoto kroku by uživatelé neměli možnost se přihlašovat pomocí svých již existujících účtů, které využívají v prostředí firmy ke všem pracovním aplikacím. Bez této synchronizace by nastala situace, kdy by byli všichni uživatelé nuceni založit si svůj vlastní nový účet na portálu Azure. Z tohoto důvodu je proto důležité zavedení synchronizace do cloudu přes poskytovaný nástroj Azure AD Connect, za předpokladu, že firma již provozuje svoji vlastní infrastrukturu s doménovým řadičem.



Obr. 9. Způsob komunikace při Azure Active Directory [47]

5.3.1 Požadavky pro službu Azure AD Connect

Před samotnou instalací aplikace je nutné splňovat určité předpoklady, které musí být nakonfigurovány, aby byla instalace provedena úspěšně. Prvotní požadavek je na fyzický nebo virtuální server a jeho prostředky, kterými disponuje. Následující tabulka ukazuje minimální hardwarové požadavky pro server s Azure AD Connect.

Tab. 4. Hardwarové požadavky serveru

Počet objektů v Active Directory	CPU	RAM	HDD
méně než 10,000	1.6 GHz	4 GB	70 GB
10,000–50,000	1.6 GHz	4 GB	70 GB
50,000–100,000	1.6 GHz	16 GB	100 GB
100,000–300,000	1.6 GHz	32 GB	300 GB
300,000–600,000	1.6 GHz	32 GB	450 GB
600,000 a více	1.6 GHz	32 GB	500 GB

Z tabulky vyplývá, že celkové hardwarové nároky serveru na provoz výrazně ovlivňuje počet objektů ve struktuře Active Directory. Tato skutečnost ovlivní především velikost operační paměti RAM, která při přechodu z 50 000 objektů na vyšší zvyšuje požadavky více než dvojnásobně oproti předchozím požadavkům. Požadavky především na paměť RAM jsou velice ostře sledované pracovníky IT, neboť právě tato paměť má vysoké pořizovací náklady a její velikost je omezena fyzickými sloty počítače. Naopak požadavky na velikost volného místa na disku je pochopitelná a roste s velikostí databáze.

Pokud máme všechny potřebné prostředky na provoz serveru, následuje další řada věcí, které budeme muset zajistit. Především musí být splněny předpoklady z licenčního hlediska, nastavení místního Active Direcotry, minimální verze operačního systému, připojení k internetu a aktuální verze .NET frameworku.

Další minimální požadavky pro provoz:

- Licence a doména
    - Azure nebo Office 365,
    - přidat a ověřit naši doménu v portálu Azure.
- Infrastruktura prostředí On-Premise
    - funkční úroveň AD minimálně verze Windows Server 2003,
    - správný překlad názvů DNS pro intranet i pro Internet,
    - otevření a povolení portů na Firewallu:
        - Interní AADC na DC – 53, 88, 135, 389, 445, 636, 49152 – 65535,

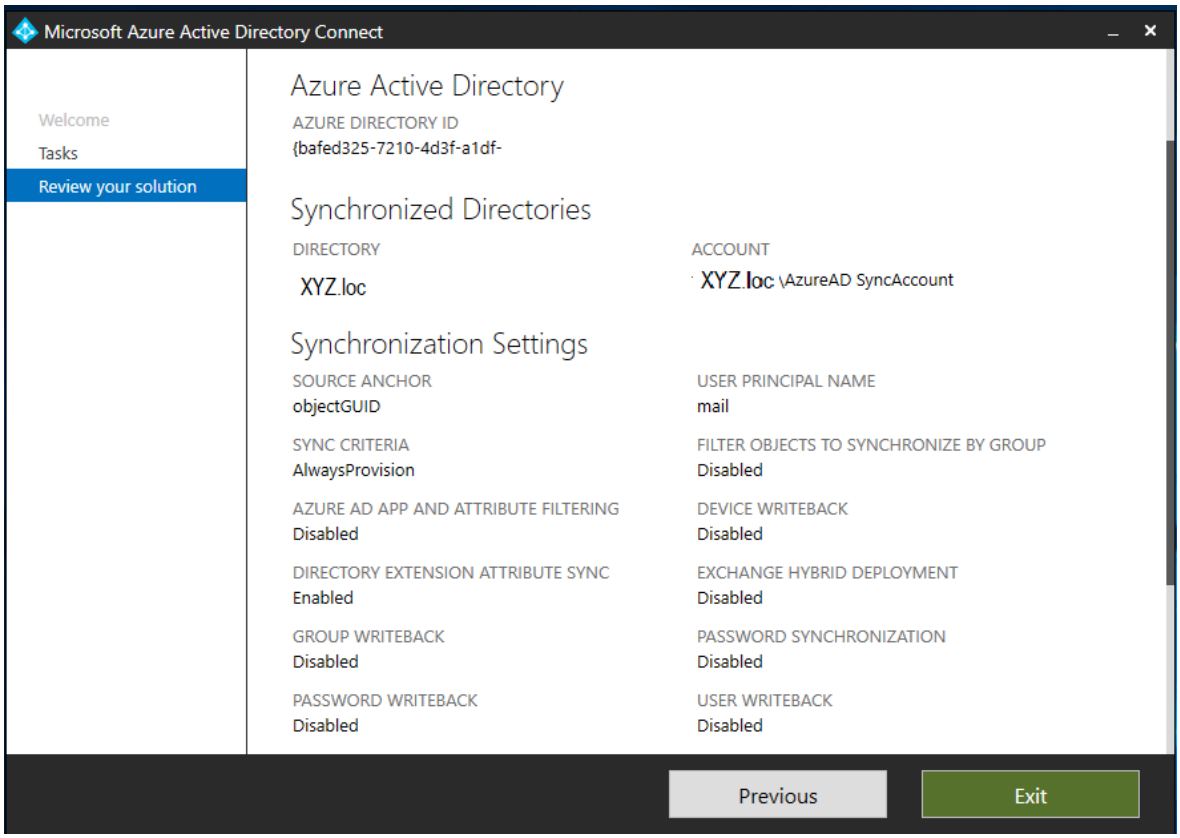
        - Externí AADC na AAD – 80, 443.
- Účty a oprávnění
    - Azure AD – Global Administrator.
- Azure AD Connect
    - operační systém – Windows Server 2008 a novější,
    - .NET Framework – 4.5.1 a novější,
    - Powershell – 3.0 a novější,
    - Microsoft SQL Server 2012 Express – do 100 000 objektů,
    - Microsoft SQL Server 2008 SP2 a vyšší – nad 100 000 objektů.

Abychom vůbec mohli přistupovat do prostředí Microsoft Azure, musíme mít zakoupenou licenci, nebo alespoň provozovat dočasnou zkušební verzi služby Azure. Nebo pokud naše firma již využívá služeb Office 365 pro přístup ke kancelářskému balíku Office, který již obsahuje licenci Azure AD. Pro korektní funkci je nutno si zakoupit vlastní doménu a přidat ji v portálu mezi spravované domény. Microsoft také samozřejmě poskytuje jeho vlastní interní subdomény pro testování, nicméně určitě nechceme naši firmu prezentovat cizí doménou ve formě „gadlenam.onmicrosoft.com“.

Nároky na prostředí v rámci firmy nejsou nikterak náročné a nekladou žádné zvláštní požadavky na provoz. Doménový řadič na funkční úrovni verze Windows Server 2003 je už zastaralý, a tudíž by mělo být ve firemním zájmu takto staré verze Windows neprovozovat. Provoz Domain Name Systém (dále jen „DNS“) je nedílnou součástí firem, kde se provozuje doménový přístup, jelikož pro provoz domény je DNS server povinností. Z pohledu bezpečnosti je nutné zasáhnout i do nastavení pravidel na Firewallu, kde spojení mezi Azure AD Connect serverem a doménovým řadičem vyžaduje poměrně mnoho protokolů a portů, i když se jedná především o základní komunikaci pouze v rámci interní sítě. K externímu připojení ke službě v cloudu je vyžadován pouhý základ, a to povolení komunikace přes http port 80 a poté zabezpečené HTTPS port 443.

Pro spojení obou prostředí je potřeba vytvořit nový servisní účet, který bude použit právě jen pro synchronizaci napříč oběma servery. Tento servisní účet musí mít také přidělená náležitá oprávnění – Global Administrator, aby mohl provádět veškeré úkony k provedení synchronizace. Jelikož tato přidělená oprávnění mají přístup k celému cloudu, je dobré server jen vytvořit a bezpečně uložit heslo s využitím jen na tuto jednu funkci.

