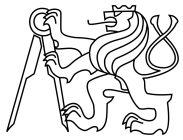
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



ZADÁNÍ DIPLOMOVÉ PRÁCE

Název:	Využití konceptu BYOD a jeho zabezpečení v bankovním prostředí
Student:	Bc. Vojtěch Dlápal
Vedoucí:	Ing. Pavel Krejčí
Studijní program:	Informatika
Studijní obor:	Webové a softwarové inženýrství
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce letního semestru 2017/18

Pokyny pro vypracování

Definujte klíčové faktory a rizika využití BYOD v bankovním prostředí. Analyzujte dostupná existující řešení BYOD, zejména z pohledu bezpečnosti. Ve vybrané bankovní organizaci analyzujte požadavky na připojení vlastních zařízení a identifikujte hlavní hrozby související s nasazením BYOD. Analyzujte stávající bezpečností procesy v připojování nefiremních zařízení do její vnitřní sítě. Vyberte nejvhodnější variantu na trhu dostupného řešení a konfrontujte ji s praxí ve vybrané organizaci. Konzultujte navrhované řešení se zástupci vybrané organizace a stanovte doporučení pro nasazení. Navrhněte nasazení řešení BYOD. Zhodnoťte uskutečnitelnost řešení a analyzujte benefity a rizika spojená se zavedením navrženého konceptu.

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

prof. Ing. Pavel Tvrdík, CSc.
děkan

V Praze dne 21. ledna 2017

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra softwarového inženýrství

Diplomová práce

Využití konceptu BYOD a jeho zabezpečení v bankovním prostředí

Bc. Vojtěch Dlápal

Vedoucí práce: Ing. Pavel Krejčí

8. května 2017

Poděkování

Děkuji technickým konzultantům této práce Viktoru Fukovi a Tomáši Prjachovi za to, že mi byli trpělivými průvodci labyrintem korporátního světa.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 8. května 2017 .....

Odkaz na tuto práci

Dlápal, Vojtěch. *Využití konceptu BYOD a jeho zabezpečení v bankovním prostředí.* Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2017.

Abstrakt

Problematika BYOD neboli používání zařízení mimo vlastnictví firmy k pracovním úkolům je čím dál více aktuální. Tato práce analyzuje a řeší BYOD s ohledem na potřeby vybrané bankovní instituce. Vzhledem ke specifikům bankovního prostředí analyzuje související hrozby a navrhuje konkrétní technická opatření pro zvýšení bezpečnosti.

Klíčová slova BYOD, Bezpečnost IT, VDI, EMM, MAM, MDM, VMware Horizon FLEX, BlackBerry Enterprise Mobility Suite

Abstract

The issue of BYOD which means use of devices not in company's ownership for working purposes is nowadays more and more current. This thesis analyzes and deals with BYOD with regard to the needs of a selected banking institution. In view of the specifics of the banking environment, it analyzes the related threats and proposes specific technical measures to increase security.

Keywords BYOD, IT Security, VDI, EMM, MAM, MDM, VMware Horizon FLEX, BlackBerry Enterprise Mobility Suite

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Cílem této práce bylo zhodnotit koncept BYOD a jeho využití v bankovním prostředí. Analýza probíhala ve vybrané bankovní organizaci, požadavkem bylo najít vhodné řešení pro BYOD, s důrazem především na bezpečnost.

Tato práce probíhala v úzké spolupráci s vybranou bankovní organizaci, a to formou schůzek a konzultací zprostředkovaných oddělením IT Security. Práce odpovídá na otázky, co to BYOD je, co vede společnosti k úvahám o tomto konceptu a jaké jsou možnosti řešení. Na základě analýzy vybrané bankovní organizace vybírá nejvhodnější řešení na aktuálním trhu a stanovuje doporučení pro jejich nasazení. Navržená řešení jsou vyhodnocena na základě benefitů a rizik spojených se zavedením a zpětné vazby od vybrané organizace.

Kapitola 1 je zaměřena na BYOD jako termín. Definuje jej s použitím několika zdrojů a uvádí jej do kontextu s aktuální situací v České republice i zahraničí. Zmiňuje důvody, proč je vhodné, aby se firmy problematikou zabývaly. Dále podrobněji popisuje obecně známe benefity a hrozby související se zavedením konceptu do firem. Závěr kapitoly se zabývá podněty nutnými ke zvážení z hlediska firemních politik, právního prostředí a především aktuální situace v oblasti kybernetické bezpečnosti.

Kapitola 2 seznamuje čtenáře s výsledky analýzy vybrané bankovní organizace. Nejdříve je organizace krátce představena a jsou vyjmenována některá specifika tohoto typu organizací. Dále je podrobně analyzován stávající proces připojování nefiremních zařízení do firemní sítě včetně použitých technických prostředků a tento proces je dále podroben analýze souvisejících hrozeb. V neposlední řadě jsou analyzovány známé požadavky na BYOD v dané organizaci a typické skupiny uživatelů a jejich potřeb. Závěr kapitoly se zabývá projekty dotýkajícími se problematiky BYOD, které byly v organizaci uskutečněny již dříve.

Kapitola 3 se zaměřuje na analýzu existujících řešení na trhu. V první části jsou definovány různé pohledy na BYOD, a to na základě vlastnictví zařízení, typů zařízení a způsobu přístupu do datové sítě. Dále je čtenář seznámen se známými technickými řešeními pro BYOD. Na základě vlastností známých

řešení je odděleně zvolen vhodný přístup řešení pro notebooky a mobilní zařízení. Pro tyto přístupy jsou vyhodnoceni nejvýznamnější poskytovatelé.

V kapitole 4 je podrobně popsán návrh řešení pro BYOD. Volba produktů pro uskutečnění řešení je odůvodněna a taktéž je popsána jejich funkcionalita. Závěr kapitoly se věnuje nasazení vybraného řešení jak po technické stránce, tak po stránce formální.

Poslední kapitola vyhodnocuje uskutečnitelnost navrženého řešení a analyzuje benefity a rizika spojená se zavedením navrženého konceptu.

Kapitola 1

Charakteristika BYOD

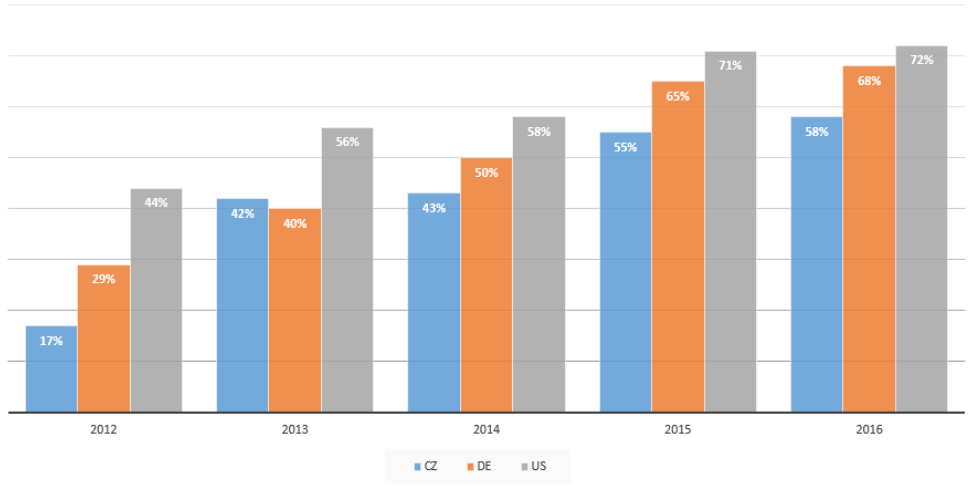
Tato kapitola je zaměřena na BYOD jako termín. Definuje jej s použitím několika zdrojů a uvádí jej do kontextu s aktuální situací v České republice i zahraničí. Zmiňuje důvody, proč je vhodné, aby se firmy problematikou zabývaly. Dále popisuje obecně známé benefity a hrozby zavedení konceptu do firem. Závěr kapitoly se zabývá podněty nutnými ke zvážení z hlediska firemních politik, právního prostředí a především aktuální situace z hlediska kybernetické bezpečnosti.

1.1 Trendy v ICT pro spotřebitele

Podle ředitele odboru statistik a rozvoje Českého statistického úřadu Martina Mana v [19]: *Je zajímavé, že počet uživatelů internetu převyšuje počet uživatelů počítače. Je to dáno hlavně rozmachem chytrých telefonů a jiných přenosných zařízení, která jsou častěji využívána i k přístupu na internet. Lze předpokládat, že internet se ve spojení s mobilem brzy stane široce rozšířenou technologií používanou napříč všemi věkovými a vzdělanostními kategoriemi.* Podle předsedkyně Českého statistického úřadu Ivy Ritschelové v citátu z [19] z května 2016: *Až do roku 2013 dominovaly českým domácnostem klasické stolní počítače. Vloni je vystřídaly počítače přenosné. Mělo je 55 % všech domácností, resp. 75 % domácností, které jsou vybaveny počítačem.*

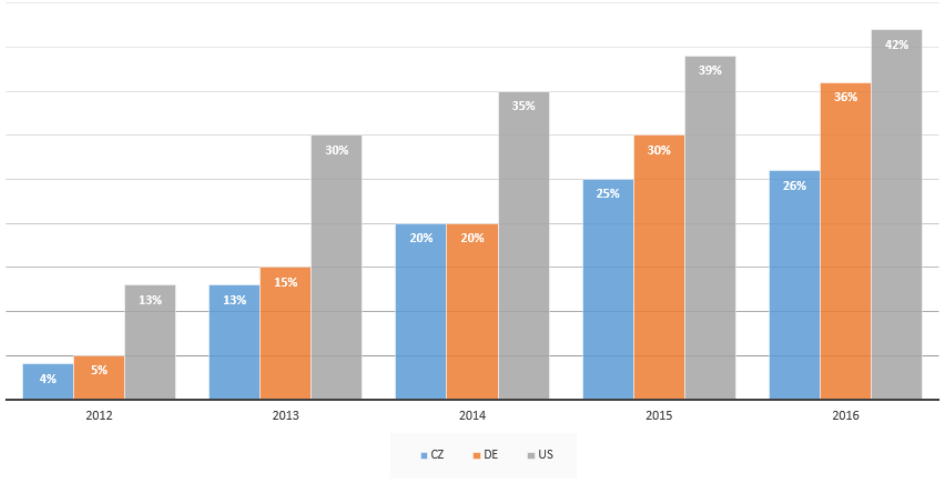
Podle výzkumu provedeného společností TNS Infratest pro společnost Google [1] vlastnilo v roce 2016 v České republice chytrý telefon připojený k internetu 50 % všech obyvatel. To je oproti 17 % z roku 2012 drastický nárůst a je možné pozorovat dále vzrůstající trend 1.1. Dále je zřejmé, že trend v České republice bude dále dohánět rozšíření chytrých mobilních telefonů v technologicky vyspělejších zemích jako jsou Spojené státy, nebo sousední Německo. Ve Spojených státech dosáhl počet vlastníků chytrých mobilních v roce 2016 72 %.

Jiným typem zařízení, která zaznamenávají zvýšenou popularitu, jsou tablety. V roce 2012 vlastnila v České republice tablet připojený k internetu 4 % oby-



Obrázek 1.1: Poměrná část uživatelů chytrých telefonů k celé populaci v České republice, Německu a spojených státech. Zdroj: [1].

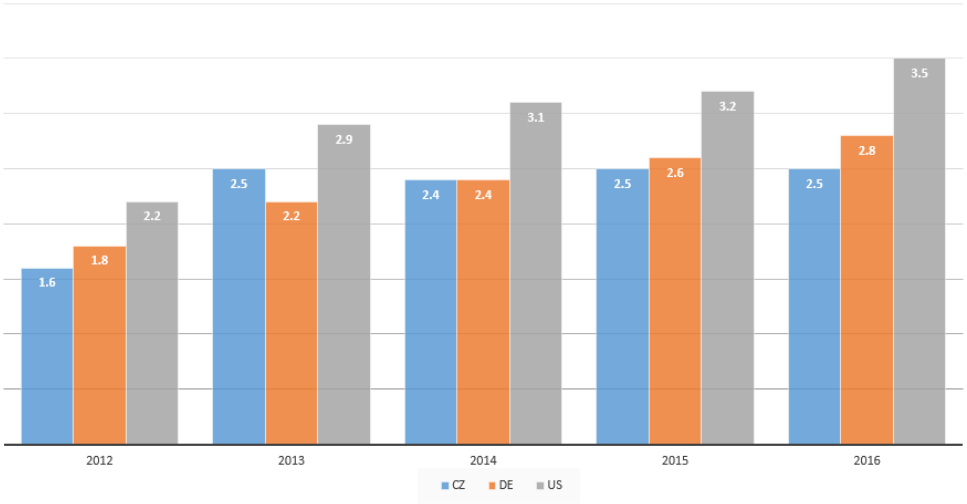
vatelstva. V roce 2016 to bylo již 26 %, což je více než šestinásobek uživatelů v rozmezí čtyř let. V USA vlastní tablet připojený k internetu dokonce 42 % obyvatelstva a trend je nadále stoupající.



Obrázek 1.2: Poměrná část uživatelů tabletů k celé populaci v České republice, Německu a Spojených státech. Zdroj: [1].

Další zajímavou statistikou je průměrný počet zařízení připojených k síti internet na jednoho obyvatele daného státu v daném státě. V roce 2012 jeden obyvatel České republiky vlastnil v průměru 1,6 zařízení, zatímco v roce 2016

to bylo 2,5. Průměrný Američan vlastnil v roce 2016 3,5 zařízení připojených k internetu. To znamená s nejvyšší pravděpodobností počítač, chytrý telefon, tablet a další zařízení.



Obrázek 1.3: Průměrný počet zařízení připojených k internetu na obyvatele v České republice, Německu a Spojených státech. Zdroj: [1].

Tato čísla ukazují, že počet obyvatel vlastnících zařízení z oblasti informačních a komunikačních technologií v posledních letech dramaticky roste. Lidé vlastnící soukromé zařízení si vytvářejí návyky a začínají upřednostňovat některé technologie nad jinými.

Své návyky na obsluhou ICT ve svém soukromém životě by tak někteří zaměstnanci rádi začali uplatňovat i v životě pracovním. To může přinést jak zaměstnanci tak zaměstnavateli mnohé výhody, ale zároveň mnohá úskalí, se kterými je třeba se vyrovnat. Nastolená praxe, kdy zaměstnanec používá své vlastní zařízení k pracovním účelům, se souhrnně označuje termínem BYOD.

1.2 BYOD jako termín

BYOD je zkratka v anglickém jazyce znamenající "Bring your own device". Oxfordský slovník [20] vysvětluje tento termín jako postup vedoucí k umožnění zaměstnancům organizace používat jejich vlastní počítače, chytré telefony a další zařízení k pracovním účelům.

Slovník Cambridge [21] definuje BYOD jako postup firem nebo škol, který říká, že zaměstnanci nebo studenti si mohou přinést své vlastní počítače, telefony, atd. do zaměstnání nebo školy za účelem jejich využití k práci.

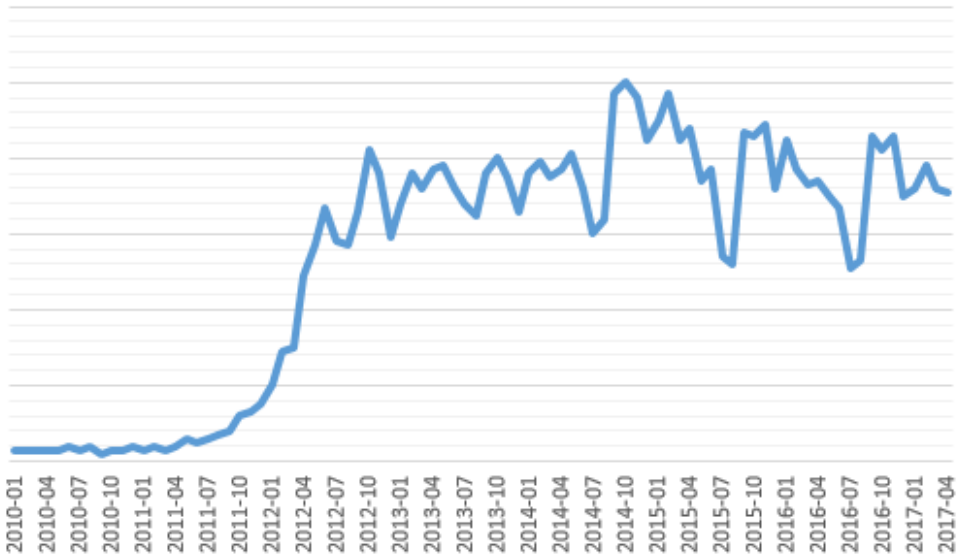
Poradenská společnost Gartner [22] BYOD definuje jako *alternativní strategii povolující zaměstnancům, obchodním partnerům a dalším uživatelům po-*

užívání osobně zvolených a zakoupených koncových zařízení ke spouštění podnikových aplikací a přístupu k datům. To typicky znamená chytré telefony a tablety, ale tato strategie může být také použita pro osobní počítače. Může obsahovat i finanční kompenzace.

Konzultační společnost Deloitte [23] definuje BYOD jako použití zařízení vlastněných zaměstnancem pro přístup k podnikovému obsahu nebo sítím. Definici dále upřesňuje ve třech kategoriích, a to zařízení, schopnosti a charakteristika.

Zařízení jsou dále specifikována jako chytrý telefon, tablet, nebo počítač vybavené procesorem. Schopnosti se mohou lišit od pouhého přístupu k internetu skrze firemní síť po přístup k podnikovým aplikacím a systémům. Charakteristikou BYOD může být používání vlastních zařízení jako doplňku k firemním zařízením, jako náhrady za firemní zařízení, nebo povolení k užití zařízení, které firma není zaměstnanci ochotna zajistit vlastními zdroji.

Podle dat ze služby Google Trends [2] se výraz BYOD začal rozšiřovat začátkem roku 2012. Graf 1.2 ukazuje popularitu vyhledávání výrazu BYOD za použití vyhledávače Google v čase vztaženém relativně k období, kdy byl zadaný výraz vyhledáván nejčastěji. Je zřejmé, že zájem o tuto problematiku nepolevuje.



Obrázek 1.4: Relativní popularita vyhledávání termínu BYOD vztažená k maximální popularitě v daném období podle Google Analytics Zdroj: [2].

Článek [24] zmiňuje mnohé výhody modelu, kdy zaměstnanci používají svá vlastní zařízení, jako například zvýšenou flexibilitu a produktivitu zaměstnanců. Dále zmiňuje snížení nákladů na technickou podporu zařízení, jelikož za svá zařízení si zaměstnanci odpovídají sami.

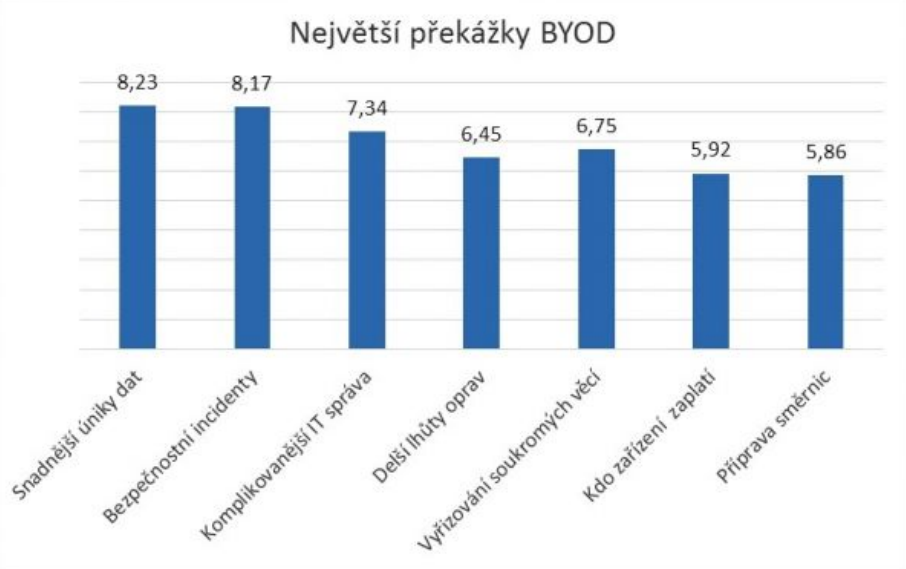
Na druhou stranu článek zmiňuje nutnost zavedení omezujících pravidel, jelikož nefiremní zařízení s sebou přinášejí řadu hrozeb jako jsou úniky dat či napadení firemní infrastruktury škodlivým softwarem. Další zmíněné negativum osobních zařízení ve firemním prostředí je nebezpečí využívání pracovní doby k soukromým účelům jako je hraní her, streamování videí a další činnosti snižující pracovní morálku.

Vzhledem k masovému rozšíření informačních technologií mezi spotřebiteli se stává pro firmy nutností zaujmout k soukromým zařízením jednoznačný postoj. BYOD zařízení ve firemním již nejsou pouze možností, ale každodenní realitou.

V době, kdy mnozí zaměstnanci vlastní výkonné chytré telefony, tablety, či dokonce nositelnosti a vnášejí je do firemního prostředí je nutné nastavit jasná pravidla, aby byla chráněna firemní infrastruktura a data.

Podle článku Pavla Housera v Hospodářských novinách [25] již BYOD do firem prorostlo a stalo se realitou i přes snahu některých firem o zákaz. Autor tvrdí, že na konceptu BYOD vydělaly především firmy, které jej pochopily nejen jako hrozbu, ale i jako příležitost.

Naopak podle tiskové zprávy společnosti Intel publikované v Hospodářských novinách [3] vítá koncept BYOD pouze 7 % českých firem, zbytek se k tématu staví odměřeně. Respondenti jejího průzkumu mají výhrady především k bezpečnosti, viz 1.2.



Obrázek 1.5: Největší negativa BYOD podle průzkumu společnosti Intel ohodnocené ve škále 1 až 10. Zdroj: [3].

Společnost Deloitte ve svém článku [23] uvádí tři možné přístupy k BYOD. Tolerovaní, zákaz nebo řízený BYOD program. Zatímco zákaz s sebou nese

vysoké riziko nerespektování zaměstnanci, a tím pádem i riziko bezpečnostní, řízený BYOD program s sebou nese náklady na přípravu, zaškolení a provoz.

Jako hlavní výhody uvádí:

- Snížení nákladů na IT
- Zvýšení produktivity
- Zvýšení spokojenosti zaměstnanců
- Lepší porozumění zákazníkům
- Lepší operační flexibilita

Snížení nákladů tkví především v podpoře. Zaměstnanci si musí vyřešit problémy se svým hardwarem na vlastní náklady. Dále je uvedeno, že zaměstnanci mají tendenci si pořizovat výkonnější zařízení, než by jim poskytla jejich firma.

Zvýšení produktivity se projevuje zvýšením ochoty pracovat mimo pracovní dobu, zvýšením pracovní efektivity vzhledem možnosti práce se známým zařízením a v neposlední řadě užíváním moderních technologií, které by jinak nemusely být pro zaměstnance dostupné.

Spokojenost zaměstnanců je zvýšená díky tomu, že si mohou vybrat zařízení, které jim nejlépe vyhovuje. Porozuměním zákazníkům je myšleno přiblížení se zákazníkům díky širší paletě zařízení používaných ve firmě a tím pádem lepšímu pochopení způsobu, jakým mohou zákazníci pracovat s veřejnými aplikacemi. Zaměstnanci s nejmodernějšími technologiemi také vylepšují obraz firmy.

Zvýšená operační flexibilita se projevuje u jednoduššího náboru a zaškolování nových zaměstnanců, jednoduššího začleňování zaměstnanců z firem po akvizicích, jednodušší práce s kontraktory a dále možností práce z domu.

Podle studie [26] trend užívání spotřebních zařízení a aplikací k pracovním účelům způsobuje střety zájmů s IT oddělením. Jedná se o střet z hlediska cílů, střet chování a střet identity. Zatím co cílem IT oddělení je zařízení kontrolovat, zaměstnanci a jejich vlastní zařízení jim to ztěžují. Zaměstnanci i s vlastními zařízeními předpokládají, že IT oddělení jim bude schopné pomoci řešit jejich problémy, ale to bohužel v případě použití nestandardních zařízení a postupů není možné. Konflikt identity znamená jev, kdy se s příchodem BYOD mění role IT oddělení, ale jeho zaměstnanci mají problémy ji uchopit.

1.3 Aspekty BYOD politiky

Pro úspěšné nasazení BYOD programu do firmy je nezbytně nutné nastavit jasná pravidla.

Společnost Deloitte v [23] doporučuje věnovat se následujícím aspektům:

- Způsobilost zaměstnanců
- Příspěvky na BYOD
- Model podpory pro soukromá zařízení zaměstnanců
- Školení zaměstnanců a řízení změn
- Soukromí a legislativa

Ne všechny pracovní úkony je možné provádět na nefiremních zařízeních, proto je třeba určit, pro které zaměstnance je BYOD program vhodný. Je dobré zvážit zda a jakým způsobem přispívat zaměstnancům na jejich zařízení používaná k práci, přičemž způsob dotace by měl být co nejjednodušší. Také je zapotřebí nastavit mechanismus pro řečení problémů. Osvědčila se různá komunitní fóra a diskuzní skupiny, avšak pro komplexnější problémy může být třeba konzultace se specialistou. Dále je třeba skloubit používání soukromých zařízení s firemními politikami. Je nutné seznámit zaměstnance s bezpečnostními riziky, která z BYOD plynou.

Požadavky na zabezpečení firemních dat často mohou být v rozporu s požadavky zaměstnanců na jejich soukromí. Jedná se například o požadavek zaměstnavatele mít možnost vzdáleně vymazat data ze zařízení po odchodu zaměstnance z firmy, na druhou stranu zaměstnanec nemá zájem na tom, aby zaměstnavatel měl přístup k jeho soukromým datům nebo monitoroval jeho aktivity.

1.4 Právní prostředí v ČR

Právními aspekty BYOD v prostředí českých společností se zabývá analýza advokátů kanceláře Havel, Holásek & Partners z ledna 2017 [27]. Český právo BYOD přímo neupravuje a proto je třeba vycházet z ustanovení zákoníku práce. Podle § 2 zákoníku práce je *zaměstnavatel povinen vytvářet zaměstnanci podmínky pro plnění pracovních úkonů a poskytnout mu k tomu pracovní pomůcky.*

Zákon umožňuje zaměstnanci taktéž použít pomůcky vlastní, ale musí to být dobrovolné rozhodnutí na základě dohody se zaměstnavatelem. Zároveň podle § 190 odst. 1 zákoníku práce, musí být zaměstnanci poskytnuta kompenzace za opotřebení.

Dalším zjištěním analýzy je, že pokud zaměstnanec odmítne využívat BYOD, musí mu zaměstnavatel nabídnout jiné řešení. Pokud by se tak nestalo, *zaměstnanec bys se mohl odvolat na nemožnost vykonávat práci pro překážku na straně zaměstnavatele ve smyslu § 208 zákoníku práce a požadovat náhradu mzdy/platu ve výši průměrného výdělku.*

Dohoda se zaměstnancem může být ve formě dodatku k pracovní smlouvě nebo smlouvou samostatnou. Nesmí vést k rozdílnému zacházení k zaměstnancům, kteří do BYOD programu nevstoupili. Kompenzace musí být odlišena od firemních bonusů a mzdy, výše však není stanovena.

Analýza [27] doporučuje vydání interní směrnice, která stanoví práva a povinnosti zaměstnance. Je třeba vzít v potaz, že směrnice nesmí zaměstnanci ukládat povinnosti nad rámec zákona, a proto je některé záležitosti lepší upravovat přímo v dohodě se zaměstnancem.

V době psaní této práce probíhá v parlamentu ČR legislativní proces novelizace zákona č. 262/2006 Sb. jako sněmovní tisk č. 903/0, který se problematiky BYOD taktéž může dotknout.

Podle Pavla Marce z advokátní kanceláře Novalia [28] novela zákona předjímá, a tím pádem legalizuje BYOD. Doporučuje platit zaměstnancům měsíční nezdanitelné paušály jako kompenzaci za BYOD a zároveň jako kompenzaci nákladů v režimu tzv. "home office". Autor tvrdí, že forma paušálu usnadní administrativu, je osvobozený od daně, ale přitom snižuje daňový základ.

1.5 BYOD z hlediska bezpečnosti

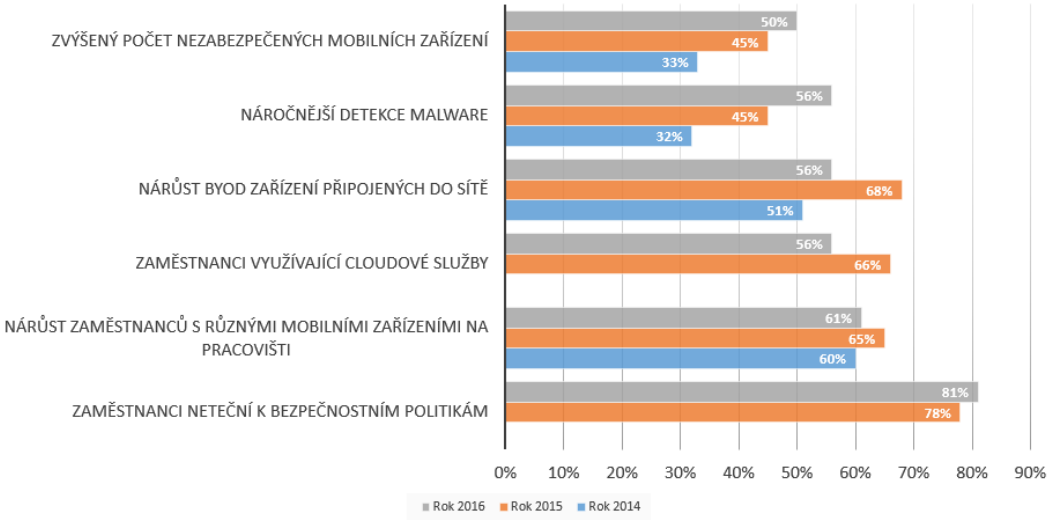
V roce 2016 provedla společnost Ponemon Institute průzkum mezi 694 odborníky na IT a IT bezpečnost ve Spojených státech [4]. Zaměřuje se na hodnocení rizik spojených s koncovými zařízeními v IT jako jsou servery, desktopy, mobilní zařízení a další. 76 procent účastníků si myslí, že v roce 2016 stoupla závažnost malwarových útoků. Zároveň 56 procent dotázaných si myslí, že útoky jsou lépe skryté, a tedy mnohem náročnější na detekci. I proto je čím dál těžší strážit firemní data.

1.5.1 Trendy v IT bezpečnosti

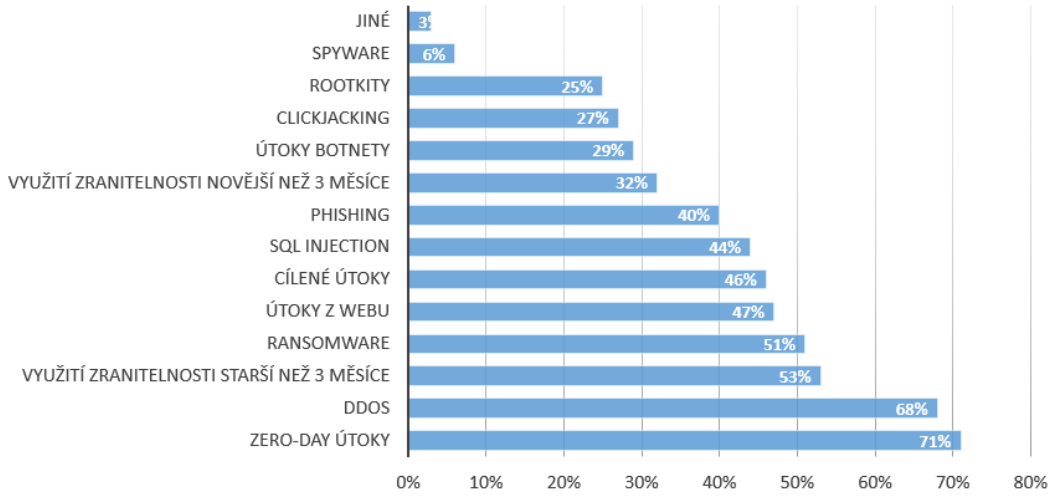
Studie [4] odhalila několik trendů v oblasti IT bezpečnosti. Kybernetické útoky využívají stále více destruktivního malware jako jsou Cryptolocker nebo Shamoon. Pouze 38 dotázaných odborníků má ve své firmě připravenou strategii pro boj proti destruktivnímu malware.

Největším rizikem v IT bezpečnosti dále zůstávají uživatelé a jejich zařízení ignorující bezpečnostní politiky firmy. Hrozba způsobená nezabezpečenými mobilními zařízeními stoupla podle 50 procent dotázaných. Nejvíce škody podle průzkumu momentálně způsobují útoky typu zero-day. Dále jsou to útoky typu denial of service.

Až 80 procent respondentů si myslí, že mobilní zařízení v jejich firmě byla během posledních dvanácti měsíců cílem útoku malware. Největší hrozbou jsou přenosné počítače a chytré telefony. Velkým rizikem je užívání komerčních cloudových aplikací uživateli a BYOD. Většina odborníků si myslí, že rozpočet pro zajištění IT bezpečnosti není dostatečný.

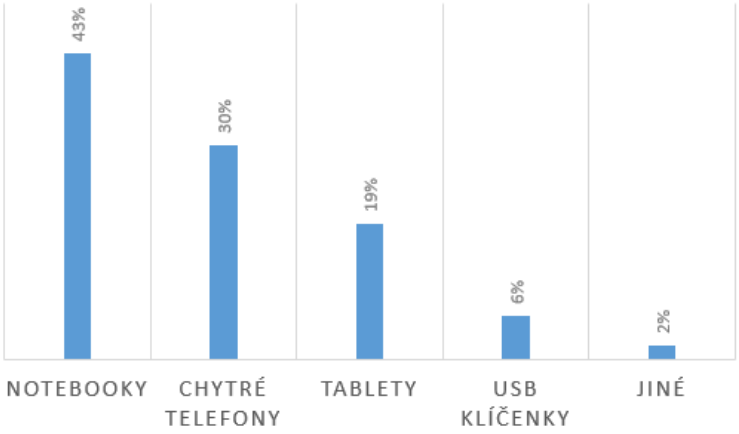


Obrázek 1.6: Jaké jsou největší hrozby pro bezpečnost koncových zařízení v organizacích účastníků průzkumu? Zdroj: [4].

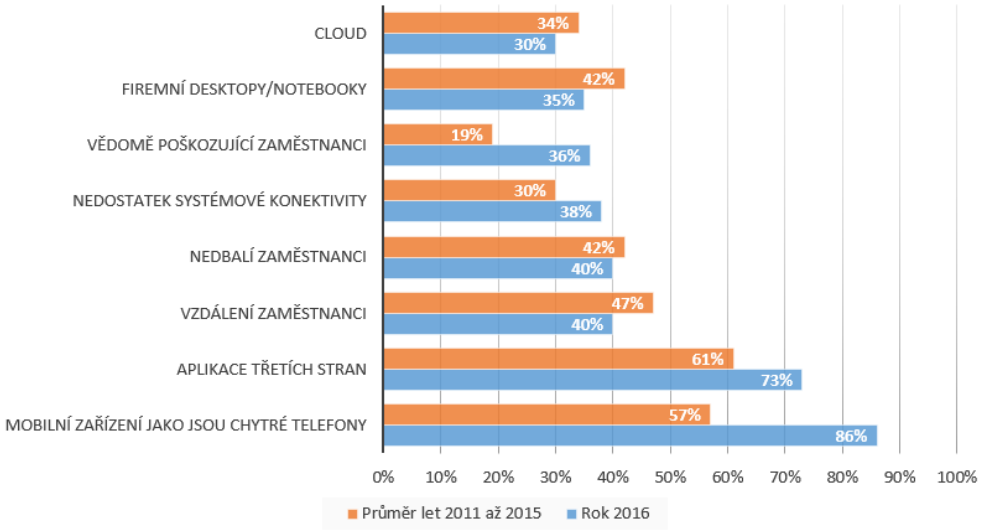


Obrázek 1.7: Jaká část účastníků průzkumu si myslí, že daný typ útoku způsobuje ty nejzávažnější incidenty? Zdroj: [4].

Zabezpečení koncových zařízení však hraje v bezpečnostní strategii IT čím dál větší roli. Oraganizace se plánují více soustředit na detekci a reakci, než na prevenci.



Obrázek 1.8: Jak velká část účastníků průzkumu si myslí, že největší hrozbou pro organizaci je právě daný typ zařízení? Zdroj: [4].



Obrázek 1.9: Jaká část účastníků průzkumu očekává nejvyšší nárůst potenciálního rizika pro bezpečnost IT v daných kategoriích? Zdroj: [4].

Kapitola 2

Analýza prostředí a požadavků

Tato kapitola seznamuje čtenáře s výsledky analýzy vybrané bankovní organizace. Nejdříve je organizace krátce představena a jsou vyjmenována některá specifika tohoto typu organizací. Dále je podrobně analyzován stávající proces připojování nefiremních zařízení do firemní sítě včetně použitých technických prostředků a tento proces je dále podroben analýze souvisejících hrozeb. V neposlední řadě jsou analyzovány známé požadavky na BYOD dané organizaci a typické skupiny uživatelů a jejich potřeb. Závěr kapitoly se zabývá projekty dotýkajícími se problematiky BYOD, které byly v organizaci uskutečněny již dříve.

2.1 Popis vybrané organizace

Zkoumaná organizace je zadavatelem této diplomové práce. Údaje pro tento popis jsou čerpány z výroční zprávy společnosti pro rok 2016. Jedná se o jednu z největších bank v České republice. Byla založena jako státní organizace, nyní se jedná o akciovou společnost. Majoritní podíl akcií drží mateřská společnost ze zahraničí. Typickým akcionářem je fyzická osoba z České republiky.

Čistý zisk v roce 2016 byl více než 13 miliard Kč, celkové provozní výnosy činily více než 31 miliard Kč, provozní náklady 14 miliard Kč.

Banka má více než 7,5 tisíce zaměstnanců, téměř 400 obchodních míst a více než 1,6 milionu klientů.

Mateřská společnost je jednou z největších evropských finančních skupin. Působí ve více než 70 zemích, má více než 150 tisíc zaměstnanců a obsluhuje více než 32 milionů klientů.

2.2 Vztah autora práce ke zkoumané organizaci

Autor této práce v době jejího vypracovávání nebyl zaměstnancem zkoumané organizace. Banka, jako zadavatel této práce, interně vedla autora této práce

jako externistu, studenta. Analýza probíhala ve spolupráci s oddělením IT Security. Schůzky a konzultace probíhaly napříč odděleními a byly zprostředkovány oddělením IT Security.

2.3 Specifika bankovního prostředí

Bankovnictví je specifický obor podnikání, a to především z důvodu vysoké státní regulace. Podle své výroční zprávy se Banka musí řídit mimo jiné následujícími právními předpisy:

- *zákon č. 21/1992 Sb., o bankách,*
- *zákon č. 256/2004 Sb., o podnikání na kapitálovém trhu,*
- *zákon č. 90/2012 Sb., o obchodních korporacích,*
- *zákon č. 257/2016 Sb., o spotřebitelském úvěru, (účinný od 1. 12. 2016)*
- *zákon č. 284/2009 Sb., o platebním styku,*
- *zákon č. 38/2004 Sb., o pojišťovacích zprostředkovatelích a samostatných likvidátorech pojistných událostí a o změně živnostenského zákona,*
- *zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu,*
- *zákon č. 69/2006 Sb., o provádění mezinárodních sankcí,*
- *zákon č. 563/1991 Sb., o účetnictví,*
- *zákon č. 101/2000 Sb., o ochraně osobních údajů,*
- *zákon č. 143/2001 Sb., o ochraně hospodářské soutěže,*
- *zákon č. 136/2011 Sb., o oběhu bankovek a mincí,*
- *zákon č. 190/2004 Sb., o dluhopisech,*
- *zákon č. 240/2013 Sb., o investičních společnostech a investičních fondech,*
- *zákon č. 89/2012 Sb., občanský zákoník,*
- *zákon č. 277/2013 Sb., o směnárenské činnosti,*
- *zákon č. 634/1992 Sb., o ochraně spotřebitele,*
- *nařízení EU č. 596/2014 o zneužívání trhu,*

- *nařízení EU č. 575/2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a navazující prováděcí nařízení Evropské komise,*

- *nařízení EU č. 648/2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů (EMIR).*

Banka, jako provozovatel kritické infrastruktury státu, též spadá pod **zákon č. 181/2014 Sb. o kybernetické bezpečnosti**, což s sebou mimo jiné nese nutnost reportovat kybernetické incidenty.