Azure AD Connnect je jednoduchá aplikace stažená přímo z portálu Azure a musí být nainstalována na server, který běží na operačním systému minimálně Windows Server 2008 a novější, ale doporučuje se samozřejmě mít systém co nejaktuálnější. S podmínkou na OS jsou spojené i další požadavky na verzi powershellu a .NET frameworku. Pokud použijeme právě tuto starší verzi OS, budeme muset aktualizovat i tyto dva serverové komponenty na minimální verze. Použití Windows serveru 2016 obejdeme tyto požadavky právě tím, že již jsou součástí nejnovějšího serverového OS a není potřeba se jimi zabývat. Co je ale důležité podotknout, je nutnost mít dostatečnou a správnou verzi databáze SQL, neboť samotná instalace Azure AD Connect poskytuje v rámci procesu konfigurace instalace možnost zdarma nainstalovat SQL ve verzi Express, která má ale své určité limitace, a to právě v počtu objektů, které lze s ní provozovat. Pokud chceme spravovat více než 100 000 objektů, bude vyžadována vyšší edice SQL serveru.



Obr. 10. Přehled nastavení synchronizace v Azure AD Connect

Na tento stejný server bude také nainstalovaný konektor zajišťující propojení on-premise Exchange serveru s cloudovou konzolí, aby se zpřístupnila vzdálená správa a konfigurace přímo z konzole. Tento způsob propojení nepřidává navíc žádné další rozšířené funkce, nýbrž jen integruje správu do jednoho místa.

5.4 Nastavení bezpečnostních politik

Zavedením bezpečností politiky by mělo mít za následek zvýšení bezpečnosti na zařízeních, na která se tato politika bude vztahovat. Jde především o dodržování předepsaných nastavení, která výrazně ovlivňují bezpečnost dat na mobilních zařízeních, tak i při přenosu dat po internetu. Je to souhrn všech druhů nastavení a doporučení, které vedou ke zvýšení bezpečnosti s firemními daty. Do tohoto souhrnu lze uvést vynucení nastavení využívání hesla PIN, biometrických prvků a šifrování lokálního uložiště. Následně se také jedná o jakási pravidla, která nelze strojově přímo vynutit, ale pracovník se zavazuje jimi řídit. Může jít například o neposílání citlivých informací přes nezabezpečené kanály (email, sociální sítě) mimo firmu i uvnitř firmy. V případě potřeby zabezpečit velkou skupinu souborů, zpravidla z důvodu jejich přenosu prostřednictvím internetu, se ve firmě stanovuje povinnost použít nástroj 7-Zip s využitím šifrování obsahu přenášeného archivu.

V organizaci platí skupinové a systémové politiky, které upravují vlastnosti a nastavení operačních systémů, programů a uživatelského prostředí. Tyto politiky jsou vynucené a uživatelsky neměnitelné. Jejich používáním je zajišťována bezpečnost, jednotnost a funkčnost. Uživatel nemá žádnou možnost tyto politiky měnit, s touto souvislostí je i zakázáno jakýmkoliv způsobem systémové politiky blokovat.

V případě, že se uživatel při používání prostředků setká s problémem či omezením, které mu brání v plnění pracovních povinností, je povinen tuto skutečnost oznámit svému přímému nadřízenému, který dále postupuje dle svých kompetencí.

Oblast zabezpečení mobilních zařízení spadá pod jednu ze skupinových politik, kde se pracovníci dělí do dvou základních skupin, a to na bezpečnostní a zaměstnaneckou. Tyto dvě skupiny mají stejný základ vynuceného nastavení na zařízení, které musí dodržovat. U skupiny bezpečnostní jsou tyto pravidla více striktní, kdežto u zaměstnanecké skupiny se ponechává volnější nastavení, aby nebyl razantně omezen komfort užívání.

5.4.1 Skupina pro zaměstnance

Do této skupiny se řadí všichni zaměstnanci firmy, kteří k výkonu své pracovní činnosti potřebují mobilní zařízení. Ať už je to pouze mobilní telefon, notebook, nebo kombinace zařízení. Při plánování bezpečnostních pravidel pro tuto skupinu byl brán ohled především na to, aby běžní uživatelé nebyli až příliš omezováni těmito pravidly. Ale nachází se poměrně vyvážený kompromis mezi zabezpečením a komfortem.

Tab. 5. Bezpečnostní zásady pro všechny platformy

Společné zásady pro všechny platformy	
Heslo pro odemknutí zařízení	Ano
Automatické uzamčení zařízení	po 15 minutách nečinnosti
Minimální délka znaků hesla	6 znaků
Heslo musí obsahovat písmena i číslice	Ano
Expirace hesla	255 dnů
Počet posledních hesel, které se nesmí opakovat	3
Google Android	
Na zařízení nesmí být tzv. root	Ano
Vyžadováno šifrování zařízení	Ano
instalace aplikací z neznámých zdrojů	Vypnuto
USB debugging	Vypnuto
Apple iOS	
Na zařízení nesmí být tzv. jailbreak	Ano
Vyžadováno šifrování zařízení	Ano
Microsoft WindowsPhone	
Vyžadováno šifrování zařízení	Ano

V tabulce jsou zaneseny hodnoty jednotlivých nastavených bezpečnostní zásad, které jsou pomocí nástroje pro mobilní správu vynuceny na každém firemním smartphonu. Tyto zásady vychází především z obecných ustanovení ohledně základního zabezpečení elektronických zařízení, které obsahují soukromá data uživatelů. Do budoucnosti se bude přidávat k těmto pravidlům i rozsah podporovaných verzí operačních systémů, aby se předcházelo připojování starých neaktualizovaných telefonů do prostředí firmy.

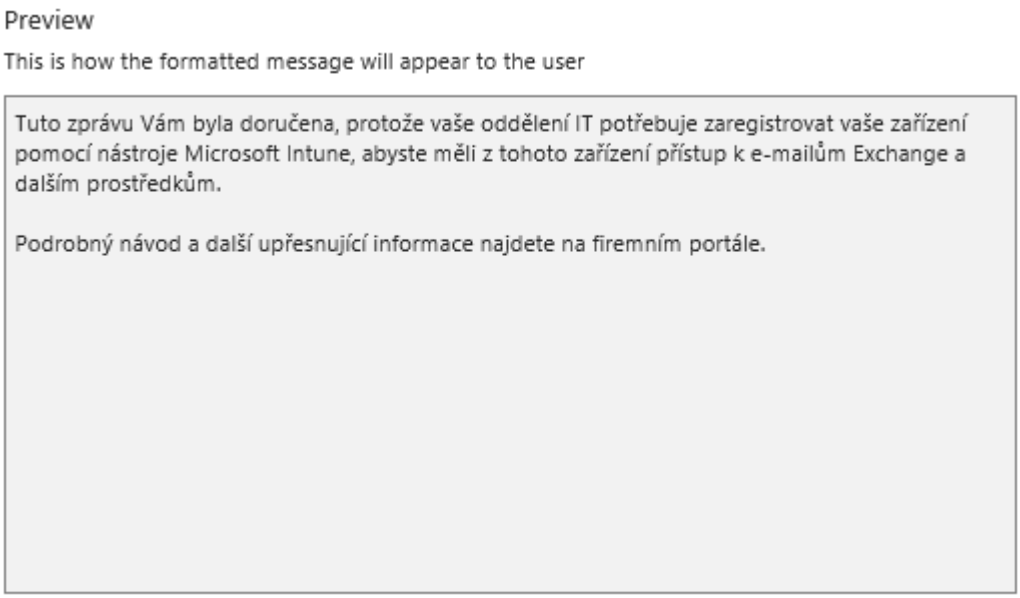
5.4.2 Bezpečnostní skupina

Do skupiny se zvýšeným zabezpečením spadají pracovníci pracující s velmi citlivými firemními daty. Zde při návrhu nastavení bezpečnostních pravidel byl kladen důraz na vyšší až nejvyšší úroveň zabezpečení než u běžných pracovníků. Míra komfortu užívání přenosného zařízení je zde daleko nižší. Této skupině je pomocí vnitřní směrnice omezen výběr mobilního telefonu pouze na iPhony od firmy Apple. Tohle omezení na jeden typ telefonu má svůj důvod ve správě MDM, protože telefony s iOS mají daleko více možností zabezpečení a správy než běžné telefony s operačním systémem Android. Členové této skupiny absolvují mnohem vetší počet školení zaměřující se na bezpečnost firemních dat, aby měli jasný přehled o aktuálních hrozbách, tak i o nových postupech ochrany firemních aktiv. Účel tohoto souboru zásad a postupů je, aby byl eliminován lidský faktor nebo alespoň minimalizován.