Vzhledem k vysoko kladeným nárokům na tento typ společností je nezbytně nutné mít jasně nastavené a kontrolované procesy. Podle výroční zprávy společnosti by z hlediska rizik spojených s nesouladem s regulatorními předpisy znamenalo *naplnění některých z rizik možné důsledky v podobě vedení sporů s regulatorními orgány, institucemi či klienty, riziko finančních pokut, náhrady škod či nákladů na nápravná opatření a dále riziko ztráty reputace a dobrého jména u klientů i široké veřejnosti, a tím další možné finanční ztráty.*

2.3.1 Řízení rizik

Problematika BYOD spadá pod operační rizika. Banka používá pro řízení operačních rizik přístup AMA – Advanced Measurement Approach. Při zajišťování informační bezpečnosti vychází z norem ISO/IRC 2700x. Pro řízení rizik se používá nástroj RSA GRC – Archer.

Hodnocení řízení rizik provádí interní audit

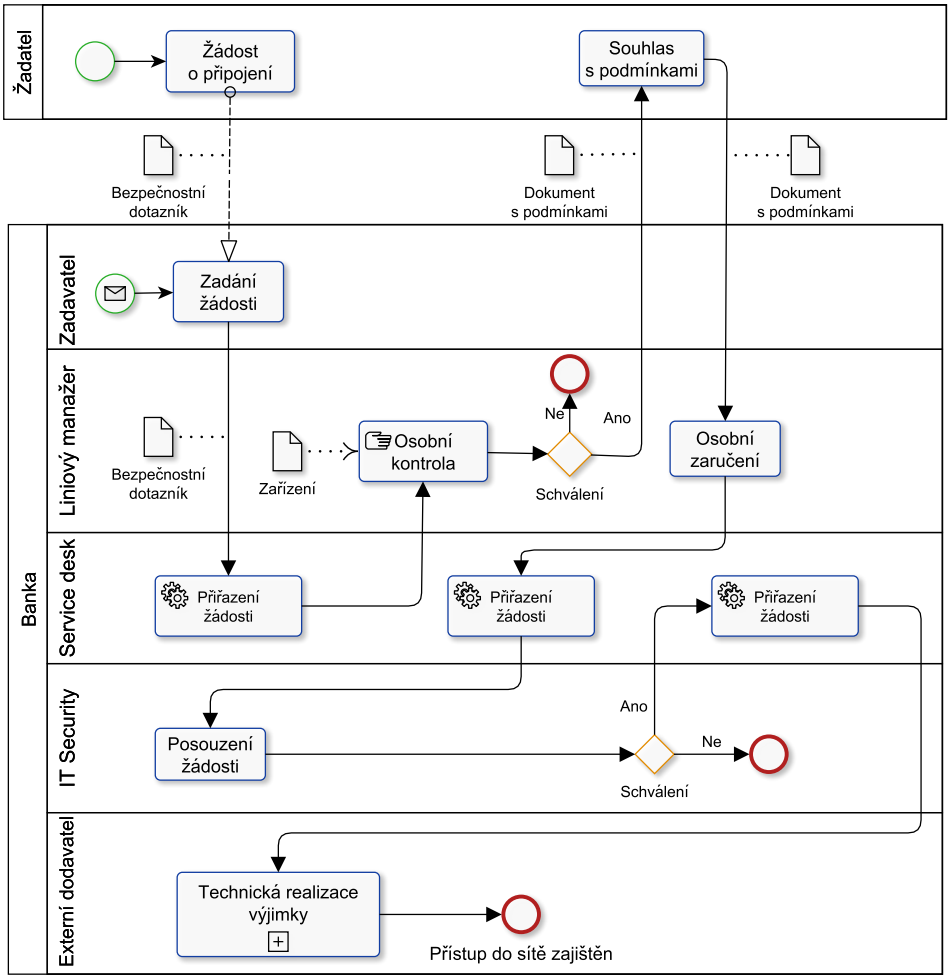
2.4 Aktuální stav připojování soukromých zařízení

Podle aktuální praxe ve zkoumané společnosti je připojení zařízení, které není ve vlastnictví společnosti, a to s ohledem na pracovní informační potřeby pracovníků, možné, ovšem toto je hodnoceno jako nesoulad s dobrou praxí a interními předpisy společnosti. Proto musí být pro každý takový případ udělena bezpečnostní výjimka.

2.4.1 Proces udělení bezpečnostní výjimky

Žádosti o připojování nefiremních zařízení se vyřizují pomocí aplikace Service desk. Jedná se o interní aplikaci vyvinutou a spravovanou uvnitř firmy za účelem řízení IT procesů. Proces pro udělení bezpečností výjimky za účelem připojení zařízení, které není ve vlastnictví společnosti, je ilustrován v diagramu 2.1.

Jelikož žadatel nemá se svým zařízením přístup do vnitřní sítě a tedy ani ke službám aplikace Service desk, je předpokládáno podání žádosti jinou osobou. Jelikož bezpečnostní standardy neumožňují, aby osoba schvalovala vlastní



Obrázek 2.1: Vizualizace procesu pro připojení nefiremního zařízení do vnitřní sítě.

žádost, předkladatelem žádosti nemůže být liniový manažer pod kterého organizačně spadá osoba žadatele. Součástí žádosti je vyplněný bezpečnostní dotazník.

Dotazník v obecné části obsahuje osobní údaje žadatele, odůvodnění žádosti, typy dat, se kterými bude pracovník nakládat či další informace o vlastnictví zařízení. Technická část dotazuje MAC adresu, použité operační systémy, přítomnost virtualizace, splnění licenčních podmínek software či přítomnost a aktuálnost bezpečnostního software (antivir, firewall, šifrování).

Vytvořený servisní případ žádosti je dále přidělen liniovému manažerovi pod kterého osoba žadatele organizačně spadá. Liniový manažer provede osobní kontrolu zařízení a podepíše se žadatelem dokument specifikující požadavky

na žadatele a zařízení. Mezi podmínky patří jednoznačná identifikovatelnost žadatele v rámci informačních systémů společnosti, správnost údajů uvedených v bezpečnostním dotazníku, splnění bezpečnostních politik či splnění licenčních podmínek. Schválením žádosti a jejím postuopením dále se liniový manažer zaručuje za svého podřízeného pracovníka.

Schválenou žádost dále přezkoumá pracovník oddělení IT security. Pokud žádost shledá oprávněnou, předá ji na externí firmu, která udělení bezpečnostní výjimky technicky realizuje. Realizace spočívá ve vytvoření přístupových účtů, přidělení přístupových oprávnění a zadání výjimky pro zařízení do systému spravujícímu přístup do sítě.

2.4.2 Další procesy související s BYOD

Další procesy jsou buďto triviální, nebo se vymykají rámci této práce a proto nebudou podrobněji analyzovány.

Ve zkoumané organizaci existuje WiFi síť pro hosty. Je určena především pro návštěvy za účelem obchodních jednání. Přístup k této síti jednoduše vytvoří zaměstnanec Banky ve speciální aplikaci. Pro dlouhodobější vytvoření přístupu zadá zaměstnanec požadavek do systému Service desk. Připojování nefiremních mobilních zařízení v době psaní této práce nebylo povoleno a tedy neexistoval související proces. Připojování firemních zařízení je mimo rámec této práce.

2.4.3 Připojení z technického hlediska

Pro správu nefiremních zařízení ve své síti používá zkoumaná společnost nástroj MAB Keeper od společnosti AleFIT. Ta jej v [29] definuje následovně: *Aplikace slouží ke správě MAC adres zařízení, která jsou v autentizačním systému použita pro autentizaci, ale nejsou kompatibilní se standardem 802.1x, nebo správě zařízení, u nichž se MAC adresa využívá jako náhradní způsob autentizace. AleFIT MAB Keeper také umožňuje díky několika modulům kontrolovat a časově omezit přístup kontraktorů, konzultantů i BYOD zařízení do firemní sítě, stejně jako využít workflow pro realizaci re-image stanic.* Jedná se o nadstavbu používaného systému Cisco Identity Service Engine (ISE).

Systém ISE řídí nasměrování zařízení do patřičné VLAN na základě adresy MAC. podle příslušnosti k patřičné VLAN má připojené zařízení zajištěna přístupová práva. Ta se řídí pomocí seznamů pro řízení přístupu neboli anglicky Access controll list (ACL). Jedná se tedy o správu připojených zařízení na úrovni topologie sítě.

Výjimky je možné najít v aplikaci MAB keeper v záložce Approved devices. MAB Keeper tak slouží pro distribuci správy. Mezi používané techniky se řadí MAC address bypass, což znamená obejití standardní autentifikace pomocí protokolu 802.1.X. Jelikož nefiremní zařízení nemají autorizační certifikát, používá se autorizační funkce. Ta zohledňuje MAC adresu a přihlašovací

údaje. Uživatelé s vlastními zařízeními a uznanou výjimkou se mohou být přiřazeni do stejné VLAN jako firemní zařízení.

Z hlediska použití bezdrátových sítí WiFi existuje datová síť a síť pro hosty. Pro přístup k datové síti je nutný certifikát, a to především z důvodu fyzické dostupnosti signálu sítě i mimo objekty firemní objekty. Není v plánu další rozšiřování datových WiFi sítí.

WiFi síť pro hosty je určena pro krátkodobé návštěvníky a umožňuje pouze přístup k síti internet. Důvodem pro její existenci jsou především prezentace obchodních partnerů a další datově méně náročné činnosti. Probíhá na ní URL filtrace.

Jednodenní přístup mohou vytvořit zaměstnanci banky pomocí speciální aplikace. Vytvoření dlouhodobějšího přístupu je možné a vytváří se pomocí žádosti v aplikaci Service desk.

2.5 Cisco ISE

Společnost Gartner v [30] popisuje Cisco ISE jako jako technologii založenou na protokolu RADIUS. Pokročilé funkce NAC potřebují užitích dalších komponent jako třeba TrustSec Security Group Tag. S použitím device profiling and feed service umožňuje analyzovat provoz a vytvářet reporty o připojených zařízeních.

Balík Cisco AnyConnect sjednocuje další funkce jako jsou VPN, NetFlow nebo ochrana proti škodlivému software. V ISE verze 2.0 je zabudována podpora pro certifikáty, Active Directory či TACACS+.

2.6 Analýza aktuálních bezpečnostních rizik spojených s BYOD

Jelikož metodika analýzy rizik je pro firemního partnera citlivou informací, není pro potřeby této práce možné pracovat s interními metrikami. Vhodné metriky pro hodnocení rizik spojených s kybernetickou bezpečností uvádí zákon o kybernetické bezpečnosti, vyhláška č. 316/2014 Sb., viz [31].

Hodnocení rizik používá následující funkci:

$$riziko = dopad * hrozba * zranitelnost$$

Zákon o kybernetické bezpečnosti udává v § 4, bod (4) vzhledem k bezpečnosti informačních systémů ke zvážení následující hrozby:

(a) porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,

(b) poškození nebo selhání technického anebo programového vybavení,

(c) zneužití identity fyzické osoby,

(d) užívání programového vybavení v rozporu s licenčními podmínkami,

(e) kybernetický útok z komunikační sítě,

(f) škodlivý kód (například viry, spyware, trojské koně),

(g) nedostatky při poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,

(h) narušení fyzické bezpečnosti,

(i) přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,

(j) zneužití nebo neoprávněná modifikace údajů,

(k) trvale působící hrozby a

(l) odcizení nebo poškození aktiva.

a dále pak v bodu 6:

(a) porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů kritické informační infrastruktury,

(b) pochybení ze strany zaměstnanců,

(c) zneužití vnitřních prostředků, sabotáž,

(d) dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,

(e) nedostatek zaměstnanců s potřebnou odbornou úrovní,

(f) cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik a

(g) zneužití vyměnitelných technických nosičů dat.

Zranitelnosti jsou vzhledem k zákonem udávaným typům pro tuto analýzu vzhledem k nastaveným bezpečnostním opatřením pro ochranu informačních systému uvnitř zkoumané společnosti konstantní.

Dále je provedeno hodnocení rizik spojených s připojováním nefiremních zařízení aktuálním postupem pomocí metrik zákona o kybernetické bezpečnosti.

Hrozby e), h), i), j), k) ve vztahu k aktuálně praktikovanému připojování uživatelů s nefiremními zařízeními neexistují, a proto jsou podle stupnice ze [31] nízké.

Hrozba a) je pravděpodobná, jelikož bezpečnostní politiky není možné vynutit. Hrozbu je tedy nutné hodnotit jako **střední až vysokou**. Jelikož porušení bezpečnostních politik může mít vliv na chod systémů avšak v omezeném rozsahu a časovém období, lze jej hodnotit jako **střední**. Výsledné riziko je tedy **střední až vysoké** a podle použité metodiky by měly být v případě nižší náročnosti zahájeny systematické kroky k jeho odstranění.

Hrozba b) je málo pravděpodobná a její dopad by byl v omezeném období a malého rozsahu. Výsledné riziko je tedy **nízké**.

Hrozba c) je reálná v případě odcizení zařízení a jeho následném použití pro připojení k firemní síti. Je málo pravděpodobná a nejsou známy žádné případy. Stupeň hrozby je tedy **střední**. Dopad je v omezeném rozsahu a časovém období, je tedy **střední**. Riziko je tedy **střední** a je tolerovatelné pouze pokud by protiopatření byla vyšší náročnosti.

Hrozba d) je pravděpodobná jelikož není možné kontrolovat veškerý nainstalovaný software na zařízení a shodu licenčního ujednání s firemními podmínkami. Stupeň hrozby je tedy **střední až vysoký**. Jelikož pracovník se smluvně zavázal, že nelicencovaný software používat nebude, břímě odpovědnosti leží na jeho osobě. Případné dopady tedy mohou být přeneseny na něj a hodnocení dopadů je tak **nízké**. Výsledné riziko je tedy **nízké až střední**.

Hrozba f) je spíše pravděpodobná. Přestože se uživatel zavázal k používání zazáplatovaného systému a aktuální antivirové ochrany, není možné toto vynutit a monitorovat bezpečné chování uživatele. Tuto hrozbu je možné hodnotit jako **střední až vysokou**. Teoretický dopad může být nezanedbatelného rozsahu a způsobit škodu. Riziko je tedy **střední až vysoké** a měly by být zahájeny kroky k jeho odstranění.

Hrozba l) je reálná, stávající opatření nijak neznesnadňují případnému pachateli odcizení aktiv, předpokládaná realizace hrozby však není častá a lze ji proto hodnotit jako **nízkou až střední**. Finanční ztráty by mohly být znatelné, avšak rozsah dopadu se zdá být omezený, dopad tak lze hodnotit jako **nízký** a celkové riziko jako **nízké až střední**.

Vzhledem k dalším uvedeným hrozbám lze konstatovat, že připojování nefiremních zařízení na základě výjimek oproti firemním zařízením znamená zvýšení pravděpodobnosti hrozby c), f) a g), a proto je třeba jim věnovat pozornost.

2.6.1 Zhodnocení analýzy rizik

Při porovnání s užitím firemního zařízení byla při stávajícím způsobu připojování nefiremního zařízení identifikována zvýšená pravděpodobnost realizace některých hrozeb potažmo rizik. Tato práce si klade za cíl hodnotit možná

řešení především z hlediska bezpečnosti a navrhnout tak řešení, která identifikovaná rizika zásadním způsobem sníží.

2.6.2 Analýza hrozeb souvisejících s nasazením BYOD

Jelikož BYOD zařízení již nyní ve firemní síti existují, nasazení navrhovaného BYOD programu nijak nezvyšuje pravděpodobnost žádné ze známých hrozeb. V této práci navrhované řešení se soustředí na bezpečnost a tedy nejenom že nezvyšuje pravděpodobnost realizace známých bezpečnostních hrozeb oproti stávajícím firemním zařízením, ale naopak zvyšuje bezpečnost oproti aktuálnímu způsobu připojování nefiremních zařízení.

2.7 Analýza požadavků na připojení vlastních zařízení

Formou konzultací se zaměstnanci zkoumané společnosti napříč různými odděleními bylo identifikováno několik požadavků a potřeb.

2.7.1 Obecné požadavky

Jedním z hlavních požadavků je přiměřenost z hlediska nákladů. Návrh řešení je třeba obhájit před vedením společnosti, které schvaluje rozpočty projektů. Zároveň je žádoucí, aby řešení mělo kladné přijetí od potencionálních uživatelů, tak aby byli ochotni jej využívat a náklady na zavedení nebyly vynaloženy zbytečně.

Smyslem vytvoření BYOD programu je vytvoření uceleného návrhu, který umožní zaměstnancům v odůvodněných případech využívat vlastní zařízení a především zvýší bezpečnost existujících BYOD, které se nyní objevují převážně u kontraktorů. Existující riziko, plynoucí z nespravovaných nefiremních zařízení v síti, je třeba potlačit, což je nejsilnějším argumentem pro prosazení projektu.

Důvody k zavedenní řešení BYOD lze tedy rozdělit na technologicko-sociální a obchodní. Je zřejmé, že vzhledem k nastoleným trendům je nutné nastolit firemní strategii pro BYOD. Pokud by se řešení nenašlo, nefiremní zařízení se přesto budou rozšiřovat, ovšem nebudou pod kontrolou firemního IT oddělení. To v důsledku znamená, že nebude možné kontrolovat rizika ani náklady s tímto spojené.

Z pohledu oddělení IT Security je majoritním důvodem pro řešení otázky BYOD aktuální stav, kdy jsou nefiremní zařízení připojována na základě bezpečnostních výjimek. Tento stav je nežádoucí a je identifikován jasný požadavek pro nastolení rámce, který eliminuje hrozby z toho plynoucí.

2.7.2 Identifikované potřeby

- Tablety pro vrcholový management
- Vlastní notebooky
- Vlastní počítače Apple
- Firemní notebooky externích konzultantů
- Přístup k dokumentům ze soukromých tabletů
- Přístup k emailu či kalendáři z osobního chytrého telefonu

2.7.3 Identifikované služby

Z hlediska souvisejících služeb poskytovaných IT byly identifikovány služby typu **PIM**[1] neboli služby pro správu osobních informací, typicky se jedná o kalendář, email a další komunikační a organizační systémy, jimiž jsou například Oultook a Skype for Bussiness. Dále je třeba zprostředkovat služby pro **tvorbu a sdílení dokumentů**. Typicky se jedná o Microsoft Office či Atlassian Confluence. V neposlední řadě je nutný přístup k **business aplikacím**.

2.7.4 Identifikované typy zařízení

Co se týče různých typů zařízení, je třeba do BYOD programu zařadit firemní chytré telefony včetně zařízení BlackBerry a tablety. Co se týče nefiremních či osobních zařízení je třeba zohlednit chytré telefony, tablety, notebooky či notebooky od firmy Apple.

2.7.5 Identifikovaní uživatelé

Jako uživatelé byli identifikováni zaměstnanci Banky, externí dodavatelé, kontraktoři a klienti.

Skupinou uživatelů, která z principu přichází s vlastními zařízeními jsou externisté, jež Banka z pravidla najímá pro účely projektů. Tito uživatelé můžou pracovat na živnostenský list, nebo mohou být zaměstnanci externího dodavatele. Uživatelé pracující na živnostenský list používají zpravidla soukromá zařízení, zaměstnanci externích dodavatelů používají zpravidla zařízení ve vlastnictví a správě svého zaměstnavatele.

Jako nejčastější typy pracovníků z externích zdrojů byli identifikováni:

- Projektoví manažeři
- Vývojáři

[1] Personal Information Management

- IT konzultanti

Projektoví manažeři jsou zpravidla najímáni pro své know-how z jiných projektů. Mezi priority v jejich potřebách patří firemní služby typu PIM (kalendář, email,...) nástroje pro vytváření dokumentů a kolaboraci, přístup k dokumentům a datům či další nástroje potřebné k řízení projektů.

IT konzultanti potřebují používat nástroje, dokumenty a služby spojené s danou konzultační činností, kterou Bance poskytují. Problematika vývojářů je popsána v odstavci 2.7.8.

V případě externích pracovníků je obzvláště nutné dbát na ochranu firemních dat. Je užitečné mít možnost zajistit, že po ukončení své činnosti tito pracovníci dále nebudou moci nakládat s firemními aktivy. Tito pracovníci se musí řídit vnitřními směrnicemi banky. V případě bezpečnostního incidentu je možné tyto pracovníky nebo jejich zaměstnavatele právně postihovat, typicky pokutou, a to na základě standardně uzavíraného právního vztahu.

Zájem o používání vlastních zařízení však mají i zaměstnanci Banky. Identifikováni byli především uživatelé z vedení společnosti (počítače Mac, tablety iPad) a vývojáři. Pokud se vinou svého vlastního zařízení dopustí bezpečnostního incidentu zaměstnanec banky, je jeho zodpovědnost obtížněji vymahatelná.

2.7.6 Způsoby připojení k síti

Z hlediska připojení k síti byly identifikovány následující možnosti: připojení do sítě LAN, připojení do lokální WiFi a připojení skrze síť internet a mobilní připojení.

2.7.7 Způsob podpory od IT oddělení

Momentálně IT oddělení poskytuje end-to-end podporu. To znamená, že dodaní služeb je podporováno kompletně od zdroje, přes dodání po podporu koncových zařízení. Tento model není trvale udržitelný pro BYOD, kdy není možné podporovat všechna koncová zařízení a je tedy třeba zavést i model, kde je podporována pouze samotná služba. Návrh způsobu podpory pro BYOD je rozveden v kapitole 4.9.

2.7.8 Identifikace potřeb specifického uživatele – vývojáře

Vývojáři patří mezi prioritní skupinu uživatelů, pro které je třeba připravit projekt BYOD. Právě mezi vývojáři je velké množství kontraktorů, kteří si přinášejí své vlastní nefiremní zařízení. Vývojáři však mají vyšší požadavky než běžní uživatelé. Konzultací se zástupci vývojářů byly identifikovány následující potřeby.

Vývojář potřebuje mít na zařízení, na kterém vyvíjí, administrátorská oprávnění. Je to především z důvodu instalace pomocných nástrojů, tak z

důvodu přístupu k některým systémovým funkcím operačního systému, například pro potřeby testování. Dále má vývojář zvýšené nároky na výpočetní výkon stroje, na kterém němž pracuje, především z důvodu potřeby lokální kompilace zdrojových kódů.

Vývojáři mají specifické požadavky na nainstalované aplikace. Každý potřebuje vývojové prostředí (Banka nemá sjednoceno, a tedy vývojáři mohou volit nástroj dle svého uvážení, například IntelliJ Idea). Poté jsou to nástroje pro vývoj databází, například Oracle SQL Developer. Dále je nutné přistupovat k dalším databázím. V prostředí zkoumané organizace se používají různé databáze (Oracle, MySQL, MS SQL). Mezi dalšími nezbytnými nástroji byl uveden SSH klient Putty.

Byla zmíněna potřeba přístupu k následujícím službám:

- Přihlašování do domény
- Přístup k logům – k centrálnímu systému logů na systému Logman
- Přístup k nástroji pro zpracování výstupních streamů Apache Kafka
- Přístup k verzovacímu systém GIT na platformě BitBucket
- Přístup k systému pro evidenci chyb Atlassian JIRA
- Přístup k nástroji pro dokumentaci Atlassian Confluence
- Přístup k nástroji pro automatizaci správy software Jenkins
- Přístup k testovacím prostředím
- Přístup k emailům
- Přístup ke službě Skype for business
- Přístup k adresářové službě LDAP
- Přístup ke správě identit ITIM

Pokud se vývojář připojuje vzdáleně, klade důraz na přístup k verzovacíu systému GIT, přístup k testovacímu prostředí a přístup k logům.

2.8 Aktuální stav podpory různých typů zařízení dle typu vlastnictví

Nejvyšší prioritou je umožnit uživatelům se soukromými zařízeními plný a kontrolovaný přístup ke službám lokální sítě. Není nutné zajišťovat vzdálený přístup pro nefiremní zařízení, je však třeba podporovat vzdálený přístup k emailu. Pro mobilní telefony je třeba zajistit přístup k emailu. Přístup k dokumentům a aplikacím zatím není vyžadován. Byl identifikován požadavek

		firemní zařízení	Soukromé zařízení	Zařízení kontraktora
Notebook	Lokálně	Dostupné	Nepodporované ale používané	Nepodporované ale používané
	Vzdáleně	Dostupné přes VPN	Nepodporované	Nepodporované
Tablet	Lokálně	Nedostupné	Nedostupné	Nedostupné
	Vzdáleně	Nedostupné	Nedostupné	Nedostupné
Chytrý telefon	Vzdáleně	Dostupné pro BlackBerry	Nedostupné	Nedostupné

Tabulka 2.1: Tabulka aktuálního stavu podpory pro jednotlivé typy zařízení podle typu vlastnictví

na firemní tablety od vrcholového managementu. Pro ty je třeba zajistit maximální přístup. Uživatelé soukromých tabletů požadují přístup k emailu a dokumentům.

2.9 Předešlé projekty

Projekt na vyhodnocení konceptu BYOD byl v bance započat již v roce 2013. Měl za cíl vyhodnotit rámec pro konkrétní potřeby, scénáře a služby, dále měly být nastaveny předpokládané výstupy a definováno možné řešení. Již v roce 2013 byl citelný příklon uživatelů ke konzumerizaci informačních technologií a prorůstání jiných než-li PC zařízení do firemního prostředí.

V té době se mobilní připojení stalo standardem i pro běžné uživatele a ti tak byli neustále připojeni se svými osobními zařízeními k internetu. Dále byla citelná osobní potřeba zaměstnanců používat svá osobní zařízení i během pracovní doby.

Projekt nastolil možnost zpřístupnění přístupu k emailu i z nefiremních zařízení. Důvodem je zvýšení pracovní efektivity při minimálních dodatečných výdajích. Na mnohých pracovních pozicích by též zavedení BYOD programu umožňovalo flexibilnější pracovní styl. S tím souvisí i snadnější přístup ke klientům. Flexibilnější přístup umožňuje lépe uplatňovat techniky křížného prodeje[2]. Bezprostřední přístup k informacím by znamenal rychlejší reakci obchodníků a konkurenční výhodu.

2.9.1 Dříve zvažované možnosti pro email

V minulosti bylo zvažováno několik možností, jak zpřístupnit email a dokumenty na soukromých chytrých telefonech a tabletech.

Exchange ActiveSync snižuje riziko krádeže díky vynucení zadání PIN kódu a možnosti vzdáleného smazání. V jeho prospěch hrála relativně snadná a rychlá implementace. Řešení bylo zamítnuto, protože nenabízelo zašifrování dat. To může znamenat ohrožení dat například při jail-breaku u zařízení iPhone.

[2]Křížný prodej, někdy též křížový prodej (anglicky cross-selling), je obchodní taktika navyšování prodeje, jejímž cílem je prodat více, doporučením souvisejícího zboží nebo služeb, viz [32]

V rámci mateřské skupiny se používá řešení Good mail (nyní BlackBerry Work). Toto řešení nevyhovovalo požadavkům vzhledem k vysokým nákladům na implementaci a provoz. Nicméně projekt pro toto řešení stále existuje.

Microsoft Outlook Web App umožňuje prohlížení příloh přímo na serveru a není tedy nutné lokální šifrování dat. Řešení je vhodné jak pro mobilní zařízení, tak tablety a nepřináší žádné dodatečné náklady, jelikož je již implementováno. Uživatelé však nehodnotí uživatelskou přívětivost tohoto řešení příliš kladně.

2.9.2 Projekt VDI pro vývojáře a testery

V Bance též existoval projekt, který se snažil ověřit možnost využití virtuálních strojů pro vývojáře a testery. Důvodem byla snaha získat řešení pro vlastní zařízení kontraktorů, která znamenají bezpečnostní riziko. Dále si Banka od projektu slibovala nalezení řešení problému s využíváním několika zařízení vývojáři, ať už z důvodu vzdálené podpory nebo zvláštních požadavků na výkon.

Test VDI se odehrál v roce 2011, probíhal tři týdny a zúčastnilo se ho 5 vývojářů. Uživatelé po dobu testu prováděli veškeré své pracovní úkony ve virtuálním prostředí. Virtuální stroje běžely na serveru Proliant DL380 G5 s parametry: 4x (2CPUx2jádra) CPU 3000MHz, 24GB RAM a 1,3TB místa na disku. Parametry pro jednotlivé virtuální stroje byly ekvivalentí k PC dvoujádrovým procesorem a 2-4 GB RAM.

Účastníci testu ohodnotili uživatelský zážitek jako dostatečný pro běžné použití. Zaznamenali však nižší odezvu a občasné záseky. Byly identifikovány problémy s periferními zařízeními, například nefungovala čtečka na čipové karty. Odezva vývojářských nástrojů byla odhadem dvakrát pomalejší. Uživatelé hodnotili přechod k virtuálním strojům jako zhoršení uživatelského komfortu oproti fyzickým firemním PC.

Test prokázal vysoké nároky na diskové úložiště především co se týče počtu požadavků na vstupně/výstupní operace. To znamená nutnost vysoké investice do kvalitního diskového úložiště. Zároveň je nutné zajistit kvalitní konektivitu. Proto bylo rozhodnuto, že VDI není vhodné pro interní vývojáře, protože zvyšuje náklady a nepřináší benefity.

Zároveň test doporučil ke zvážení zkoušený model VDI pro kontraktory, a to pod podmínkou užití vlastního zařízení bez dalších nákladů pro Banku, bez zajištění vysoké dostupnosti a omezení velikosti diskové kapacity pro virtuální stroje na odhadovaných 70-80GB.

Kapitola 3

Možné varianty řešení

Tato kapitola se zaměřuje na analýzu existujících řešení na trhu. V první části jsou definovány různé pohledy na BYOD na základě vlastnictví zařízení, typů zařízení a způsobu přístupu do datové sítě. Dále jsou definovány známá technická řešení pro BYOD. Na základě vlastností známých řešení je odděleně zvolen vhodný přístup řešení pro notebooky a mobilní zařízení. Pro tyto přístupy jsou vyhodnoceni nejvýznamnější poskytovatelé.

3.1 Různé pohledy na BYOD

Na problematiku nefiremních zařízení je možné nahlížet z různých úhlů pohledu. V této sekci budou představeny různé možnosti dělení zařízení dle různých kategorií a taktéž budou představeny odpovídající řešení.

3.1.1 Rozdělení zařízení podle vlastnictví

Na základě toho, kdo je vlastníkem zařízení připojovaného k firemní síti, je určena míra kontroly zařízení firmou.

3.1.1.1 Firemní zařízení

Jedná se o zařízení, které nakupuje a zároveň spravuje firma. Je ve vlastnictví firmy a pod dohledem IT oddělení. Zařízení plně splňuje politiky firmy a je plně kontrolované.

3.1.1.2 Externí firemní

Jedná se o firemní zařízení pracovníka externí firmy, jedná se tedy o firemní zařízení, ale jiné firmy. Je tedy pod správou IT oddělení externí firmy.

Zařízení splňuje bezpečnostní politiky externí firmy a je kontrolované externí firmou. Není možné zařízení kontrolovat, je však možné vynutit potřebné bezpečnostní politiky smluvním vztahem s externí firmou.

3.1.1.3 Externí soukromé

Zařízení externího pracovníka, které není kontrolované firemní politikou externí firmy. Není možné jej kontrolovat a je obtížné vynucovat bezpečnostní politiky.

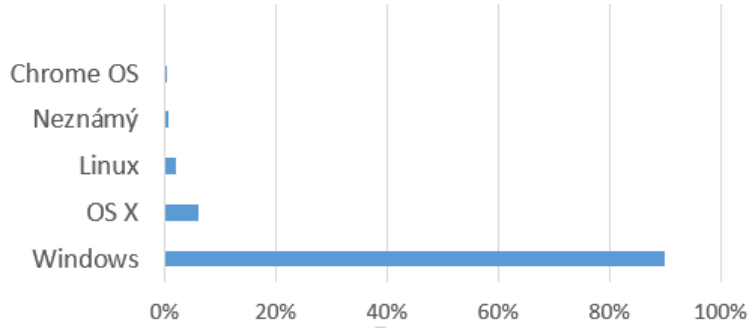
3.1.1.4 Zaměstnanec se soukromým zařízením

Vlastní zařízení zaměstnanců. Není kontrolované a může představovat bezpečnostní hrozbu.

3.1.2 Rozdělení podle typu zařízení

3.1.2.1 PC

V užším slova smyslu se jedná o osobní počítače s operačním systémem Windows od firmy Microsoft, viz [33]. Windows je aktuálně nejrozšířenější operační systém pro korporátní zařízení. Systém je určený pro zařízení postavená na architektuře x86. Typicky se jedná o stolní počítače a notebooky. Podle statistiky StatCounter [5] měl operační systém Windows v únoru 2017 90 procentní podíl na trhu operačních systémů pro desktopy podle počtu přístupů na web. Podle celosvětových statistik přístupů na web v souhrnu všech typů zařízení podle StatCounter má však Windows pouze 38,6 procenta přístupů a mezi běžnými uživateli je zřejmá tendence v upřednostňování jiných zařízení na úkor PC [34].

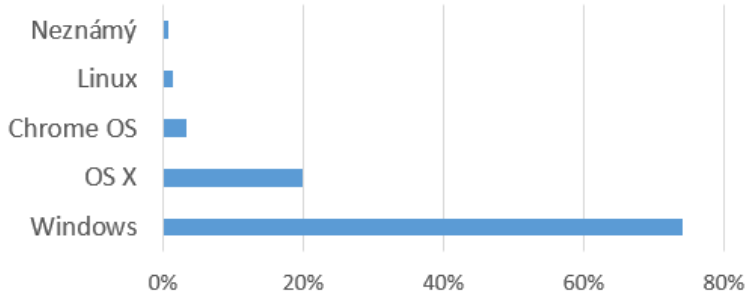


Obrázek 3.1: Statistika podílu operačních systémů pro desktopy v České republice podle přístupů na web. Převzato z [5].

3.1.2.2 Mac

Počítač s operačním systémem MAC OS [35]. Jedná se o proprietární operační systém pro počítače firmy Apple. Podle StatCounter je jeho podíl na trhu mezi desktopovými operačními systémy podle počtu přístupů na web v

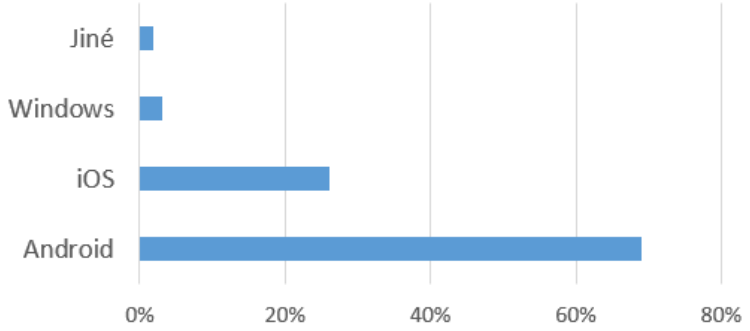
České republice necelých šest procent. Populární je zejména ve Spojených státech, kde se jeho podíl mezi desktopovými operačními systémy podle metodiky StatCounteru pohybuje okolo dvaceti procent.



Obrázek 3.2: Statistika podílu operačních systémů pro desktopy v USA podle přístupů na web. Převzato z [5]

3.1.2.3 Chytrý telefon či tablet

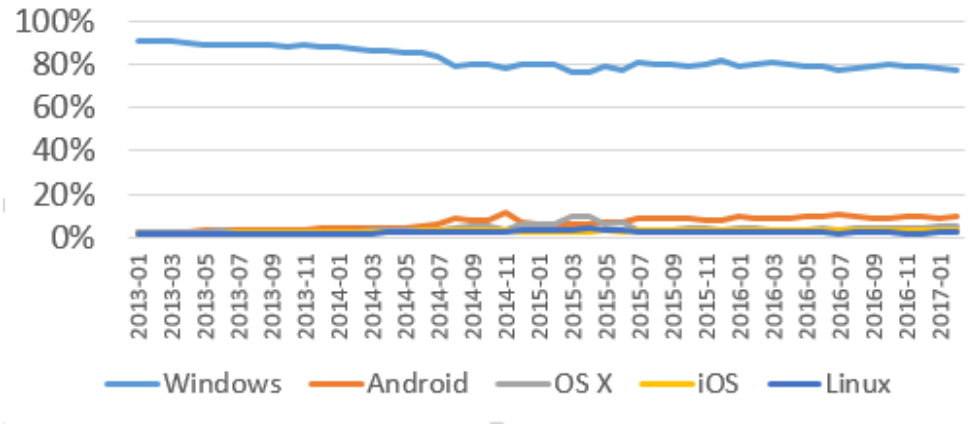
Podle společnosti Gartner [36] je chytrý telefon definován jako mobilní komunikační zařízení používající identifikovatelný otevřený operační systém. Tento systém je podporován aplikacemi třetích stran od komunity vývojářů. Aplikace třetích stran mohou být instalovány nebo odstraněny a mohou být vytvořeny přímo pro operační systém zařízení a aplikační programové rozhraní, případně pro oddělenou vrstvu jakou může být například Java. Operační systém musí podporovat multitaskingové prostředí a uživatelské rozhraní, které dokáže obsloužit více aplikací najednou. Například zobrazení emailu během přehrávání hudby.



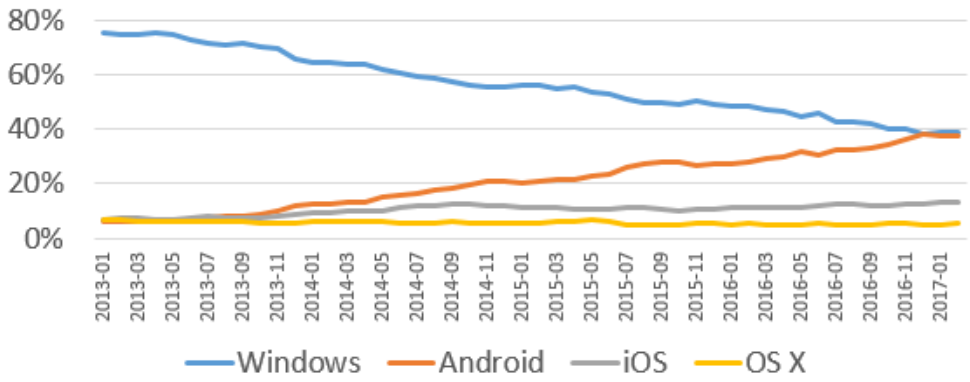
Obrázek 3.3: Statistika podílu operačních systémů pro mobilní zařízení v České republice podle přístupů na web. Převzato z [5].

Obecněji se jedná o mobilní zařízení s možností instalace aplikací. V současné době jsou nejpopulárnější zařízení s operačním systémem Android od firmy Google a iOS od firmy Apple. V České republice je podle metodiky měření společnosti StatCounter pro únor 2017 nejpopulárnější operační systém Android s podílem 68 procent. Operační systém iOS je na drůhém místě s podílem 26 procent. Více než jednoprocentní podíl má již pouze Windows s necelými čtyřmi procenty [34].

Celosvětově je zřejmá rostoucí obliba mobilních zařízení mezi uživateli, a to především na úkor klasických PC s operačním systémem Windows. Vzhledem k postupné změně návyků uživatelů je vyžadováno, aby firemní prostředí na tento trend vhodně reagovalo.



Obrázek 3.4: Statistika vývoje podílů všech operačních systémů v České republice podle přístupů na web. Převzato z [5].



Obrázek 3.5: Statistika vývoje podílů všech operačních systémů celosvětově podle přístupů na web. Převzato z [6].

U těchto zařízení se nepředpokládá nutnost přístupu k podnikovým aplikacím, ale je vyžadován okamžitý přístup k emailům, kontaktům či dokumentům, a to nezávisle na místě použití.