Bezpečnostní skupina se odlišuje od zásad pro běžné zaměstnance v nastavení minimální délky hesla, kde vzrostla povinnost mít alespoň 8 znaků. Komplexita a vynucení užití hesla k odemknutí telefonu je nutností. Automatické uzamykání telefonu bylo sníženo na pouhých 5 minut s tím, že tato hodnota je maximální, ale doporučuje se všem pracovníkům ani tohle nastavení nevyužívat, ale mít telefon ihned zamknutý po vypnutí obrazovky. V tomto případě zde byl ujednán určitý kompromis v užívání. Počet posledních hesel, které mohou být použity, byl zde nastaven na 5 předešlých hesel. Ostatní nastavení zůstávají neměnná.

5.4.3 Upozornění pro uživatele při nedodržení zásad

Vychází se z předpokladu, že každý uživatel, již před prvotní synchronizací se server Exchange, má své zařízení plně vyhovující všem předpisům a požadavkům nastavených od IT oddělení. To lze pouze předpokládat u telefonů vlastněné firmou a nelze tohle deklarovat u vlastních zařízení pracovníků. Proto je připraveno upozornění, které se doručí uživatelům do poštovní schránky, pokud nastane jakýkoliv rozpor s bezpečnostní politikou.



Obr. 11. Příklad nastavení notifikační zprávy pro uživatele

Příklad nastavení notifikační zprávy, uvádí jednoduché informace, proč je přístup na vašem zařízení zablokován, s přiloženým podrobným návodem pro další postup, jak tuto situaci vyřešit bez nutnosti zásahu IT oddělení. Tento text je pouze informační, který lze modifikovat ve výsledném emailu, který je pak zasílán přímo zainteresovaným pracovníkům. K této informaci jsou dále přidány i stručné základní informace o zařízení, ze kterého se pracovník pokouší připojit k firemnímu Exchange serveru. Mezi tyto základní informace je zahrnut

například: model zařízení, typ, ID (přidělené Exchange serverem), operační systém, IMEI (pokud je k dispozici), verze služby ActiveSync, a jako poslední položkou je uveden stav zařízení, který může nabývat stavů zablokován nebo umístěn do karantény. Poslední řádek celého seznamu pojednává o důvodu stavu přístupu, proč byl danému zařízení přiřazen takový stav. Celý informační email lze nalézt v příloze P1 na konci dokumentu.

5.5 Postup registrace zařízení do InTune

Registrace telefonů, tabletů a notebooků do prostředí správy MDM Intune je velice jednoduchá a přívětivá. Tento proces registrace umožní, jak už bylo zmíněno, přístup ke všem firemním aktivům, ke kterým máme jako pracovník přístup a právo jej užívat. Tento postup se neaplikuje pouze na firemní zařízení, ale je totožný i ve školství, kde se u jednoho notebooku nebo tabletu střídá velký počet uživatelů. Nicméně zde takovéto zařízení neregistruje sám student, ale IT pracovník v rámci dané školy.

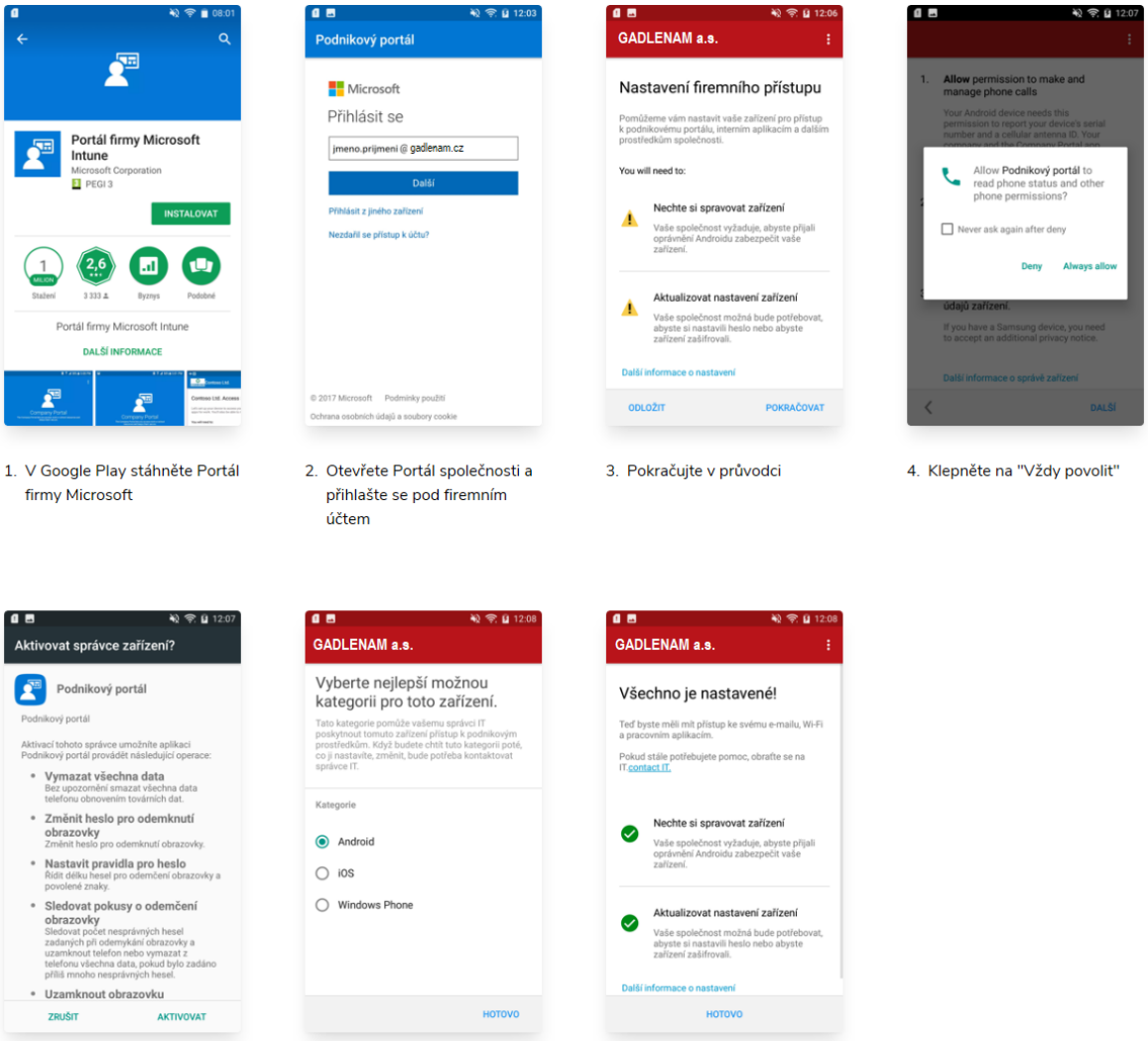
Na konci celého procesu registrace bude uživatel vyzván k výběru kategorie dle telefonu, ze kterého registraci provádí, aby odpovědní pracovníci mohli lépe rozlišovat, o jaký typ operačního systému se jedná a následně rychleji a efektivněji pomoct s případnými problémy.

5.5.1 Interní informační web

Pro snadnější orientaci v problematice mobilní správy nasazené do prostředí firmy byl zřízen jednotný informační web se všemi důležitými informacemi pro pracovníky, kde jsou především vypracovány jednotlivé postupy registrací telefonu podle operačního systému i možnost jejich odhlášení. Na webu lze také zjistit, jak si připojit svůj účet do AAD a automaticky se přiřadí licence, po tomto kroku se zpřístupní možnost přihlášení do Intune. Tohle tlačítko obsahuje i funkci odebrání licence, kterou si může sám uživatel spravovat. Samozřejmostí jsou kontakty na IT oddělení a odpovědné pracovníky, na které se lze kdykoliv obrátit s prosbou o pomoc. Celkový náhled na webovou stránku s informacemi lze nalézt v příloze P2.

5.5.2 Postup pro registraci na platformě Android

Celkový počet kroků potřebných k úspěšnému dokončení představuje pouze sedm dílčích kroků. U smartphonu s operačním systémem Android je tento postup záležitostí několika málo minut, kde se přepokládá, že daný telefon má je již připojen v Google Play s osobním účtem od Google. Nutnost připojení k internetu je také další podmínkou.