Dle reportu od společnosti Nokia Thread Intelligence Lab [37, 38], který monitoroval aktivitu malwaru v sítích mobilních operátorů mezi lety 2012 a 2015 měly 60 % veškeré aktivity malwaru v mobilních sítích na svědomí chytré telefony, zbytek šel na vrub Windows PC.

V prosinci 2015 vykazovalo známky napadení škodlivým softwarem 0,3 % všech chytrých telefonů. Nejvíce napadení zaznamenala zařízení s operačním systémem Android, ovšem na seznam s dvaceti nejčastěji se vyskytujícími druhy škodlivého software se dostali i dva zástupci pro operační systém iOS (XcodeGhost a Flexispy). V říjnu 2015 bylo 6 % všech napadených zařízení značky iPhone.

3.1.3 Rozdělení podle typu přístupu do datové sítě

3.1.3.1 Ethernet

Jedná se o pevné připojení do sítě pomocí kabelu [39]. Je vhodné pro firemní počítače, není vhodné pro zařízení typu mobilní telefon či tablet.

Je definované ve standardu IEEE 802.3.

3.1.3.2 WiFi

Bezdrátové připojení pomocí WiFi sítí. Jedná se o standardní technologii pro bezdrátové sítě WLAN [40]. Tento typ připojení je vhodný pro přenosné počítače, mobilní telefony i tablety. WiFi je definováno standardem IEEE 802.11.

3.1.3.3 VPN

Virtual private network čili vzdálené připojení do firemní sítě. Hlavním smyslem VPN je vytvořit soukromou síť pomocí tunelování a nebo šifrování skrze veřejný internet tak, aby uživatelé mohli vzdáleně přistupovat ke službám dostupným pouze zevnitř sítě [41].

3.2 Známé způsoby řešení BYOD

3.2.1 Virtualizace

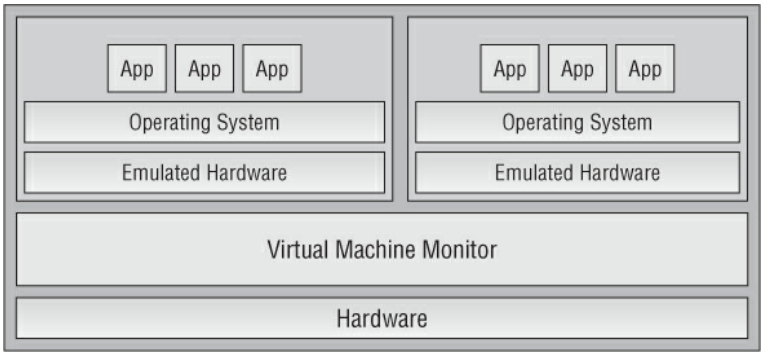
Podle [7] je virtualizace abstrakcí výpočetních zdrojů od fyzické hardwarové vrstvy. Virtuální stroj vystupuje jako samostatný výpočetní systém dostupný z jiného stroje. Díky virtualizaci je možné oddělit data a prostředí fyzického a virtuálních strojů. Jako hostitel je nazývána platforma na které běží hypervizor. Virtuální stroj je pak systém na kterém běží virtuální prostředí. Re-

prezentuje kompletní hardwarovou platformu. Virtuální stroje pak běží nad hypervizorem.

Hypervizor je hlavní komponenta virtualizece. Rozeznáváme 2 druhy:

3.2.1.1 Hypervizor typu 1

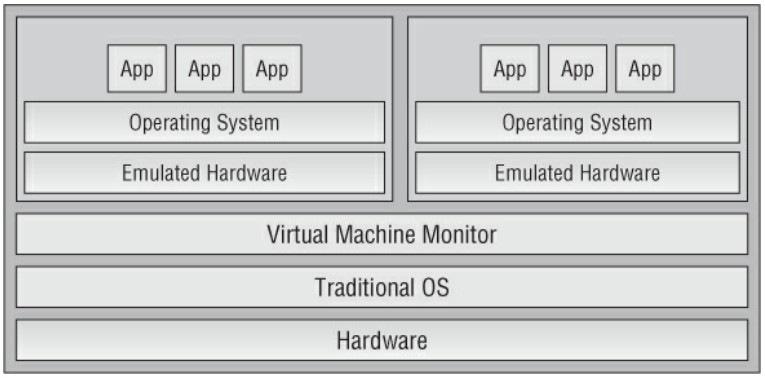
Hypervizory prvního typu jsou nainstalovány přímo nad hardware. Mezi hardware a virtuálními stroji s operačními systémy tak není žádná další vrstva. Hypervizory typu 1 jsou zpravidla instalovány na servery ve výpočetních střediscích.



Obrázek 3.6: Schéma virtualizace s hypervizorem typu 1. Převzato z [7].

3.2.1.2 Hypervizor typu 2

Hypervizory druhého typu jsou aplikace instalované v rámci existujícího operačního systému. Mezi hardware a operačními systémy virtuálních strojů je tak navíc vrstva operačního systému hostitelského stroje. Hypervizory typu 2 jsou zpravidla instalovány na pracovní stanice.



Obrázek 3.7: Schéma virtualizace s hypervizorem typu 2. Převzato z [7].

3.2.2 Hrozby spojené s virtualizací

Hlavní výhodou virtualizace je oddělení jednotlivých prostředí. Samotnou virtualizací se však bezpečnost nezvyšuje a ve virtualizovaném prostředí existují stejné hrozby jako v prostředím fyzickém. Z hlediska BYOD je však právě oddělení prostředí tou zásadní vlastností, jelikož úroveň zabezpečení firemního virtuálního stroje lze odděleně spravovat.

Kniha [7] identifikuje několik hrozeb spojených s provozem virtuálních strojů. Relevantní pro tuto práci jsou:

Škodlivý software Byly objeveny některé druhy škodlivého softwaru, které dokáží detekovat, že se nachází ve virtualizovaném prostředí. Díky tomu dokáží modifikovat svoje chování a lépe se tak maskovat.

Únik z virtuálního stroje Podle [7] zatím nebyl zaznamenán takový útok, kdy by kódu běžícímu uvnitř virtuálního stroje podařilo dostat ven a ohrozit tak hostitelský systém nebo jiný virtuální stroj. Koncept toho druhu útoků byl však několikrát dokázán v laboratorních podmínkách. Pro tyto koncepty je však nutné připravit jak software uvnitř hostitelského tak virtualizovaného systému, nebo využít některou z funkcí klienta pro sdílení mezi hostitelským a virtualizovaným systémem.

Další zranitelnosti Chyby v softwaru pro virtualizaci mohou znamenat například možnost vzdáleného vyřazení stanice z provozu, spuštění škodlivého kódu nebo dalších útoků. Zranitelnosti jsou předmětem bezpečnostních záplat.

3.2.3 Centralizovaná virtualizace

Pod pojmem centralizovaná virtualizace se rozumí běh virtuálních strojů na serveru ve výpočetním středisku. Používají se tedy hypervizory typu 1. Klienti k těmto virtuálním strojů přistupují vzdáleně pomocí technologie VDI. Nejsou tedy spotřebovávány výpočetní prostředky klienta, ale je zapotřebí kvalitní konektivita do výpočetního střediska.

Nejznámějšími zástupci centralizované virtualizace jsou: Microsoft remote desktop, VMWare Horizon, Citrix XenDesktop.

3.2.4 Distribuovaná virtualizace

Pojmem distribuovaná virtualizace se rozumí běh virtuálních strojů přímo na koncových stanicích uživatelů. Používá se tedy hypervizor typu 2. Spotřebovávají se tedy výpočetní prostředky stroje klienta, není však obecně potřeba konektivita s vnějším světem.

Nejznámějšími zástupci jsou: Oracle Virtualbox, VMWare Fusion, VMWare Workstation, VMWare Player, VMWare Horizon Flex, Parallels Desktop.

3.2.5 DaaS

Desktop as a service je variace na centralizovanou virtualizaci. Výpočetní středisko však není uvnitř společnost, ale vlastní jej externí subjekt. Ten pak jednotlivé pracovní stanice pronajímá formou pravidelných poplatků za službu. Pro IT oddělení tak odpadají náklady na správu serverů, síťové infrastruktury a dalších souvisejících opatření. Tento model není pro zkoumanou společnost vhodný, jelikož firemní data by se nacházela mimo společnost a docházelo by tak k ohrožení firemních aktiv.

Nejznámější poskytovatelé jsou: VMWare Horizon Air, Citrix XenDesktop, Amazon Work Spaces.

3.2.5.1 Virtualizace aplikací

Další možností je nevirtualizovat celý operační systém, ale pouze aplikace. Mezi výhody patří snadná aktualizace aplikací, snadná správa přístupu k aplikacím či nenáročnost na výpočetní výkon klienta. Data a přístupy je takto však možné oddělit pouze v rámci takto nasazených aplikací.

Mezi hlavní nevýhody patří problémy s periferiemi jako např. tiskárny či nutnost stálé a kvalitní konektivity.

Nejznámějšími zástupci služeb pro virtualizace aplikací jsou: Citrix XenApp, VMware Horizon, Dell vWorkspace, and Microsoft RDSH.

3.2.5.2 Používání webových aplikací

Variací na virtualizaci aplikací je jejich úprava pro přístup z webového prohlížeče. To však není možné u všech používaných aplikací ve zkoumané společnosti.

3.2.6 Rozlišení na úrovni sítě

Použitím Network Access Controll neboli NAC je možné spravovat přístup zařízení do sítě. Je možné nastavit autentifikační kontroly a další bezpečnostní politiky, které musí zařízení splňovat aby bylo do sítě vpuštěno.

Společnost Gartner identifikuje několik funkcí, které tato řešení nabízejí [30]. Politiky mohou pojmout různé fukce jako například autentifikaci zařízení, autorizaci uživatele, lokaci, čas či přístup k aplikacím a zdrojům.

Dále je možné posoudit stav zařízení z hlediska aktuálnosti systému a antivirových definic co se týče zařízení s Windows, nebo přítomnost EMM, viz 3.2.6.1, na mobilních zařízení.

Přístup je přidělován pomocí síťové infrastruktury s použitím 802.1X protokolu, virtuálních LAN, či seznamů pro řízení přístupů neboli ACL (Access Control List).

Dalšími službami poskytovanými NAC řešeními může být vytváření sítí pro hosty, monitoring připojených zařízení či integrace s dalšími bezpečnostními prvky.

Gartner ve své studii [30] zmiňuje následující prudukty: Aruba ClearPass, Auconet BICS, Brandford Networks Network Sentry, Cisco ISE, Extreme Networks ExtremeControll, ForeScout CounterACT, Impulse Point SafeConnect, Info Express CGX, Portnox CLEAR, Pulse Policy Secure, SnoopWall Netshield.

3.2.6.1 EMM/EMS

Enterprise mobility management nebo též Enterprise Mobility suite umožňují integrovat a spravovat mobilní zařízení v rámci firemní infrastruktury. Dle agentury Gartner jsou EMM balíky lepidlem, které připojuje mobilní zařízení do firemní infrastruktury. [11]

EMM mají následující funkce:

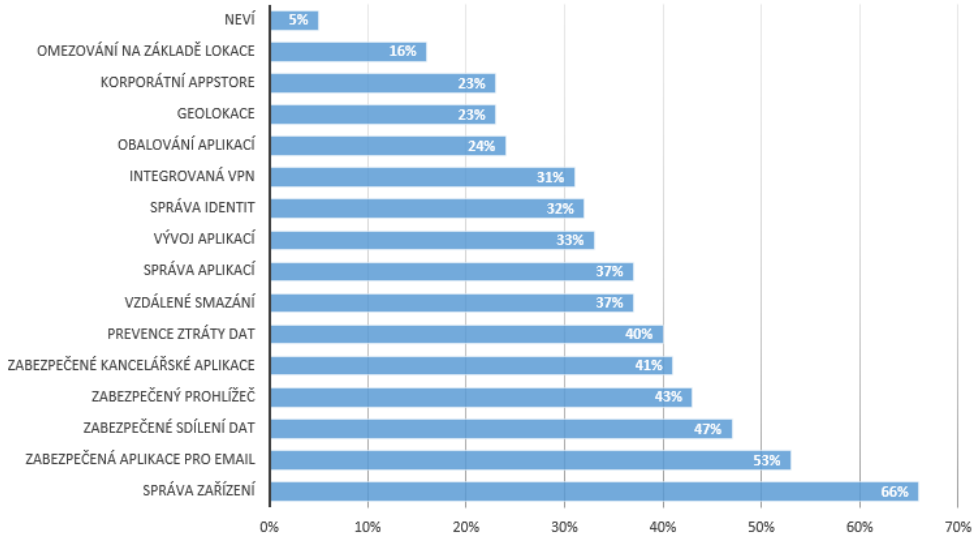
- nastavují zařízení a aplikace pro nasazení ve firemním prostředí
- sledují dodržení firemních politik a spravují firemní aktiva
- snižují riziko ztráty dat, krádeže či dalších incidentů řízením šifrování dat, přístupových práv, sdílených zařízení, obalováním aplikací či zamknutím zařízení.
- umožňují vzdálenou podporu zařízení pro IT oddělení

Výzkum společnosti J Gold Associates z roku 2016 [8] ukazuje, že firmy v drtivé většině nenasazují všechny funkce, které EMM řešení nabízejí. Nejpoužívanější funkce EMM jsou vypsány na obrázku (3.2.6.1)

3.2.7 MDM

Mobile device management je software pro správu mobilního zařízení. Je podmnožinou EMM. Mezi základní funkce tohoto software podle [42] patří:

- Automatické nastavení mobilního zařízení. Umožňuje IT oddělení nastavit zařízení podle firemních potřeb. To zahrnuje instalaci bezpečnostních certifikátů, nastavení uživatelských účtů či dalších nastavení umožňující přístup k firemní síti.
- Možnost vzdáleného vymazání. Umožňuje vzdáleně vymazat data tak, aby nebyla dostupné. To je užitečné v případě ztráty či krádeže zařízení, nebo po ukončení pracovního poměru se zaměstnancem.
- Vynucení bezpečnostních politik. To zahrnuje vynucení silného hesla, šifrování dat či omezení některých funkcí, například propojení se soukromým cloudovým úložištěm.



Obrázek 3.8: Které komponenty EMM řešení organizace zapojené do průzkumu aktuáně používají? Převzato z [8].

- Detekce jailbreak/root zařízení. Detekuje spuštění zařízení v administrátorském režimu, což je ve firemním prostředí nepřípustné.
- Blacklisting/whitelisting aplikací. Umožňuje správci zařízení zvolit, které aplikace je a není možné instalovat.
- Monitoring. Umožňuje sledovat přístupy uživatele k jednotlivým službám.
- Administrace. Umožňuje hromadné aktualizace, instalace či odinstalace aplikací pro zařízení ve firemní flotile.

3.2.8 MAM

Mobile application management. MAM je též podmnožinou EMM. Narozdíl od MDM nespravuje zařízení jako celek, ale pouze podnikové aplikace. Tyto aplikace jsou získávány přes speciální obchod s aplikacemi. Podle [43] mezi hlavní funkce MAM patří:

- Podnikový obchod s aplikacemi. Umožňuje nasazování vlastních i komerčních aplikací pro potřeby businessu.
- Podpora správy a distribuce aplikací s užitím API operačního systému či hromadného nákupu aplikací.
- Kontejnerizace aplikací

- Reporting o užívání aplikací

Podle [11] jsou pomocí MAM běžně uplatňovány následující politiky:

- Vyžadování iniciace VPN spojení pro aplikaci při spuštění
- Šifrování podnikových dat (často s použitím silnějšího šifrování než by bylo použito v rámci operačního systému)
- Omezení sdílení dat mezi aplikacemi pouze na podnikové aplikace
- Omezení copy/paste funkcionality
- Vyžadování specifického stavu při spuštění nebo při přístupu – například nebyl detekován root nebo jailbreak

3.2.9 MCM

Mobile content management. Jedná se o software pro správu obsahu na mobilních zařízeních. podle [11] má tři základní role:

- Vynucování politik. Dokáže vynutit politiky pro jednotlivé soubory včetně šifrovacích klíčů nezávislých na zařízení, autentifikace, pravidel pro sdílení souborů či pravidel pro copy and paste funkcionalitu.
- Přístup k obsahu. Vynutí pravidla pro distribuci, záměnu a mazání souborů.
- Integrace Přidává kompaktibilitu pro systémy správy práv, jako jsou ochrana ztráty dat (DLP) nebo podniková správa práv (EDRM) od třetích stran.

3.3 Výběr nejvhodnější varianty

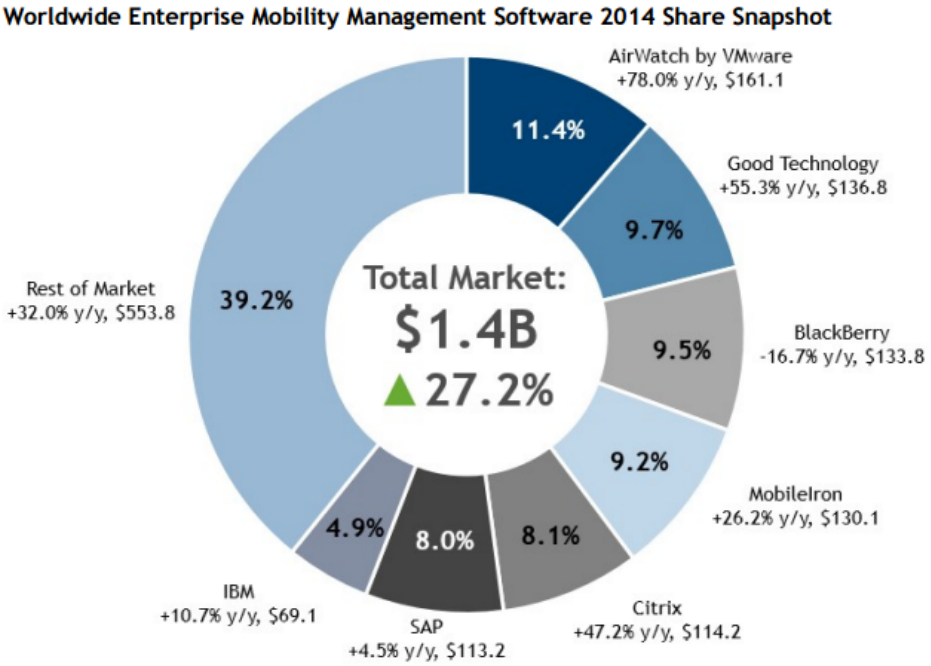
Předchozí analýzy prokázaly, že neexistuje řešení, které by dokázalo zastřešit všechny případy užití vlastních zařízení ve firemním prostředí. Proto tato práce bude dále dělit BYOD podle typu zařízení, a to na mobilní zařízení jako jsou mobilní telefony či tablety a notebooky.

3.4 Výběr řešení pro mobilní telefony a tablety

Podle analýzy 2.7.2 uživatelé žádají ze svých osobních mobilních telefonů a tabletů přístup k emailům a ke kalendáři. Firma se naopak snaží oddělit firemní data od soukromých tak, aby nad nimi měla kontrolu. Tyto požadavky splňují řešení EMM.

Trh s nástroji v posledních letech výrazně rostl, zároveň se však konsolidoval [44]. V grafech 3.9 a 3.10 je patrný nárůst trhu s EMM mezi lety 2014 a

2015 z 1,4 miliardy dolarů na 1,8 miliardy dolarů, tedy o 26,9 %. Zároveň je vidět zvyšování tržního podílu velkých hráču. Výrazný vliv měla také akvizice společnosti Good Technology společností BlackBerry.