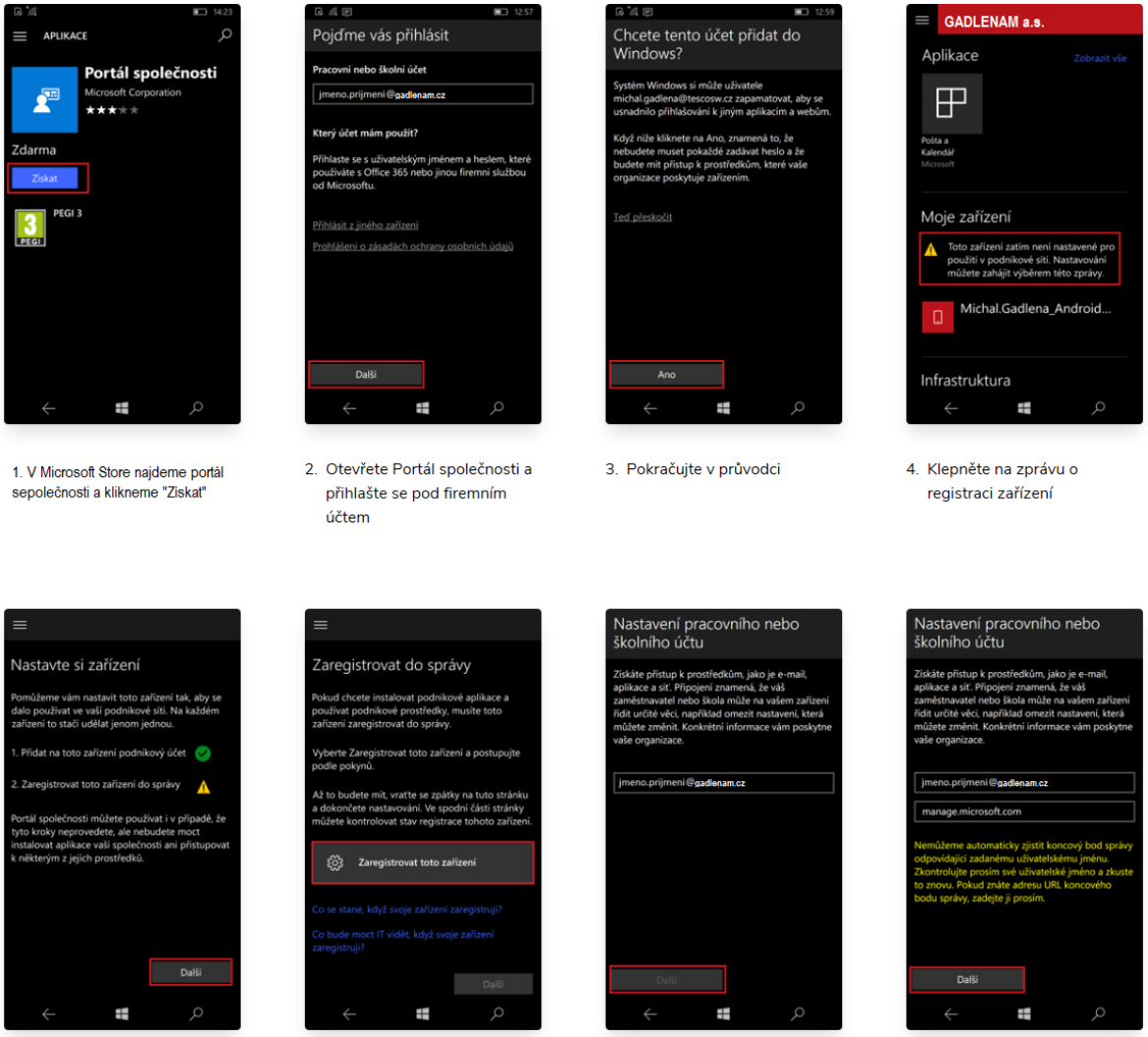


1. V Google Play stáhněte Portál firmy Microsoft
2. Otevřete Portál společnosti a přihlašte se pod firemním účtem
3. Pokračujte v průvodci
4. Klepněte na "Vždy povolit"
5. Klepněte na "Aktivovat"
6. Pokračujte v průvodci
7. Hotovo

Obr. 12. Postup registrace Android

5.5.3 Postup pro registraci na platformě Windows Phone

U systému, který vytváří stejná firma jako dodavatel řešení MDM, jímž je společnost Microsoft, lze z teoretického hlediska očekávat nejhladší průběh registrace, ale tak tomu není. Právě postup na této platformě je poněkud zmatečný a špatně zdokumentovaný, a přitom tyto neduhy paradoxně neplatí u konkurenčních platforem.



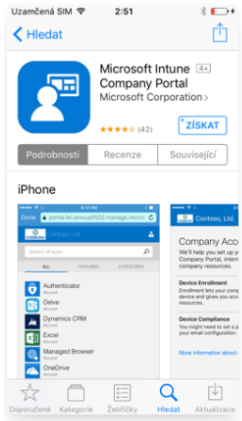
Obr. 13. Postup registrace WindowsPhone

Po instalaci aplikace „Portál společnosti“ z Microsoft Store nás nově nainstalovaná aplikace ihned vyzve k zadání firemních přihlašovacích údajů. Po přihlášení se dostaneme do prostředí aplikace, kde nyní zjistíme, že celý proces není ještě zdaleka u konce a pokračujeme dle pokynů průvodce registrací dále. Problém nastává tehdy, když narazíme na krok sedm, kde po opětovném vyplnění podnikového emailu se vrátí varovná hláška, která žádá o upřesnění serveru správy MDM. Po ručním vyplenění je vše v pořádku a hotovo.

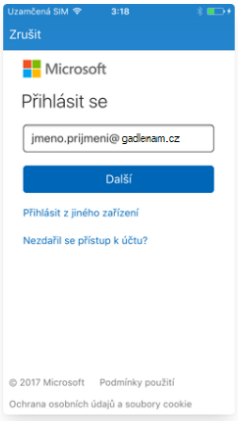
5.5.4 Postup pro registraci na platformě iOS

Jelikož trh s mobilními operačními systémy si rozdělují přinejmenším tři hlavní hráči, i tak se každý jednotlivý systém výrazně liší. Odlišný je i přístup jednotlivých platforem k přístupu postupu registrace do MDM. Ve společnosti Apple je všechna správa nastavována

skrze vestavěnou podporu profilů napříč celým portfoliem produktů od Applu. Způsob registrace je tedy poněkud odlišný a vyžaduje více uživatelské interakce než předešlé řešení. Hlavním rozdílem je zde navíc krok „importování profilu“, který vyžaduje zadání hesla telefonu a následně je uživatel vyzván k nastavení důvěry novému profilu.

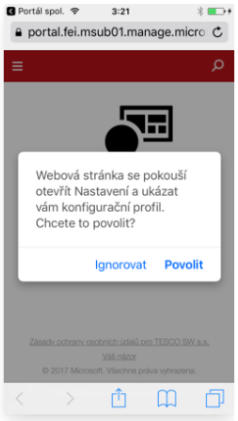


1. V App Store stáhněte Microsoft Intune Company (Portál společnosti)

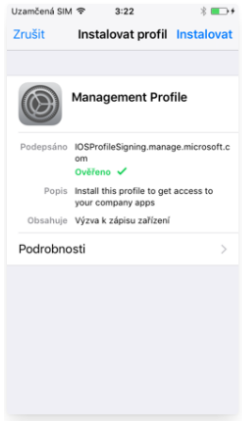


2. Otevřete Portál společnosti a přihlašte se pod firemním účtem

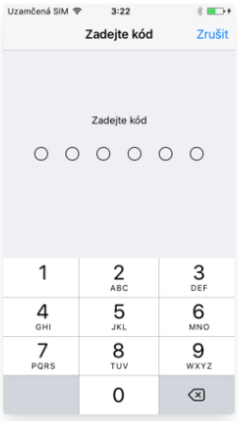
3. Pokračujte v průvodci



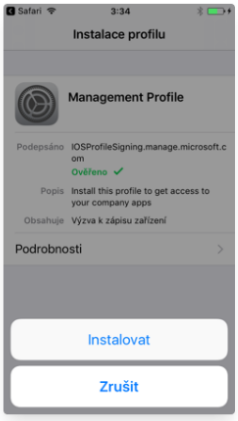
4. Klepněte na "Povolit"



5. Klepněte na "Instalovat"

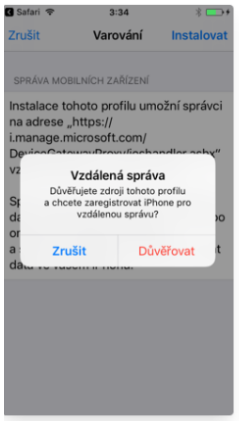


6. Zadejte kód telefonu

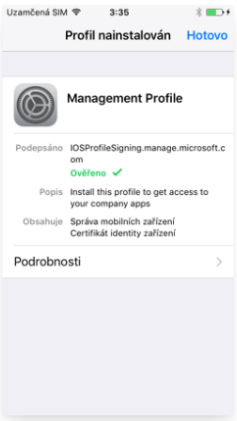


7. Potvrďte instalaci

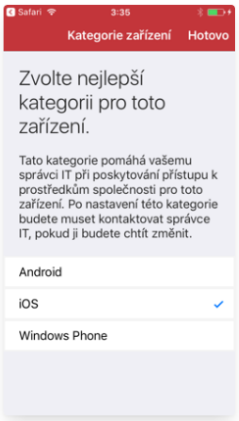
8. Klepněte na "Instalovat"



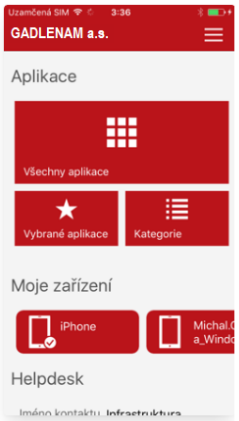
9. Klepněte na "Důvěřovat"



10. Klepněte na "Hotovo"



11. Pokračujte v průvodci



12. Hotovo

Obr. 14. Postup registrace iOS

6 TESTOVACÍ PROVOZ

Proces zabírající nejdelší časový interval z celého projektu nasazování MDM je právě testovací provoz, kde se musí nasimulovat především nejpravděpodobnější scénáře, které mohou nastat při registraci telefonů a notebooku do MS Intune.

Testování je rozděleno celkově na tři samostatné fáze. První část představuje pouze interní testování schopností softwarového nástroje, druhá a zároveň nejdelší část procesu je zaměřena na vybrané pracovníky napříč celou firmou a trvá celý kalendářní měsíc. Poslední fáze se zúčastňují všichni pracovníci a ladí se už jen menší detaily neobjevené v druhé fázi.

Samotná registrace je pouze začátek celého testovacího procesu. Následně se musí otestovat každá dílčí komponenta MDM Intune, zdali funguje korektně a v jakém časovém intervalu je schopna zareagovat od zaslání požadavku na vykonání určité operace. Nedílnou součástí jsou také bezpečnostní politiky, které musí projít nejvýraznějším testováním a na největším vzorku dostupných mobilních telefonů, aby byla konfigurace a schopnost vybraného řešení vynutit tyto politiky opravdu na každém zařízení, které se dostanou do správy firmy. Z jednou hlavních příčin, proč se taková správa nasazuje, je omezení přístupu k lokálnímu serveru Exchange k synchronizaci pošty.

V rámci tohoto testovacího provozu bylo objeveno několik závažných problémů tykajících se problémů s licencemi, nastaveních Exchange serveru, omezené funkčnosti AAD a špatné komunikace s poštovními aplikacemi. Ke všem těmto objeveným komplikacím, které nastaly, byly úspěšně nalezeny jejich příčiny. Po objevení zdroje komplikací byly všechny úspěšně odstraněny a nalezeny správné postupy, aby se jim předcházelo.

6.1 Nastavení Exchange ActiveSync přístupu

Cílem je zamezení přístupu nespravovaných zařízení k firemním poštovním službám. A povolit přístup zařízením, které synchronizují poštu za podmínky registrace zařízení pod správu firmy, a to s důrazem na minimální využití počtu licencí Intune.

Problém je v možnostech konfigurace omezování přístupu k firemním poštovním schránkám. Aby se tohoto cíle dosáhlo, je zapotřebí připojit službu Exchange s MDM Intune, jako nový nástroj pro správu přístupů k těmto poštovním službám skrze cloudovou bránu. K vykonání tohoto nastavení je nutno použít dodávaný nastroj „Exchange Active Sync on-premises connector“, který zajistí vzájemnou synchronizaci. Tento nástroj operuje ve dvou možnostech omezení. První možnost pojmenovaná „Allow access“, která zahrnuje nastavení

povolení přístupu všem zařízením připojujících se k serveru. Mobilní telefony a tablety, které patří uživatelům v zahrnutých skupinách, jsou zablokovány, pokud jsou při kontrole vyhodnoceny jako nevyhovující s bezpečnostními politikami firmy, anebo nejsou registrovány v Intune. Druhá opačná možnost s názvem „Block access“ naopak zablokuje přístup všem zařízením, která se snaží připojit na poštovní server on-premise. Následně potom také platí, že telefony a tablety patřící uživatelům ze zahrnuté skupiny, mají přístup pouze tehdy, je-li jejich zařízení úspěšně zaregistrováno a vyhovující politikám.

Z této skutečnosti vyplývá, že nelze splnit úkol využití co nejmenšího počtu licencí, protože ve firmě, kde bylo tohle nasazení použito, využívá ten samý Exchange i několik dalších dceřiných společností. Nicméně těmto společnostem by byl také omezen přístup k emailovým schránkám, kdyby byla nastavena možnost „Block access“.

K vyřešení tohoto problému proto musí být vybrána možnost první, která povoluje přístup všem zařízením právě z dceřiných firem a zamezuje jen těm, které jsou v zahrnutých skupinách. Aby mohl být tento návrh řešení proveden, musí se přiřadit licence všem uživatelům společnosti.

6.2 Dynamická skupina uživatelů dle jejich zařízení

Cílem zadání je vytvoření dynamické skupiny uživatelů dle jejich zaregistrovaných zařízeních v MDM. Například „Android Users“, do které se automaticky přidávají či odebírají uživatelé, pokud mají pod svým jménem připojen telefon či tablet s operačním systémem Android. Od tohoto cíle si vedení slibuje lepší organizaci a přehlednost nad skupinami.

Problém při plnění daného cíle nastává u služby Azure Active Directory (AAD), která v prostředí cloudu Azure má do budoucna nahradit zavedené zvyky z minulých dob, při používání on-premise služeb Active Directory (AD). Tato nová služba vylepšuje určité nedostatky ve starém řešení, kde se používají organizační jednotky dle objektů, který je do nich ukládán, například skupiny uživatelů či počítačů. V AAD jsou organizační jednotky nahrazeny globálními skupinami obsahující, jak jednotlivé uživatele, tak i počítače současně. U těchto skupin lze jednoduše využít funkci dynamického přiřazování dle vybraných vlastností zařízení, nikoliv ale uživatelů.

Pro řešení tohoto problému musel být vytvořen vlastní synchronizační skript, který v podstatě tuto funkcionalitu doplňuje do prostředí AAD. Skript funguje na bázi automatického spouštění v pravidelných intervalech po 5 minutách, kde se dotáže serveru AAD na všechny

uživatele mající nějaké zařízení. Tito vybraní uživatelé jsou nadále zpracováni a za předpokladu, že daný uživatel vlastní a má registrované zařízení s operačním systémem Android, iOS, WindowsPhone, přiřadí jej do příslušné skupiny. Naopak pokud skript při spuštění a provádění kontroly aktuálního stavu najde neshodu v podobě přebývajícího uživatele v příslušné skupině, aniž by měl zaregistrovaný podmíněný telefon s operačním systémem, tak jej ze skupiny vyloučí.

6.3 Nepodporování aplikace Microsoft Outlook

Cíl zde má za úkol sjednotit spravované prostředí v rámci celé organizace. S využitím jednotné aplikace na mobilních operačních systémech. Zde se jedná o použití aplikace od společnosti Microsoft, který je autorem emailového klienta Outlook, kde stejnojmenná aplikace je také využívána na všech pracovních stanicích v organizaci. Celkovým výsledkem je jednotná aplikační platforma napříč všemi pracovními prostředími.