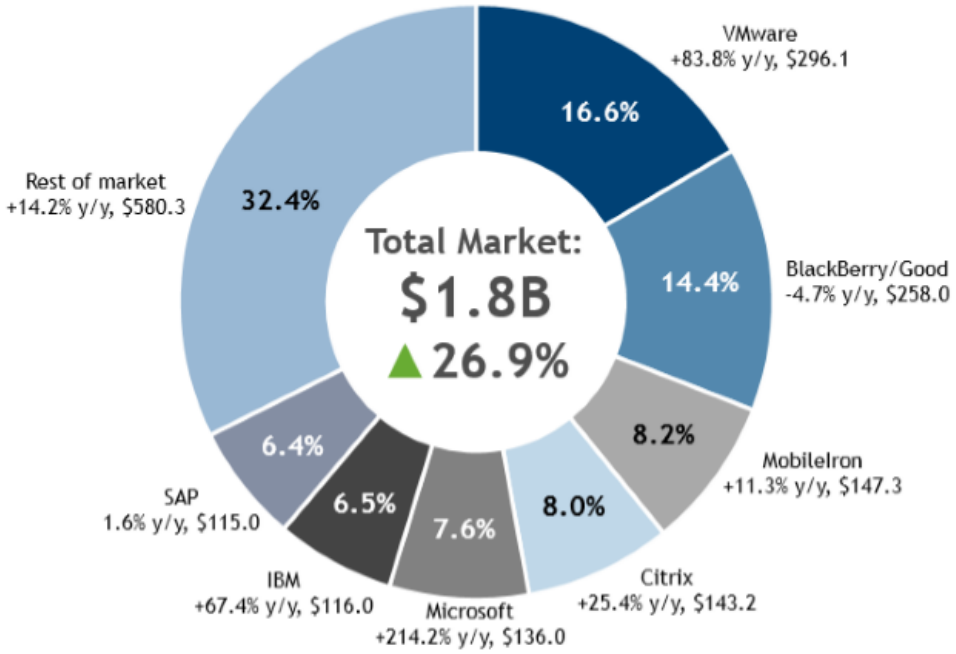


Obrázek 3.9: Podíl jednotlivých poskytovatelů EMM na trhu v roce 2014 podle IDC. Převzato z [9].

Podle magazínu CIOReview [45] bylo v roce 2016 pro BYOD nejslibnějších následujících dvacet poskytovatelů softwaru: Accelion, API Systems, Cyber adAPT, Ericom Software, Excelerate Systems, GSG Telco, High Point Solutions, LANDESK Software, Mathe, MobileIron, MobilityLab, Movius, RES Software, Sirama Consulting, Skycure, Storgrid, Tangoe, Tyfone, VmWare AirWatch, Zix Corporation.

Některé z nich jsou však příliš úzce zaměřené, či jsou pouze minoritními hráči na trhu. Analýza společnosti Gartner [11] z roku 2016 pro EMM rozděluje jednotlivé poskytovatele dle jejich postavení na trhu a zároveň hodnotí jejich schopnost zohlednit v produktu aktuální požadavky trhu a nasměrování produktu k budoucím potřebám zákazníků. Tato kritéria shrnuje společnost Gartner jako osy "schopnost vykonat"a "úplnost vize"ve svém grafu nazývaném magic quadrant 3.11.

Následující společnosti se nacházejí v kvadrantu lídrů:



Obrázek 3.10: Podíl jednotlivých poskytovatelů EMM na trhu v roce 2015 podle IDC. Převzato z [10].

3.4.0.1 VMWare Airwatch

VMWare koupil společnost AirWatch v roce 2014, viz [46]. Od té doby VMWare zařadil tento EMM do svého porfolia a postupně jej integruje s dalšími produkty jako jsou jeho nástroje pro IAM (Identity and Access Management) a SDN (software-defined networking). AirWatch nabízí širokou podporu pro nástroje třetích stran a je jedním ze zakládajících členů standardu AppConfig. VMWare AirWatch je vhodný pro společnosti, které hledají rozsáhlou funkcionalitu s podporou mnoha platforem.

Podle [11] byla prokázána nasaditelnost do rozsáhlých prostředí a snadná administrace. Na druhou stranu se objevily problémy s technickou podporou a také nutnost použít řešení od třetí strany pro PIM (Person information management).

3.4.0.2 MobileIron

MobileIron je veřejně obchodovatelná společnost (NASDAQ: MOBL), která se jako jedna z posledních soustředí pouze na svůj EMM produkt. Nabízí však širokou podporu aplikací třetích stran a je jedním ze zakládajících členů standardu AppConfig. Společnost je ceněna pro schopnost přinášet nové funkce na všechny tři hlavní mobilní platformy a plnění amerických bezpečnostních

Obrázek 3.11: Gartner Magic quadrant. Převzato z [11]

certifikací. Jedná se o produkt, který nabízí mnoho funkcí, škálovatelnost, stabilitu a integraci s dalšími aplikacemi.

Řešení nabízí nástroj pro reporting, pokročilou integraci se SIEM (security information and event management) řešeními třetích stran či správu z mobilního zařízení. Získává kladné ohlasy na svou stabilitu, použitelnost, škálovatelnost a rozsáhlý ekosystém přidružených aplikací AppConnect. MobileIron se drží mezi prvními při nasazování pro nové verze operačních systému.

Na druhou stranu podle [11] jsou známé případy, kdy zákazníci měli potíže získat technickou podporu. Aplikace Apps@Work nabízejí zastaralý uživatelský zážitek a zároveň existuje nejistota ohledně budoucnosti firmy vzhledem ke změnám ve vrcholném managementu.

3.4.0.3 Citrix

Řešení od společnosti Citrix se skládá z produktů NetScaler, ShareFile a Xen Mobile. Je silné především díky balíku kontejnerizovaných aplikací Worx. ShareFile je kvalitní EFSS (Enterprise file synchronization and sharing) řešení. Obsahuje též uživatelsky přívětivé DLP (Data loss prevention). XenMobile je vhodný pro společnosti s existující infrastrukturou od Citrixu nebo pro ty, jež požadují široké spektrum funkcí.

Společnost Gartner zaznamenala problémy u nasazení XenMobile jako SaaS (Software as a service) u velkých projektů (tj. více než 20000 zařízení) [11]. Přestože XenMobile nabízí možnost virtualizace Windows aplikací pro mobilní zařízení, použitelnost je na na mobilních zařízeních sporná, vzhledem k dotykové povaze ovládání uživatelského rozhraní.

3.4.0.4 IBM

IBM nabízí kompletní balík EMM nástrojů MaaS360. Podporuje všechny významné operační systémy, nabízí dobrou spolupráci s dalším bezpečnostním software od IBM. Jedná se o produkt, který má velký záběr, co se týče funkcionality, ale přitom je snadno nasaditelný, viz [11].

3.4.0.5 BlackBerry

BlackBerry nyní prodává svůj nástroj jako Good Secure EMM Suite. Skládá se z BES12, Good collaboration apps, Good dynamics a WatchDox Enterprise. Produkty pod značkou Good a WatchDox získala Blacberry akvizicemi které byly dokončeny v roce 2015, viz [47, 48].

Podle agentury Gartner je Good Secure EMM Suite vhodný pro organizace s přísnými požadavky na bezpečnost či působící v regulovaném sektoru. Těm nabízí silnou sadu nástrojů pro ochranu. Zároveň existuje silná podpora pro starší verze software od BlackBerry. Nástroj Good Work nabízí jeden z nejlepších zabezbečených Personal information manager (PIM) nástrojů. Podpora od BlackBerry získává mnoho kladných hodnocení od zákazníků.

Vícevrstvá cloudová verze produktu BES12 umisťuje data do datacenter ve dvou lokacích, a to Kanadě a Nizozemsku. To by mohl být pro některé bezpečnostní politiky problém. Zároveň u balíku od společnosti BlackBerry dochází k roztříštěnosti služeb mezi jednotlivými produkty.

Další řešení:

3.4.0.6 Cisco

Cisco se dostalo mezi společnosti nabízející MDM software akvizicí společnosti Meraki v roce 2012 [49]. Kromě řešení pro Android a iOS nabízí také podporu pro Windows a MAC OS X. Nabízí hlubokou integraci do síťové in-

grastruktury. Správa produktu nabízí velice jednoduché a přívětivé uživatelské rozhraní. Cenově se jedná o levnější řešení než u většiny konkurentů.

Výhody integrace do síťové infrastruktury je možné využít pouze v případě, že organizace používá sítovou infrastrukturu od Cisco/Meraki. Meraki neobsahuje všechny součásti EMM, soutředí se pouze na MDM.

3.4.0.7 Microsoft

EMM produkt od Microsoftu se nazývá Enterprise Mobility Suite. Skládá se z Microsoft Intune, Azure Active Directory Premium, Advanced Threat Analytics a Azure Rights Management. MDM a MAM služby jsou soustředěny v Microsoft Intune. Toto řešení je nabízeno pouze jako služba v cloudu. Řešení od Microsoftu je vhodné pro společnosti, které nemají vysoké nároky na správu a používají Office 365 nebo Azure Active Directory.

3.4.0.8 Landesk

Landesk se zaměřuje především na UEM (User Evironment Management) a jeho řešení Landesk Mobility Suite tak zapadá do jeho portfolia jako doplněk pro mobilní zařízení. Je tedy vhodné především pro firmy, které mají potřebu spravovat desktopové prostředí a mobilní zařízení zároveň.

3.4.0.9 Další řešení

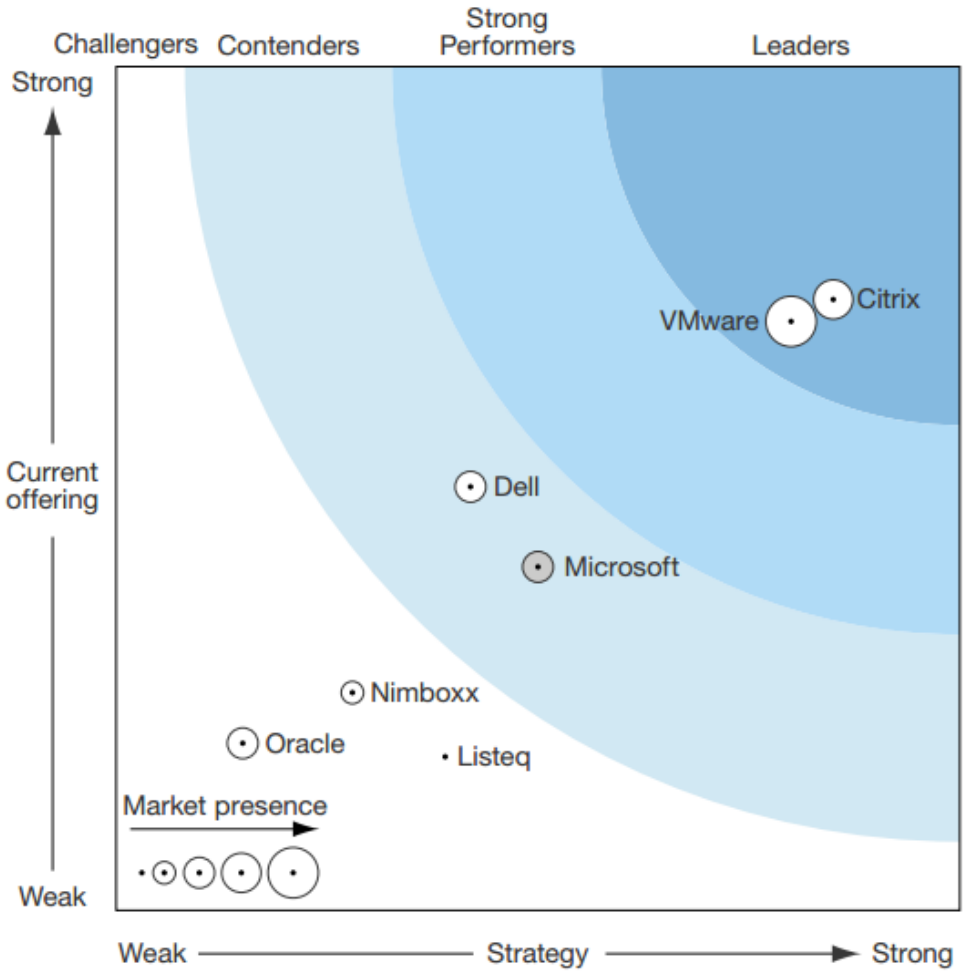
Ostatní řešení byla v [11] prezentována jako nabízející příliš úzké zaměření, nedostatečnou funkcionalitu nebo nevhodnost pro nasazení ve větším měřítku

3.5 Výběr řešení pro notebooky

Vzhledem k požadavkům na bezpečnost a dodržování přísných firemních politik v bance a zároveň k potřebě přístupů k různým typům software a aplikací se zdá jako jediné vhodné řešení BYOD virtualizace desktopu. Způsobů, jakými může virtualizace sloužit pro řešení BYOD je více.

Analýza [12] ze září roku 2015 od společnosti Forrester se zaměřuje na virtuální desktopy umístěné na vlastním serveru. Výhodou oproti DaaS řešení je, že aplikace i data jsou pod úplnou kontrolou IT oddělení, což snižuje riziko ztráty nebo krádeže dat. Nevýhodou těchto řešení může být problémová funkčnost některých periferních zařízení, jako jsou webové kamery nebo tiskárny. Dále jsou tato řešení velmi citlivá na stabilitu a rychlost internetového připojení, a především u graficky náročnějších aplikací.

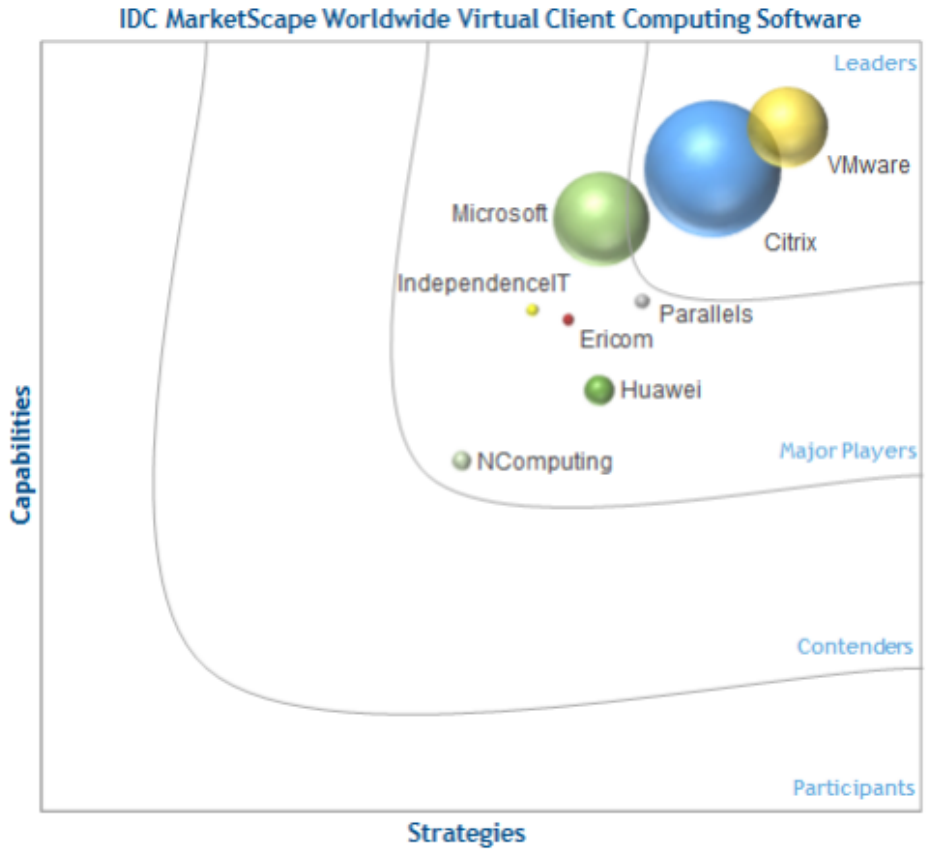
Podle této analýzy jsou jasnými lídry trhu s centralizovanou virtualizací společnosti Citrix a VMWare, a to s obrovským tržním i technologickým náskokem. V grafu 3.12 je vidět také společnost Dell, která však již vlastní řešení dále nenabízí a prohlubuje spolupráci s produkty od VMWare, jelikož tuto



Obrázek 3.12: The Forrester Wave: Virtuání desktopy umístěné na serveru. Převzato z: [12].

společnost získala akvizicí jejího původního vlastníka společnosti EMC, v září roku 2016 [50].

Průzkum trhu od společnosti IDC [13] z roku 2016 má širší zaměření, a to na poskytovatele VCC (Virtual Client Computing). Ty definuje jako poskytovatele, kteří tvoří a prodávají software pro virtualizaci se zaměřením na centralizované virtuální desktopy, distribuované virtuální desktopy a software pro virtuální uživatelské sezení (VUS). Průzkum je zaměřen především na obchodní úspěch hodnocených společností. Dále doporučuje zohlednit při výběru poskytovatele kvalitu systému pro správu zařízení, bezpečnost řešení, možnosti grafického výstupu a kompaktibilitu s užívanými aplikacemi.



Obrázek 3.13: IDC MarketScape: Hodnocení dodavatelů VCC. Převzato z: [13].

Podle tohoto průzkumu trhu s VCC jasně vládnou společnosti VMWare a Citrix. Nikdo další již nebyl zařazen do segmentu lídrů. Za zmínku dále stojí Microsoft, který má na trhu silnou pozici.

3.5.1 Citrix

Řešení XenDesktop se vyznačuje podporou vlastního protokolu HDX díky kterému se snaží o adaptivní kompresi, de-duplikaci síťového provozu a přesměrování tíhy renderování dle okolností na klienta a to na všech podporovaných platformách [51]. Dále podporuje vícenásobné 4k monitory a pokročilé funkce pro multimedia a videokonference. Výhodou je podpora amerického bezpečnostního standardu FIPS 140-2. Podle [12] má XenDesktop výborné uživatelské hodnocení, avšak technická podpora je pomalá.

Oproti konkurenčnímu produktu od VMWare nabízí Citrix i virtualizaci Linuxových desktopů. Chlubí se třikrát rychlejším tiskem, šestkrát rychlejším

spouštěním aplikací, pětkrát rychlejším ukládání souborů či podporou virtualizovaného Skype for Bussiness. Je možné jej nasadit na jakýkoliv cloud, jakýkoliv hypervizor, síť, do cloudu, lokálně či hybridně, viz [52, 53].

XenDesktop je možné provozovat také v cloudu. Zvolit lze libovolný hypervizor z nabídky VMWare ESX, Microsoft Hyper-V nebo Citrix XenServer. Pro offline použití existuje hypervizor typu 2 pro MacOS a Windows jménem DesktopPlayer.

Pro virtualizaci aplikací nabízí Citrix platformu XenApp.

3.5.2 VMWare

VMWare nabízí produkt VMWare **Horizon View**. Použitý protokol je PCoIP od firmy Teradici. Je vhodný v kombinaci serverem vSphere, kdy nabízí dobrou integraci. Nabízí též škálování do cloudu v kooperaci s řešením Horizon Air. Taktéž moduly software od VMWare splňují bezpečnostní standard FIPS 140-2 [54]. Horizon View je také možné zakoupit jako součást kompletního balíku, který obsahuje taktéž Horizon Flex pro offline použití. Podle [12] hodnotí zákazníci produkt jako dobrý s několika problémy, jako například nutnost použití příkazové řádky pro některá nastavení.

Další produkty pro virtualizaci pracovních prostředí jsou podle výrobce [55] následující:

Horizon 7 je platforma od VMWare pro virtuální desktopy a aplikace. *Řešení Horizon 7 umožňuje zajišťovat, spravovat a chránit virtuální desktopy (VDI) a aplikace prostřednictvím jedné platformy.*

Horizon Air je DaaS řešení od VMWare. *Poskytuje virtuální desktopy a aplikace hostované v cloudu s širokou škálou možností včetně sdílených desktopů a aplikací.*

Horizon Flex je řešení, které *doručuje, spravuje a zabezpečuje místní virtuální desktopy se systémem Windows na počítačích Mac i PC a současně zajišťuje zabezpečení, možnosti řízení a dodržování požadavků.*

App Volumes je *portfolio integrovaných řešení pro správu aplikací a uživatelů pro virtuální prostředí řešení Horizon, Citrix XenApp a XenDesktop a RDSH.*

Mirage *nabízí správu bitových kopií desktopů pro fyzické desktopy a zařízení POS v nejrůznějších distribuovaných prostředích.*

NSX for Horizon *je síťové řešení infrastruktury virtuálních desktopů (VDI) se zásadami, které jsou dynamicky spojeny s desktopy.*

Virtual SAN for Horizon *Řešení VMware vSAN snižuje zákazníkům počáteční náklady a umožňuje jim využívat celou řadu předkonfigurovaných zařízení pro řešení Horizon, včetně zařízení Virtual SAN Ready Node a infrastruktury postavené na řešení EVO SDDC.*

*VMware **ThinApp** je řešení pro virtualizaci aplikací bez agentů, které izoluje aplikace od použitých operačních systémů a díky tomu eliminuje konflikty a zjednodušuje doručování a správu.*

Řešení User Environment Manager *nabízí podnikovou správu uživatelů vytvářející přizpůsobené prostředí pro koncové uživatele na všech zařízeních a místech.*

Produkty Fusion počítače Mac *Pomocí řešení VMware Fusion a VMware Fusion je možné používat na počítači Mac bez restartování systém Windows a stovky dalších operačních systémů.*

Produkty Workstation systém Windows Řešení VMware Workstation a VMware Workstation Player představují oborový standard pro používání více operačních systémů jako virtuálních strojů na jednom počítači PC.