Problémem se zde stává přímo společnost vybraná pro poskytování mobilní správy, a to Microsoft. Ten ve své dokumentaci uvádí seznam podporovaných emailových klientů:

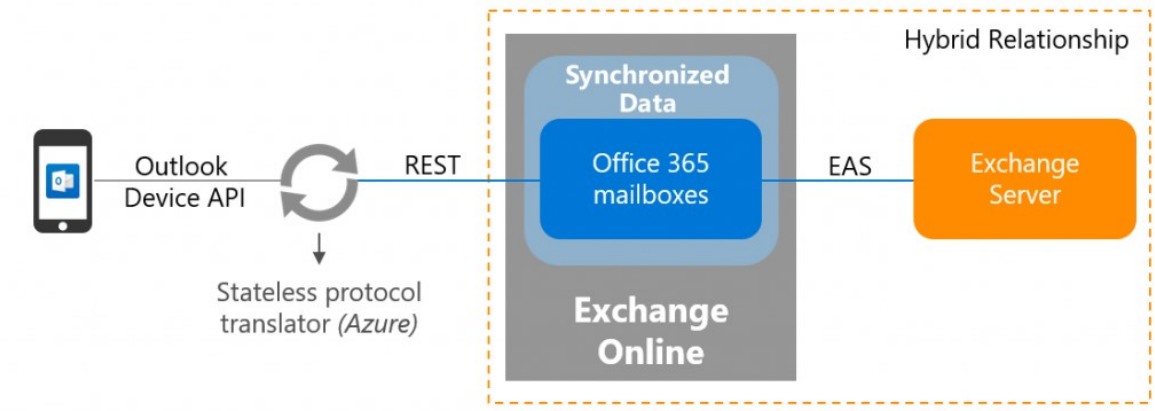
- nativní klient ve Windows Phone 8.1 a novější,
- vestavěná aplikace email v iOS
- EAS email klient jako je Gmail aplikace na Androidu 4 a vyšší,
- EAS email klienti Android for Work jak jsou Gmail nebo Nine Work. [48]

V tomto seznamu právě nenajdeme aplikaci Microsoft Outlook, která je hojně využívána v mnoha společnostech především na pracovních stanicích. Právě s touto souvislostí by dávalo nejlepší uživatelský požitek mít jednu a tu samou aplikaci i na svých telefonech. Tuto variantu bohužel ale Microsoft nepodporuje. [48]

Pokud nebudeme dbát na tento fakt a použijeme aplikaci k synchronizaci pošty, tak vše proběhne v pořádku a objeví se pošta v aplikaci. Nekorektní chování nastane až pouze tehdy, když je zapnuta funkce „Allow access“ nebo „Block access“, následně se Outlooková aplikace objeví v přehledu všech registrovaných telefonů a tabletů do Intune, jako nové zařízení a dochází tak k duplikacím. Po tomto jevu dojde k blokaci tohoto imaginárního zařízení, který je ve skutečnosti aplikace a nemůže dojít korektně k nastavením politik tak ani k jejich vyhovění a outlooku je bezpodmínečně zablokován přístup.

Vyřešení tohoto problému je v principu poněkud jednoduché, a to využívání nativních klientů specifických dle OS. Nicméně s touto variantou řešení se vedení společnosti nechtělo

smířit, a tak byly kontaktování přímo experti z partnerského programu s firmou Microsoft, kteří nám tuto skutečnost potvrdili, že se jedná opravdu o nepodporované řešení. Ale také nám předali informaci i o existujícím podporovaném scénáři, u kterého lze využívat Outlook bez sebemenších problémů.



Obr. 15. Schéma hybridního provozu Exchange služeb [49]

Nově představená architektura připojení k Exchange serveru s využitím Office 365 a Exchange online zvyšuje zabezpečení skrze mobilní aplikaci Outlook pomocí nové hybridní moderní autentizace. Umožňuje zákazníkům a uživatelům kombinovat sílu spojení AAD a Intune k zabezpečení firemních zpráv. [49]

Jakmile zákazníci Microsoftu připojí své on-premise servery k hybridní konfiguraci skrze Microsoft cloud Azure a zapnou moderní autentizaci uživatelů, mohou začít synchronizovat poštovní schránky do Exchange online. Po tomto spojení emailový mobilní klient Outlook se již nikdy nespojí právě z on-premise serverem a nebude způsobovat nekorektní chování. [49]

6.4 Bezpečnostní chyba způsobená aplikací AquaMail

Cíl je eliminovat výskyt bezpečnostní chyby objevené po spuštění testovacího provozu Intune, kde jedna konkrétní aplikace AquaMail stahuje pomocí protokolu Exchange Web Services (EWS) nepravidelně všechny emaily ze všech emailových schránek ve firmě.

Problém s emailovým klientem stahující náhodné emaily ze všech podnikových schránek měl nejvyšší prioritu na vyřešení. Nutno dodat, že tuhle aktivitu se podařilo zcela náhodně objevit u jednoho z uživatelů v testovací skupině, který z ničeho nic začal vídat cizí emaily. Po bližším prozkoumání se podařilo najít zdroj tohoto chování. Spojení, které bylo navázáno

se serverem poštovních služeb, procházelo přes firewall od firmy FortiGate, kde byla nastavena terminace Secure Sockets Layer (SSL). Tohle nastavení způsobovalo po určitém časovém intervalu právě nekorektní chování zmíněné aplikace, po každém restartu firewallu vše fungovalo správně. Terminaci SSL mohou taky provádět přímo Exchange servery, které po nastavení fungovaly bez chyby, bohužel tento přístup není přímo nejvhodnější provozovat dlouhodobě. Chyba je tedy na straně výrobce firewallu a jeho firmwaru zároveň v kombinací terminace SSL a následným vyvažováním zátěže počtu připojených klientů k serveru Exchange.

Řešením je bezprostřední aktualizace firmwaru, firewallu a rekonfigurace vyvážení zátěže, které nepovede ještě přes proxy server mezi firewallem a servery pošty. Nýbrž naopak přímo na Exchange server. Lze konstatovat, že tento problém byl způsobem špatným nastavením a včasnou neaktualizací prostředků ve firmě.

ZÁVĚR

V rámci této práce byl vytvořen návrh nasazení a konfigurace vybraného vyhovujícího softwaru pro mobilní správu zařízení do prostředí firmy. Aby se dospělo k adekvátnímu výběru správného nástroje, byl také zhotoven přehled všech nástrojů, o které firma jevila zájem. Všechny srovnávané řešení od jednotlivých dodavatelů splňovaly zadané požadavky na funkcionalitu vybíraného softwaru. Jedinými měřitelnými rozdíly byly cenové licenční tarify. Dalším rozdílem byly různé přidané hodnoty každého nástroje pro správu, kde právě vybraný software Intune měl výhodu v podobě nevyžadování duplicitních aplikací k zabezpečení firemních dat. Dalším nejdůležitějším prvkem přidané hodnoty byla korespondence možného potencionálního rozvoje firmy se zaměřením na služby, které Microsoft Intune nabízí a o jaké další možnosti se v budoucnu rozroste.

Vytvořený návrh nasazení pracoval s reálnými fakty a požadavky od zadavatelské firmy. Nicméně postup zahrnuje všechny nezbytné kroky k úspěšnému nasazení do prostředí podniku i s dostatečným časem na testování nastavení a řešení problému odhalených testovací skupinou po dobu pilotního provozu. K dosažení určitého stupně pochopení a porozumění nově zaváděnému přístupu firmy k zařízením vlastněnými pracovníky byl vypracován interní informační web se všemi základními informacemi na jednotném místě, kde lze najít především postupy pro registraci všech mobilních platforem. V souvislosti s touto myšlenkou byl kladen důraz i na průběžné zaškolování a objasňování dotazů v celém intervalu nasazování až po ostrý provoz.

V průběhu testovacího provozu bylo objeveno několik problémů, kde jeden představoval přímo bezpečnostní chybu. Celý proces testování je rozdělen na tři fáze. Všechny dílčí fáze celkově zabírají nejdelší časový úsek 40 dní. Všechny objevené chyby a nedostatky způsobené dodavatelem MDM řešení nebo chybnou konfigurací firemního prostředí se podařilo úspěšně vyřešit.

Tento kompletní návrh je možné jednoduše zobecnit natolik, že jej lze použít jako kostru pro další nasazení v rozdílných prostředích nebo za jiných podmínek.

SEZNAM POUŽITÉ LITERATURY

[1] Co je „mobilní zařízení“?, ©2007. *Fórum MobilMania.cz* [online]. [2018-04-02]. Dostupné z: http://forum.mobilmania.cz/viewtopic.php?f=15&t=23378&hilit=+Mobiln%C3%AD+za%C5%99%C3%ADzen%C3%AD+

[2] BYOD (Bring Your Own Device), ©2011-2016. *Management Mania* [online]. [cit. 2018-04-03]. Dostupné z: https://managementmania.com/cs/byod-bring-your-own-device

[3] BENEŠOVSKÁ, Michala. BYOD už je v českých firmách běžné, 2016. *Hello world.* [online]. [cit. 2018-04-04]. Dostupné z: http://www.helloworld.cz/byod-uz-je-v-ceskych-firmach-bezne/

[4] DIBLIK, Jan a Pavel ZAHRADNÍČEK. Právní aspekty BYOD (Bring Your Own Device) a jeho praktická využitelnost v českých společnostech, 2017. *Právní prostor*. [online]. [cit. 2018-04-03]. Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/pravni-aspekty-byod-bring-your-own-device-a-jeho-prakticka-vyuzitelnost-v-ceskych-spolecnostech

[5] STANČÍK, Martin. Tři způsoby zabezpečení firemní sítě v rámci politiky BOYD, 2012. *Computerworld.* [online]. [cit. 2018-04-03]. ISSN 1210-9924. Dostupné z: http://computerworld.cz/technologie/tri-zpusoby-zabezpeceni-firemni-site-vramci-politiky-boyd-49129

[6] ROUBÍK Tomáš. Na co si dát pozor při používání BYOD zařízení ve firmách?, 2014. *LUPA* [online]. [cit. 2018-04-03]. Dostupné z: https://www.lupa.cz/clanky/na-co-si-dat-pozor-pri-pouzivani-byod-zarizeni-ve-firmach/

[7] MIKUDÍK, Radek. Android s iOS drtí mobilní svět. Ostatní jsou v klinické smrti, 2016. *Mobil.iDNES.cz.* [online]. [cit. 2018-04-03]. Dostupné z: https://mobil.idnes.cz/android-s-ios-drti-mobilni-svet-dmu /mob_tech.aspx?c=A160225_194408_mob_tech_ram

[8] Marketshare of Androin versions vsi OS versions [OC], ©2018. *Dataisbeautiful.* [online]. [cit. 2018-04-03]. Dostupné z: https://www.reddit.com/r/dataisbeautiful/comments/7twb2s/marketshare_of_android_versions_vs_ios_versions_oc/

[9] Google Enterprise, ©2018. *Better Cloud.* [online]. [cit. 2018-04-03]. Dostupné z: https://www.bettercloud.com/monitor/g-suite/google-universe-mobile/

[10] What is the cost to get grante a GMS certification?, ©2018. *Hatch.* [online]. [cit. 2018-04-03]. Dostupné z: http://www.hatchmfg.com/what-is-cost-gms-license-certification/

[11] Android Logo, ©2012. *Famouslogos.* [online]. [cit. 2018-04-03]. Dostupné z: https://www.famouslogos.us/

[12] Správa mobilních zařízení, ©2018. *G Suite*. [online]. [cit. 2018-04-03]. Dostupné z: https://gsuite.google.cz/intl/cs/products/admin/mobile/#

[13] GREBEŇ, David. Kompletní historie iOS: od prvního iPhonu až po iOS 9, 2016. *Letem světem Apllem*. [online]. [cit. 2018-04-03]. Dostupné z: https://www.letemsvetemapplem.eu/2016/03/06/kompletni-historie-ios/

[14] Logo společnosti Apple, ©2014. *AplleWikipedia.* [online]. [cit. 2018-04-03]. Dostupné z: http://applewikipedia.org/index.php?title=Logo_spole%C4%8Dnosti_Apple

[15] Hromadná správa Apple zařízení ve firmách – jak to funguje (DEP, MDM, VPP), ©2018. *Wefree.* [online]. [cit. 2018-04-03]. Dostupné z: http://wefree.cz/blog/hromadna-sprava-apple-dep-mdm-vpp/

[16] Comprehensive App Deployment & Management, ©2018. *Simple MDM.* [online]. [cit. 2018-04-03]. Dostupné z: https://simplemdm.com/features/#supervision

[17] FRANCIS, Ryan. Jak správně zabezpečit mobilní pracovníky?, 2018. *Computerworld.* [online]. [cit. 2018-04-03]. Dostupné z: https://computerworld.cz/securityworld/jak-spravne-zabezpecit-mobilni-pracovniky-54638?utm_source=rss&utm_medium=web&utm_campaign=rss

[18] Jak nejlépe zabezpečit mobilní telefon – rady a tipy, ©2018. *Aktuálně.cz*. [online]. [cit. 2018-04-03]. Dostupné z: https://magazin.aktualne.cz/jak-nejlepe-zabezpecit-mobilni-telefon-rady-a-tipy/r~23ccd42ae6ce11e6b0e5002590604f2e/?redirected=1526758458

[19] MORAVEC, Petr, 2016. Čtečky otisku prstů pod drobnohledem – jak fungují?, *Mobilizujeme.* [online]. [cit. 2018-04-05]. Dostupné z: https://mobilizujeme.cz/clanky/ctecky-otisku-prstu-pod-drobnohledem-jak-funguji

[20] Microsoft Intune iOS device restriction settings, 2018. *Microsoft.* [online]. [cit. 2018-04-05]. Dostupné z: https://docs.microsoft.com/en-us/intune/device-restrictions-ios

[21] TŮMA, Ondřej. Co je PIN, ©2000-2018. *Peníze.cz.* [online]. [cit. 2018-04-05]. Dostupné z: https://www.penize.cz/slovnik/pin

[22] PIN, ©2017. *Computer Hope.* [online]. [cit. 2018-04-03]. Dostupné z: https://www.computerhope.com/jargon/p/pin.htm

[23] Šifrování dat na Androidu: Ano, nebo ne?, ©2018. *Data help.* [online]. [cit. 2018-04-05]. Dostupné z: https://www.datahelp.cz/clanky/sifrovani-dat-na-androidu--ano-nebo-ne

[24] Co je to VPN a potřebujete ji, ©2018. *vpnMentor.* [online]. [cit. 2018-04-05]. Dostupné z: https://cs.vpnmentor.com/blog/co-je-vpn-potrebujete-ji/

[25] BOŘÁNEK, Roman. VPN pro začátečníky: princip fungování, výhody a nevýhody, 2017. *Root.cz.* [online]. [cit. 2018-04-03]. Dostupné z: https://www.root.cz/clanky/vpn-pro-zacatecniky-princip-fungovani-vyhody-a-nevyhody/

[26] XAVER, Jandura. Rozpoznávání obličeje u Galaxy S8 ošálíte obyčejnou fotografií, 2017. *Samsung magazine.* [online]. [cit. 2018-04-03]. Dostupný z: https://samsungmagazine.eu/2017/04/03/rozpoznavani-obliceje-u-galaxy-s8-osidite-jednoduchym-trikem-staci-vam-k-tomu-obycejna-fotografie/

[27] ZAVŘEL, Roman. Vše, co byste měli vědět o Face ID, 2017. *Letem světem applem.* [online]. [cit. 2018-04-05]. Dostupný z: https://www.letemsvetemapplem.eu/2017/09/16/face-id/

[28] LIU, Haowei. Facial detection and recognition on mobile devices. 2015, *Amsterdam: Elsevie, Morgan Kaufmann.* ISBN 978-0-12-417045-2

[29] PIERER, Markus. Mobile Device Management: Mobility Evaluation in Small and Medium-Sized Enterprises. 2016, *Springer.* ISBN 9783658150464

[30] RŮŽIČKA, Petr. Aktualizace operačního systému, 2017. *Pohyb je život.* [online]. [cit. 2018-04-03]. Dostupné z: https://www.petrruzicka.com/blog/aktualizace-operacniho-systemu/

[31] ZECHMEISTER, Jindřich. Deset tipů na zabezpečení mobilního telefonu, 2013. *SSL Market.* [online]. [cit. 2018-04-03]. Dostupné z: https://blog.sslmarket.cz/ssl/deset-tipu-na-zabezpeceni-mobilniho-telefonu/

[32] Bezpečnost a správa mobilních zařízení, 2011. *BusinessIT.* [online]. [cit. 2018-04-04]. Dostupné z: http://www.businessit.cz/cz/bezpecnost-sprava-mobilnich-zarizeni-android-apple-mdm.php

[33] HOLUBCOVÁ, Petra a Edward PLCH. Řešení pro správu firemní mobility, 2016. *ITSystems.* [online]. [cit. 2018-04-04]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/reseni-pro-spravu-fremni-mobility.htm

[34] Samsung KNOX – technologie, která nabízí „telefon v telefonu", ©2018. *System4u.* [online]. [cit. 2018-04-04]. Dostupné z: https://www.system4u.cz/samsung-knox/

[35] Příprava aplikací pro Android na zásady ochrany aplikací pomocí nástroje Intune App Wrapping Tool, 2018. *Microsoft.* [online]. [cit. 2018-04-04]. Dostupné z: https://docs.microsoft.com/cs-cz/intune/app-wrapper-prepare-android

[36] SPEED, Tim, Darla NYKAMP, Mari HEISER, Joseph ANDERSON a Jaya NAMPALLI. Mobile security: how to secure, privatiza, and recover your devices: keep your data secure on the go, 2013. *Birmingham: Packt Publishing*. ISBN 978-1-84969-360-8

[37] MOLAG, Trevor. Microsoft EMS E3 vs E5, 2017. *Encore.* [online]. [cit. 2018-04-04]. Dostupné z: https://www.encore-business.com/blog/microsoft-ems-e3-vs-e5/