Řešení Workstation systém Linux Produkty řešení VMware Workstation systém Linux představují oborový standard pro používání více operačních systémů jako virtuálních strojů na jednom počítači se systémem Linux.

VMware tvrdí, že jeho řešení nabízí oproti konkurenčnímu Citrixu lepší správu a reporting nebo také centrální správu obrazů systémů ať už pro fyzické, virtuální nebo BYOD stroje [56].

3.5.3 Microsoft

Microsoft nabízí virtuální pracovní stanice skrze platformu Windows Server. Nenabízí sice DaaS řešení, ale nabízí virtualizaci aplikací Microsoft Azure RemoteApp. Ty mohou fungovat buďto v čistě cloudovém nebo hybridním módu. VDI je provozováno pod značkou RDS (Remote Desktop Service) jako uživatelské sezení na Windows Server. Z toho důvodu nenabízí tolik možností nastavení a správy jako plná virtualizace [57].

3.5.4 Oracle

Oracle nabízí nástroj Secure Global Desktop, který je možné použít s různými hypervizory, je ovšem optimalizovaný pro Oracle. Hlavní devízou řešení je kvalitní konzole pro správu Oracle Enterprise Manager. Podle [12] toto řešení není vhodné pro případy užití mimo prostředí s vysokým podílem aplikací od Oracle.

Dále nabízí program VirtualBox. Jedná se o hypervizor typu 2, v základní verzi je zdarma i pro komerční užití. Je zaměřený spíše na vývojáře a nenabízí mnoho nástrojů pro vzdálenou správu [58].

3.5.4.1 Amazon

Amazon nabízí DaaS službu Amazon Workspaces. Je postavená na platformě Windows server 2008 a používá protokol PCoIP, viz [59]. Je možné volit z mnoha hardwarových konfigurací. Službu lze propojit s firemním Active directory.

Kapitola 4

Návrh řešení

V této kapitole bude podrobně popsán návrh řešení pro BYOD program ve vybrané organizaci. Volba produktů pro uskutečnění řešení bude odůvodněna a taktéž bude popsána jejich funkcionalita. Závěr kapitoly se věnuje nasazení vybraného řešení jak po technické stránce, tak po stránce formální.

4.1 Návaznost na stávající řešení

V Bance existuje projekt pro centralizovanou virtualizaci. Navržené řešení na tento projekt nenavazuje a navrhuje jiný přístup. Zároveň je nasazována infrastruktura pro použití BlackBerry Work. Tato práce na toto řešení navazuje a rozšiřuje jeho použití jako součást koncepce návrhu uceleného BYOD programu.

Použitá síťová infrastruktura ve firmě je nyní vcelku komplexní. Navržené řešení se snaží nasazené infrastruktury využít a nenavrhuje žádné významné změny.

Stávající proces připojování nefiremních zařízení by měl být nahrazen zařazením nefiremních zařízení do uceleného BYOD programu

4.2 Návrh řešení pro notebooky

Banka nehledá komplexní řešení pro virtualizaci pracovních stanic. Stávající situace, kdy zaměstnanci používají firemní zařízení, je vyhovující a není důvod do ní jakkoli výrazněji zasahovat. Je však třeba najít odpověď na narůstající trend vlastních zařízení a především představit rámec pro kontraktory, kteří firemním zařízením nedisponují tak, aby nebyli rizikem pro vnitřní síť a jejich chování v rámci sítě bylo kontrolováno firemními politikami.

Vzhledem k nárokům kladeným na BYOD v Bance, viz 2.7.1, vychází jako řešení nejlépe distribuovaná virtualizace. Navržené řešení umožňuje pokročilou správu distribuovaných virtuálních strojů nutnou pro plnění firemních politik,

odděluje pracovní prostředí od soukromého operačního systému, viz 2.6.1, neklade vysoké náklady na konektivitu a síťovou infrastrukturu, viz 2.9.2, a dokonce umožňuje práci offline. Jediným uceleným řešením s distribuovanou virtualizací a současnou možností vzdálené správy klientů je VMware Horizon FLEX. Tato práce jako řešení BYOD pro notebooky tedy navrhuje produkt VMware Horizon FLEX.

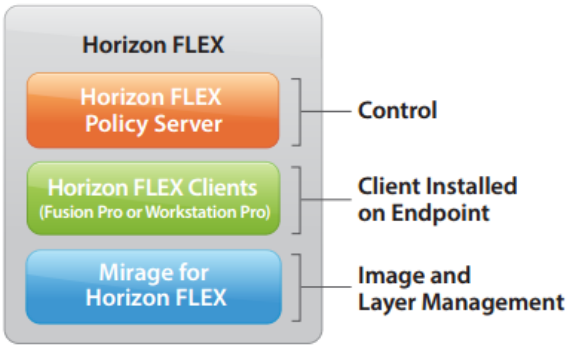
4.2.1 VMware Horizon Flex

V roce 2014 VMware představil VMware řešení VMware Horizon Flex. Jedná se o kombinaci některých stávajících technologií jako je Fusion, Player, Mirage či AirWatch. Dle [60] je odpovědí na požadavky zákazníků provozovat virtuální desktopy offline. Zároveň přináší výhody virtualizace, ale nenese s sebou velké náklady v podobě nutnosti výkonných serverů a dostatečného diskového úložiště, jako tomu je v případě centralizované virtualizace, což byl jeden s hlavních důvodů, proč centralizovaná virtualizace ve zkoumané organizaci není rozšířena jako alternativa pro řešení BYOD, viz 2.9.2. Oproti centralizované virtualizaci taktéž odpadají problémy s vysokými nároky na konektivitu a špatnou odezvou.

Uživatelé mohou přistupovat do korporátní sítě z korporátního obrazu operačního systému, ale přitom používat své vlastní notebooky nebo počítače od firmy Apple, bez toho, aby tyto zařízení muselo IT oddělení podporovat. Jinými slovy, IT může plně spravovat korporátní systém bez toho, aby zasahovalo do operačního systému uživatele. Bezpečnostní rizika jsou minimalizována díky oddělení obou operačních systémů a možnosti vzdáleně řídit omezení pro virtuální stoj, či ho dokonce vzdáleně uzamknout či smazat. Tato možnost je obzvláště výhodná u externích pracovníků, kterým může vypršet kontrakt. Do systému Horizon FLEX je možné zapojit také obrazy virtuálních strojů sloužící pro testování a lépe je tak spravovat.

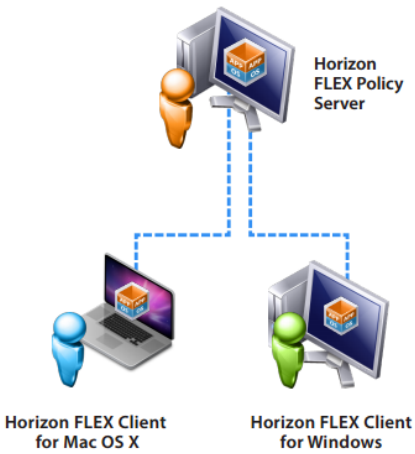
Technicky se jedná o hypervizor typu 2, který je spravovaný centrálně. Je možné jej nasadit jak pro koncové stanice s Mac OS, tak s Windows. Spravovat, zálohovat a záplatovat systém je též možné centrálně, a to s užitím serveru Mirage for Horizon FLEX. Pro nastavení politik řešení obsahuje Horizon FLEX Policy Server, jako klient je použit VMware Fusion Pro pro počítače Mac a VMware Workstation Player pro počítače s Windows, viz [14]. Pro klienta jsou podporovány následující 64bitové operační systémy: Windows 7, Windows 8.1, Windows 10, Mac OS X 10.9, Mac OS X 10.10 a Mac OS X 10.11.

Různě nastavené virtuální stroje je možné distribuovat různým uživatelům. Uživateli musí být nejdříve nainstalován klient, a tedy Fusion Pro nebo Workstation Player. Uživatelský systém potřebuje přístup k Horizon FLEX Policy serveru v následujících případech: pro úvodní stažení obrazu stroje a pro získání aktualizací politik a omezení. Horizon Flex Policy Server musí být pro klienta dostupný pomocí protokolu https. Je možné nastavit maximální



Obrázek 4.1: Vrstvy produktu VMWare Horizon FLEX. Převzato z: [14].

počet dní bez připojení k Policy Serveru. Minimimální hardwarové požadavky serverů jsou sepsány v příloze (C)



Obrázek 4.2: Schéma pro připojení k Horizon Flex Policy serveru. Převzato z: [14].

S užitím Policy serveru mohou administrátoři mimo jiné spravovat inventář omezených virtuálních strojů, procházet seznam uživatelů a skupin ve službě Active Directory, přiřazovat uživatele a skupiny k jednomu či více virtuálnímu stroji, specifikovat politiky pro dané přiřazení, omezit uživateli přístup k virtuálnímu stroji vzdáleným zamknutím nebo kontrolovat stav virtuálního stroje.

Pro nastavování politik slouží webové uživatelské rozhraní. Je možné nastavit následující omezení:

- Expirační doba – Doba, po kterou je virtuální stroj přístupný.

- Použití USB zařízení – Blokování použití zvolených USB zařízení.
- Copy&Paste operace – Omezení funkce copy and paste mezi hostitelským a virtualizovaným operačním systémem.
- Drag&Drop operace – Omezení drag and drop funkcionality mezi hostitelským a virtualizovaným operačním systémem.
- Zadání hesla pro kopírování či přesouvání virtuálního stroje.
- Omezení existujících instancí virtuálního stroje na jednu.
- Omezení možnosti přidělování hardwarových prostředků pro virtuální stroj.

Virtuální stroj je též možné vzdáleně uzamknout a nebo smazat.

4.2.2 Doporučení pro korporátní obraz virtuálního stroje

Obraz virtuálního stroje by měl odpovídat nastavení operačního systému pro firemní zařízení. Speciálním omezením by mělo být vynucení přístupu do sítě pouze prostřednictvím firemní VPN.

4.2.3 Dodatek k návrhu pro uživatele s operačními systémy linuxového typu

Řešení Horizon Flex bohužel nepodporuje operační systém Linux. Pro tento specifický typ uživatelů je tedy třeba navrhnout alternativu. Jelikož klient řešení Horizon Flex je produkt VMware workstation Pro, je vhodné pro zachování konzistence návrhu uživatelům operačního systému Linux navrhnout tohoto klienta. VMware Workstation for Linux podporuje následující operační systémy: Ubuntu 8.04 a vyšší, Red Hat Enterprise Linux 5 a vyšší, CentOS 5.0 a vyšší, Oracle Linux 5.0 a vyšší, open SUSE 10.2 a vyšší, SUSE Linux 10 a vyšší. U dalších distribucí systému typu Linux a Unix není oficiální podpora, ale řešení může být funkční.

V tomto klientu je možné spouštět zašifrované omezené virtuální stroje určené pro Horizon Flex. Vzhledem k neexistenci komunikace s Policy serverem však není možné nastavené politiky dodatečně měnit či vzdáleně smazat nebo spravovat obraz virtuálního stroje. Přístup do stroje a firemní sítě však lze znemožnit zneplatněním přístupu daného uživatele skrze Active directory, stále se tedy jedná o bezpečné řešení.

4.2.4 Licencování

Licence na Horizon Flex se vztahuje k zařízení. Prodávají se pouze v balících. Jeden balík obsahuje 10 licencí pro klienta a licenci pro VMWare Mirage For Flex a Horizon FLEX Policy Server.

Pro klienty VMware Workstation For Linux je třeba zakoupit zvláštní licenci.

4.3 Návrh řešení pro mobilní zařízení

Z analýzy požadavků uživatelů, viz 2.7.3, vyplynulo, že pro mobilní telefony je požadována především dostupnost emailu a pro tablety je to především dostupnost emailu, dokumentů a PIM. Z hlediska požadavků byznysu je to vzhledem k povaze bankovního sektoru především vysoká bezpečnost.

Přestože leaderem trhu EMM je řešení AirWatch od společnosti VMware, v klíčových vlastnostech není nejsilnější. AirWatch je vysoce modulární řešení schopné plnit vysoké nároky. Jeho slabou stránkou je PIM, kde je doporučeno použít řešení od třetí strany.

V klíčových požadavcích exceluje řešení od společnosti BlackBerry. Pro email a PIM nabízí kvalitní produkt BlackBerry Work. V oblasti bezpečnosti je společností Gartner hodnocen, viz [15], jako nejsilnější hráč na trhu. Tato práce navrhuje jako řešení BYOD pro mobilní telefony a tablety řešení BlackBerry Enterprise Mobility Suite.

Společnost Gartner hodnotila produkt v několika kategoriích.

Z hlediska certifikací a ocenění je situace rozdílná pro každou aplikaci v balíku. Good Dynamics je certifikován jako EAL4+. Kryptografické komponenty jsou certifikovány jako FIPS 140-2 Level 1. Mezi další certifikace, které splňují komponenty od Good technologies, patří například ISO 19790 či další státní a armádní normy.

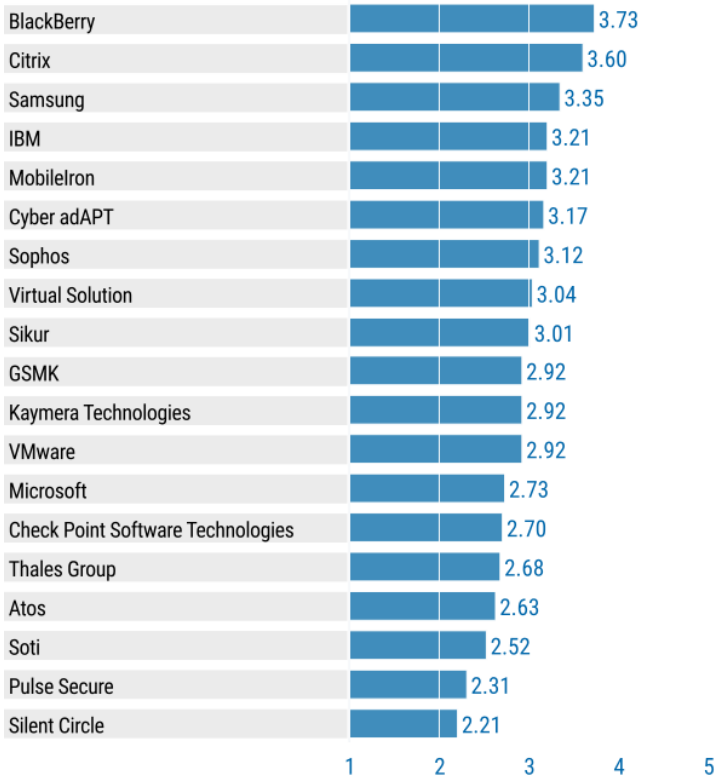
Co se týče MDM, nabízí BlackBerry všechny běžné funkce. Platforma podporuje Android for Work i Samsung Knox. Kontejnerizaci aplikací zajišťuje komponenta Good Dynamics. Aplikace je možné chránit hesly a přiřazovat jim certifikáty. Kontejnery mezi sebou mohou komunikovat s užitím certifikátů podepsaných backendovým serverem.

Dalším důvodem pro volbu BlackBerry je použití tohoto řešení v mateřské firmě. Během analýzy bylo zjištěno, že toto řešení se připravuje také pro zkoumanou organizaci, a že během vypracovávání této diplomové práce začala fáze plošného nasazování. Jelikož je řešení od BlackBerry podle analýzy požadavků v této práci nejvhodnějším řešením, tato práce nasazení zvoleného řešení podporuje. Řešení je integrovatelné s řešením od různých poskytovatelů NAC včetně použitého řešení od Cisca.

4.4 BlackBerry Enterprise Mobility Suite

Nejdůležitější komponentou pro potřeby Banky je BlackBerry Work. Dle specifikací [61] nabízí následující funkcionalitu:

Email:



Obrázek 4.3: Hodnocení dodavatelů software pro vysoce bezpečnou správu mobilních zařízení v kategorii BYO od společnosti Gartner. Převzato z: [15].

- Synchronizace emailu
- Správa emailu
- Zabezpečené zobrazování příloh
- Správa fotografií
- Vyhledávání emailů na serveru
- Prioritizace oznámení
- Integrace s nositelnostmi

Kalendář:

- Synchronizace kalendáře
- Připojení ke konferenčním hovorům
- Plánování meetingů

- Zprávy "mimo kancelář"
- Zobrazení přijatých pozvánek

Kontakty:

- Synchronizace kontaktů
- Vyhledávání v pracovních kontaktech přímo z telefonu
- Historie zpráv

Kolaborace:

- Ukládání souborů do repozitáře
- Zabezpečený prohlížeč pro přístup k firemnímu intranetu
- Správa úkolů
- Přístup k dokumentům ve službách SharePoint, OneDrive nebo Box
- Prezentační mód pro prezentaci PowerPoint dokumentů

Zajímavou funkcí je jednoduchý přístup pomocí funkce Touch ID na zařízeních s operačním systémem iOS podporující funkci Touch ID.

Možnoti administrace:

- Šifrovaný kontejner
- Integrované MDM
- Jednotný dokumentový server
- Integrované MAM
- Použití technologie Exchange ActiveSync
- Rozdělení účtování dat na pracovní a soukromý provoz

4.4.1 Návrh licencování

Nejnutnější funkce pro splnění požadavků předpokládaných uživatelů BYOD splňuje komponenta BlackBerry Work. Ta je součástí skupiny služeb BlackBerry Dynamics. Aplikace BlackBerry Dynamics se licencují pouze jako součást balíku Blackberry Enterprise Mobility Suites, který je nabízen v různých edicích.

Pro splnění požadavků na funkce emailu postačuje edice BlackBerry Enterprise Mobility Suite – Enterprise Edition. Pro pokročilejší práci s dokumenty

vyžadovanou pro BYOD tablety je třeba zakoupit vyšší edici BlackBerry Enterprise Mobility Suite – Collaboration Edition, viz [62]. Tato vyšší edice je též třeba pro integraci s IM klientem Skype for Bussiness.

Tato edice nabízí následující typy aktivace: Work and personal - Regulated, Work space only, Work and personal - user privacy (Android for Work – Premium), Work space only (Android for Work - Premium), Work and personal - user privacy (Samsung KNOX), Work and personal - full control (Samsung KNOX), Work space only (Samsung KNOX). Nabízí tedy vhodné možnosti jak pro BYOD zařízení, tak pro správu firemních zařízení.

Pro BYOD mobilní telefony s operačním systémem Android je tedy vhodná licence BlackBerry Enterprise Mobility Suite – Enterprise Edition a typ aktivace Work and personal – user privacy.

Pro BYOD mobilní telefony s operačním systémem iOS je vhodná licence BlackBerry Enterprise Mobility Suite – Enterpirse Edition a typ aktivace user privacy.

Pro BYOD tablety s operačním systémem Android je nejvhodnější licence BlackBerry Enterprise Mobility Suite – Collaboration Edition a typ aktivace Work and personal - user privacy (Android for Work - Premium).

Pro BYOD tablety s operačním systémem iOS je nejvhodnější licence BlackBerry Enterprise Mobility Suite – Collaboration Edition a typ aktivace User privacy.

Pro všechny BYOD užití je vhodnější serverový typ licence.

Informace o licencování byly čerpány z oficiální dokumentace [63].