[38] LORENC, Kasia. IBM MaaS360 Enterprise Mobility Management Review, 2016. *Tom's IT Pro.* [online]. [cit. 2018-04-04]. Dostupné z: http://www.tomsitpro.com/articles/ibm-maas360-review,2-1043.html

[39] LINDER, Josh. VMware AirWatch Enterprise Mobility Management Review, 2016. *Tom's IT Pro.* [online]. [cit. 2018-04-04]. Dostupné z: http://www.tomsitpro.com/articles/vmware-airwatch-review,2-3.html

[40] FERRILL, Paul. VMware AirWatch, 2017. *PC.* [online]. [cit. 2018-04-05]. Dostupné z: https://www.pcmag.com/review/342696/vmware-airwatch

[41] MITCHELL, Robert. Výběr správného nástroje pro správu podnikové mobility, 2014. *Computerworld.* [online]. [cit. 2018-04-06]. Dostupné z: http://data.computerworlds.cz/file/specialy/BYOD-2014.pdf

[42] Enterprise Mobility + Security Pricing Options, ©2018. *Microsoft.* [online]. [cit. 2018-04-05]. Dostupné z: https://www.microsoft.com/en-us/cloud-platform/microsoft-intune-pricing

[43] IBM Security expands partner ekosystém, ©2018. *IBM.* [online]. [cit. 208-04-06]. Dostupné z: https://www.ibm.com/security/mobile/maas360

[44] Co je Intune?, 2018. *Microsoft.* [online]. [cit. 2018-04-06]. Dostupné z: https://docs.microsoft.com/cs-cz/intune/introduction-intune

[45] Multi-Factor Authentication: Better Protect Your Office 365 Data, 2018. *SherWeb.* [online]. [cit. 2018-04-05]. Dostupné z: https://www.sherweb.com/blog/office-365-multi-factor-authentication/#https://www.sherweb.com/blog/office-365-connectors-microsoft-teams/

[46] MOLAG, Trevor. What is Microsoft Enterprise Mobility + Security (EMS)?, 2017. *Encore.* [online]. [cit. 2018-04-05]. Dostupné z: https://www.encorebusiness.com/blog/what-is-microsoft-ems/

[47] Integrace místních adresářů do služby Azure Active Directory, 2018. *Microsoft.* [online]. [cit. 2018-04-05]. Dostupné z: https://docs.microsoft.com/cs-cz/azure/active-directory/connect/active-directory-aadconnect

[48] Create a conditional access policy for Exchange on-premises and legacy Exchange Online Dedicated, 2018. *Microsoft.* [online]. [cit. 2018-04-06]. Dostupné z: https://docs.microsoft.com/en-us/intune/conditional-access-exchange-create

[49] SMITH, Ross. A new architecture for Exchange hybrid customers enables Outlook mobile and security, 2018. *Microsoft.* [online]. [cit. 2018-04-06]. Dostupné z: https://blogs.technet.microsoft.com/exchange/2018/04/02/a-new-architecture-for-exchange-hybrid-customers-enables-outlook-mobile-and-security/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BYOD	Bring your own device.
OS	Operační systém.
TV	Television
SBC	Single Board Computer
GMS	Google Mobile Services
MDM	Mobile device management
DEP	Device Enrollment Program
SMS	Short message service
QR	Quick Response code
PIN	Personal Identification Number
SIM	Subscriber identity module
Wi-Fi	Wireless Fidelity
SD	Secure Digital
VPN	Virtual private network
3D	Trojrozměrný
IT	Information technology
SCCM	System Center Configuration Manager
GPS	Global Positioning Systém
SE	Security Enhanced Android
AAD	Azure Active Directory
EMM	Enterprise mobility management
MAM	Mobile application management
EMS	Enterprise Mobility Security
RAM	Random Access Memory

AIP	Azure Information Protection
ATA	Microsoft Advanced Threat Analytics
SSO	Single Sign-On
AD	Active Directory
ADFS	Active Directory Federation Service
CPU	Central processing unit
HDD	Hard Disk Drive
DNS	Domain Name Systém
AADC	Azure AD Connect
DC	Domain Controller
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
SQL	Structured Query Language
ID	Identification
IMEI	International Mobile Equipment Identity
EWS	Exchange Web Services

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P 1: PŘIJATÝ INFORMAČNÍ EMAIL

Odpovědět Odpovědět všem Přeposlat Rychlé zprávy

Microsoft Outlook | Gadlena Michal

Vašemu mobilnímu zařízení byl odepřen přístup na server prostřednictvím služby Exchange ActiveSync kvůli zásadám serveru.

Vaše mobilní zařízení se nebude moci synchronizovat se serverem prostřednictvím služby Exchange ActiveSync kvůli zásadám přístupu definovaným na serveru.

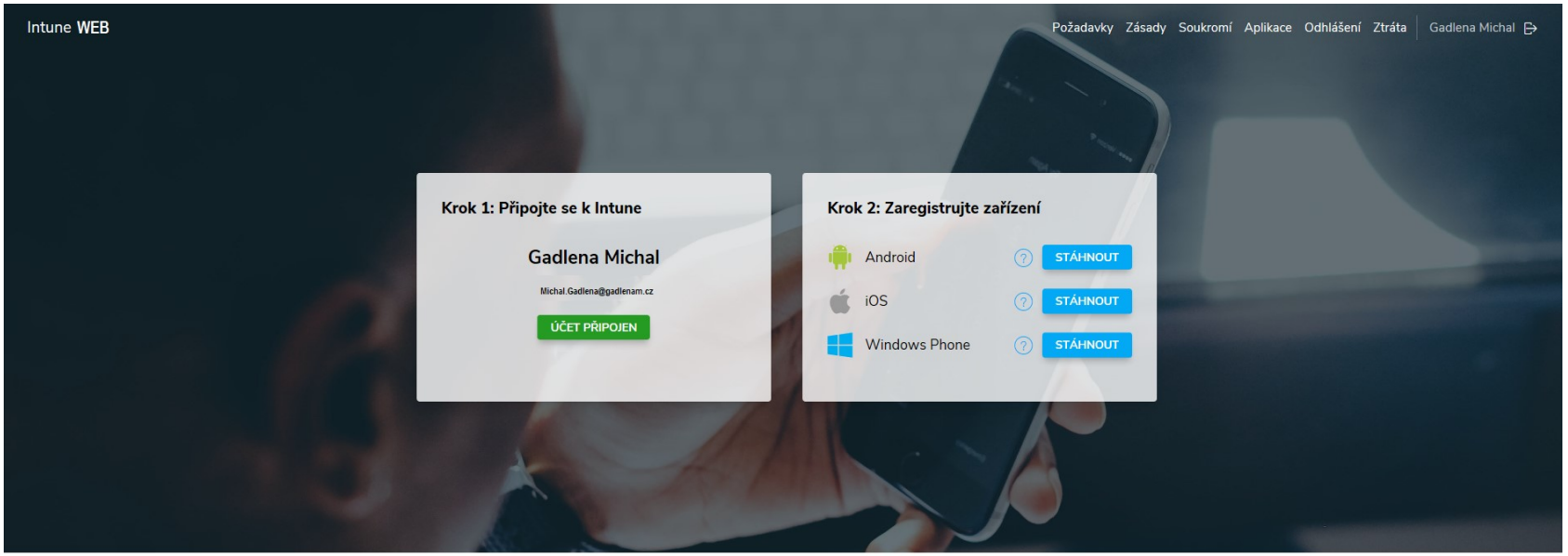
Tuto zprávu jste obdržely, protože vaše oddělení IT potřebuje zaregistrovat vaše zařízení pomocí nástroje Microsoft Intune, abyste měli z tohoto zařízení přístup k e-mailům Exchange upřesnující informace najdete na firemním portále.

Informace o vašem mobilním zařízení:

Model zařízení:	Android
Typ zařízení:	Android
ID zařízení:	androidc185730680
OS zařízení:	Android 7.1.2
Agent uživatele zařízení:	Android/7.1.2-EAS-1.3
IMEI zařízení:	
Verze služby Exchange ActiveSync:	14.1
Stav přístupu k zařízení:	Blocked
Důvod stavu přístupu k zařízení:	Individual

Odesláno v 10. 4. 2018 19:08:40

PŘÍLOHA P 2: INTERNÍ INFORMAČNÍ WEB



Požadavky na zařízení

Jaké jsou požadavky kladené na zařízení pro jednotlivé platformy?

- Na zařízení nesmí být tzv. root
- Vyžadováno šifrování zařízení
- Vypnutá instalace aplikací z neznámých zdrojů
- Vypnutý USB debugging

- Na zařízení nesmí být tzv. jailbreak

- Vyžadováno šifrování zařízení