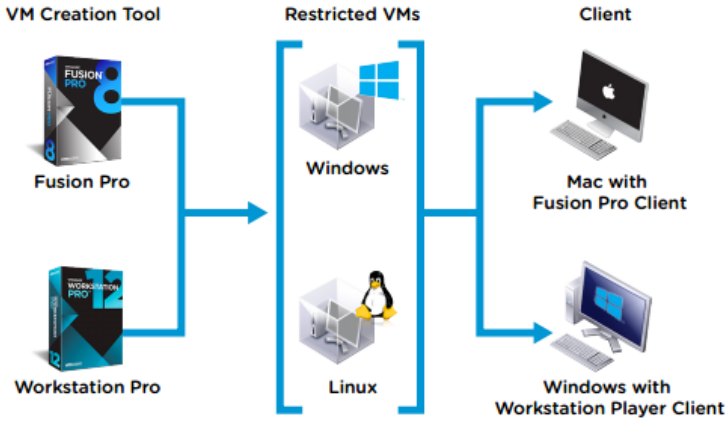
4.5 Hodnocení navrhované varianty zástupci organizace

Zástupci vybrané společnosti ohodnotili návrh jako jako splňující požadavky. Ocenili především splnění nároků na bezpečnost díky důslednému oddělení soukromého a pracovního prostředí. Z hlediska nasazení je hodnocen jako proveditelný, přičemž detailní plán nasazení by musel být analyzován a schválen dalšími odděleními vzhledem k zásahům do infrastruktury a součinnosti s jinými běžícími projekty. Úskalím projektu by mohlo být vyjednávání o zapojení do programu s externími dodavateli a kontraktory.

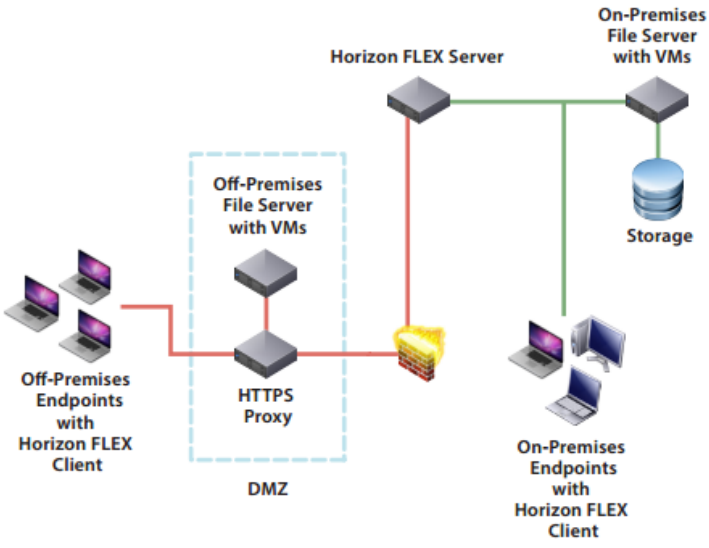
4.6 Návrh nasazení řešení pro notebooky

V první řadě je třeba vyhradit prostor ve kterém budou umístěny obrazy pro virtuální stroje. Je vhodné připravit souborové servery pomocí IIS, a to jeden uvnitř podnikové sítě a jeden vně. Dále je potřeba nainstalovat Mirage Management server a jeho komponenty. Po zadání sériového čísla se zpřístupní funkce pro Horizon FLEX, viz [16].

Jelikož se v prostředí Banky používá operační systém Windows, pro vytvoření obrazu pro virtuální stroj je potřeba použít nástroj VMware Workstation Pro, viz. obrázek 4.4



Obrázek 4.4: Schéma postupu pro vytvoření obrazu virtuálního stroje. Převzato z: [16].



Obrázek 4.5: Ilustrační schéma infrastruktury pro nasazení VMware Horizon FLEX. Převzato z: [16].

Po instalaci serveru Mirage je třeba nainstalovat ostatní komponenty Horizon FLEX, nastavit certifikáty pro virtuální stroje, vytvořit a přiřadit vir-

tuální stroje a nakonec nainstalovat klienty na koncová zařízení. Klienty je možné distribuovat uživatelům s připravenými virtuálními stroji.

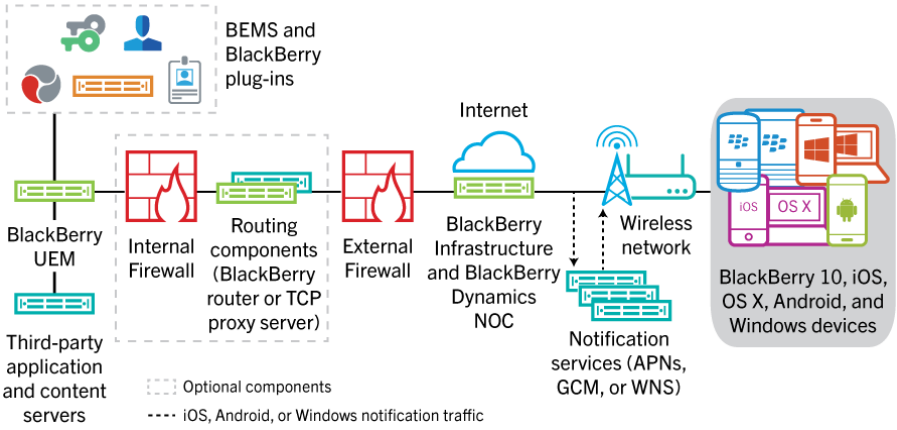
Jelikož jeden Horizon FLEX Server dokáže obsloužit až 10000 uživatelů, stačil by pro potřeby organizace pouze jeden server. Firemním standardem je však zajistit u podobných služeb vysokou dostupnost.

4.7 Návrh nasazení řešení pro mobilní zařízení

Jelikož nasazení řešení ve zkoumané organizaci již započalo, návrh nasazení se soustředí spíše na popis a využitelnost řešení, nežli na technickou specifikaci návrhu pro nasazení.

4.7.1 Komponenty řešení

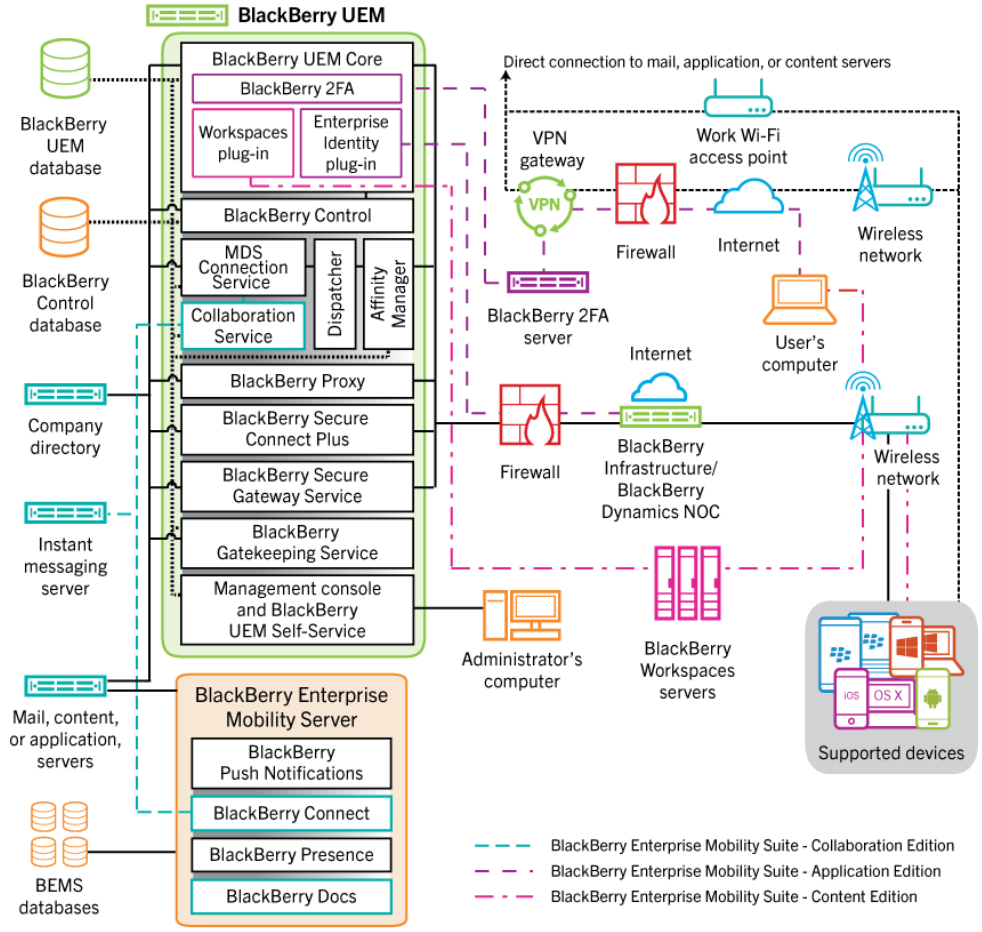
Základním kamenem řešení je BlackBerry Unified Endpoint Management (UEM). Jedná se o infrastrukturu pro zajištění MDM, viz [17]. BlackBerry Infrastructure je vnější server, který spravuje informace o zařízení, jako jsou licence a šifrovaně komunikuje s UEM a také s koncovými zařízeními.



Obrázek 4.6: Architektura BlackBerry UEM. Převzato z [17].

Pro potřeby splnění požadavků na BYOD je nutné nasadit další komponenty balíku BlackBerry Enterprise Mobile Suite na úrovni edice Collaboration Edition. Na obrázku 4.7 jsou jednotlivé komponenty rozkreslené.

Jádrem řešení je BlackBerry UEM, který dále obsahuje subkomponenty jako jsou mimo jiné logování, monitoring, reportování, funkce pro správu, služby pro autentifikaci a autorizaci, plánování a zasílání příkazů či IT politiky a profily zařízení. BlackBerry Control slouží k zasílání konfiguračních dat do aplikací BlackBerry Dynamics v koncových zařízeních. BlackBerry Collaboration Service poslouží k propojení se službou Microsoft Skype For Business.



Obrázek 4.7: Schéma komponentů balíku BlackBerry Enterprise Mobility Suite. Převzato z: [17].

BlackBerry Enterprise Mobility Server slouží k posílání dat do BlackBerry Dynamics Apps. Většina funkcí je využitelná až u vyšších edicí BlackBerry Enterprise Mobility suite.

4.7.2 Kroky instalace

V první řadě je třeba nainstalovat BlackBerry UEM. Dále je třeba nainstalovat BlackBerry Enterprise Mobility Server. V rámci tohoto severu je třeba nakonfigurovat BlackBerry Dynamics a nastavit certifikáty. Dále je třeba nastavit přístup do Active directory, SMTP server a Exchange ActiveSync. Dalším krokem je nastavení konektivity pro BlackBerry Dynamics. Po té je nutné nastavit BlackBerry Dynamics profil a zpřístupnit tak uživatelům aplikace BlackBerry Work a BlackBerry Access.

V BlackBerry dynamics je možné nastavit některé politiky. Pro účely BYOD zařízení je třeba nastavit zamezení přístupu uživatelům s operačním systémem umožnující administrátorské operace (JailBreak/Root) a nastavit interval nutný pro synchronizaci s UEM.

Posledním krokem je nastavení uživatelských účtů a skupin. Aktivace z hlediska uživatele spočívá v instalaci software BlackBerry UEM a BlackBerry Work z obchodu s aplikacemi pro daný operační systém. Další postup aktivace je triviální.

Maximální počet uživatelů na jeden server je 20 000, což znamená, že zkoumané organizaci bude stačit jediný server.

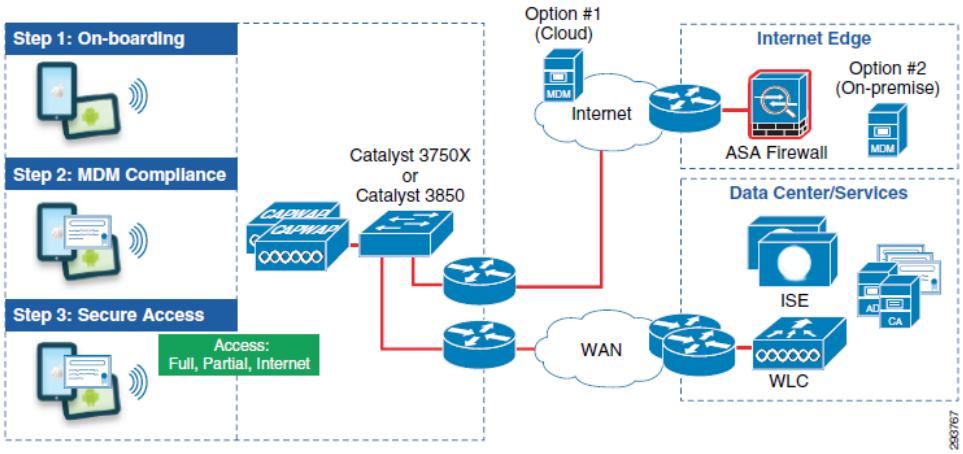
4.7.3 Integrace s Cisco ISE

BlackBerry UEM je možné integrovat s Cisco ISE, čož je NAC prvek používaný v Bance. Díky této integraci ISE může od UEM získávat data o zařízení, na základě kterých může povolit nebo zamítnout přístup zařízení do firemní sítě, viz [18].

Cisco ISE vyžaduje v UEM vlastní administrátorský profil, ten je třeba nastavit. Dále je třeba importovat do ISE BlackBerry Web Service Certificate exportovaný z UEM. V ISE je nyní možné nastavit připojení k UEM.

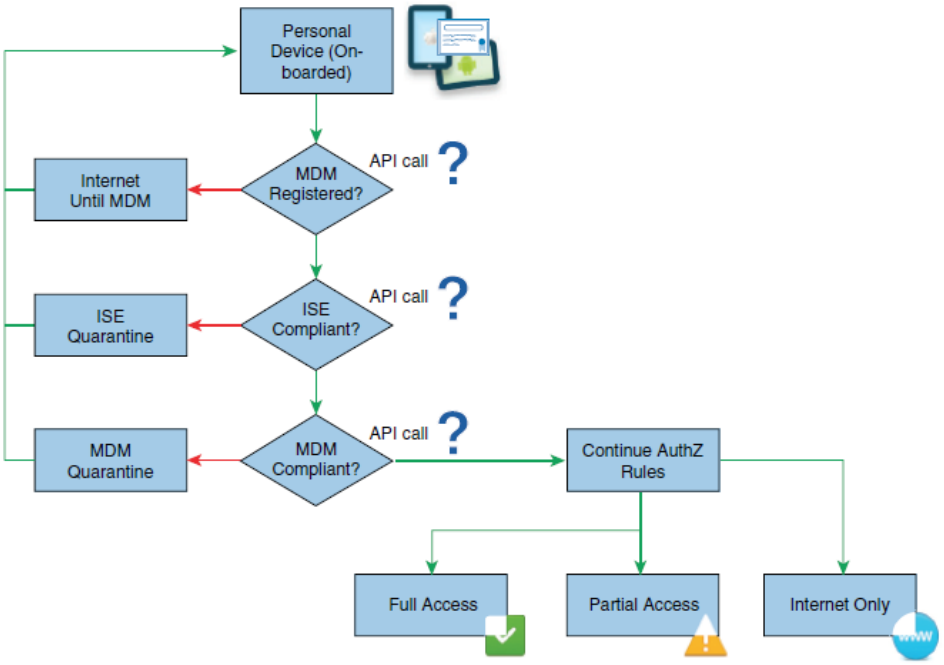
Nyní může ISE získávat data o zařízení jako je MAC adresa, splnění politik, nastavení šifrování, informace o aktivaci v UEM, detekce jailbreak, výrobce, model, sériové číslo, verze operačního systému nebo nastavení zaheslování.

Dále je díky integraci přímo z ISE možné vymazat ze zařízení pracovní data nebo jej uzamknout.



Obrázek 4.8: Ilustrace připojování uživatelů do sítě s využitím MDM. Převzato z: [18].

Obrázek 4.8 ilustruje návrh připojování uživatelů k bezdrátové síti s využitím integrace s MDM. Nejdříve se uživatel připojí k SSID pro přihlášení. Po úspěšném přihlášení se uživatel připojí k zabezpečené zaměstnanecké síti. ISE zavolá API MDM serveru a pokud není registrováno, je přesměrováno. V tomto kroku je možné přesměrovat uživatele na stránku produktu BlackBerry UEM obchodu s aplikacemi jeho operačního systému a automatizovat tak jeden z kroků pro nasazení na straně uživatele. Dále ISE získá informace od MDM serveru a do uloží jej do cache. Poté zkontroluje splnění politik. Pokud je kontrola úspěšná, zařízení jsou přiřazena patřičná práva v rámci sítě. Celý postup je vyobrazen v diagramu 4.9.



Obrázek 4.9: Diagram pro připojování zařízení do sítě. Převzato z: [18].

4.8 Síťová infrastruktura nutná k nasazení navrženého řešení pro notebooky

Navržené řešení neklade zvýšené nároky na síťovou infrastrukturu. Jelikož se jedná o distribuovanou virtualizaci, není třeba zajistit vyšší kvalitu sítě než je běžné.

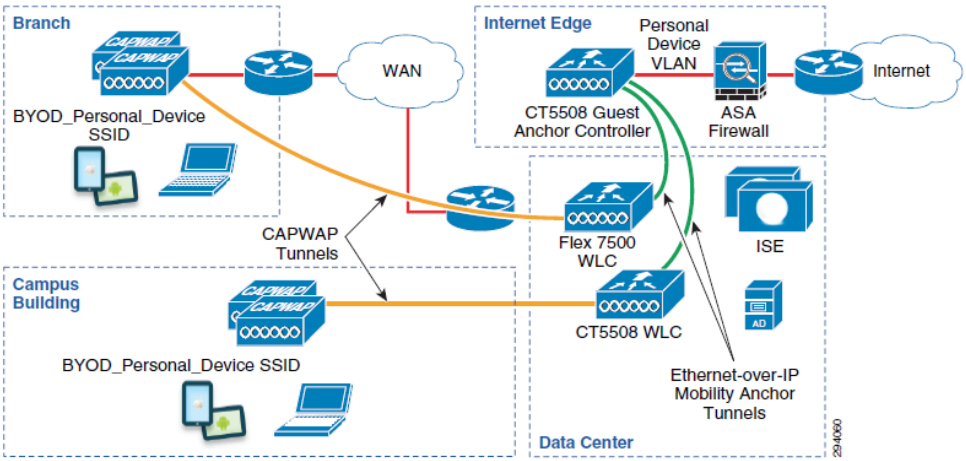
Pokud by však bylo přistoupeno k oddělení sítě pomocí SSL tunelů, pak by muselo dojít k navýšení kapacity sítě a případně nákupu i dalšího nezbytného

hardware jako jsou VPN koncentrátory, firewally, routery a podobně – ne však nezbytně.

Vzhledem k povaze BYOD notebooků se jeví jako nejlepší řešení připojení k internetu pomocí bezdrátové sítě podobného charakteru jako ta k dispozici pro hosty. Přístup do podnikové sítě pak bude zajištěn pomocí VPN. Každý obraz virtuálního stroje bude obsahovat VPN klienta Cisco AnyConnect pro kterého již Banka vlastní licence.

Cisco doporučuje [18] odlišit tuto síť od sítě pro hosty několika vylepšeními. Je vhodné umožnit zaměstnancům zajistit si svépomocí přihlašovací údaje a rozšířit možnosti autentifikace o využití Microsoft Active Directory. Taktéž je vhodné narozdíl od sítě pro hosty zajistit vyšší kvalitu služby.

Pro přihlášení k síti se využívá Cisco ISE Sponsor Portal. Po přihlášení je možné porovnat přihlašovací údaje s Active Directory. Taktéž je možné nastavit, které skupiny uživatelů mohou udělovat přístupy a monitorovat, kdo a kdy přístupy vytvořil. Je vhodné pro BYOD notebooky vytvořit vlastní zabezpečenou síť, viz obrázek 4.10.



Obrázek 4.10: Návrh SSID pro BYOD s využitím technologie Cisco Unified Wireless Network. Převzato z [18].

Oddělení IT Security však doporučuje nepoužívat bezdrátové sítě a využít stávající kabelovou síť a stávající proces připojování uživatelů s pomocí aplikace MAB Keeper. VLAN přidělená pro BYOD zařízení by poskytovala pouze připojení k internetu a skrze toto připojení by bylo s užitím VPN tunelováno připojení do vnitřní sítě.

4.9 Návrh dalších opatření

Další opatření jsou navržena dle sekce 1.3.

Z hlediska způsobilosti zaměstnanců je navrženo hodnotit způsobilost zaměstnanců pro vstup do BYOD programu. Způsobilost zaměstnance by měl zhodnotit jeho nadřízený. Je nutné určit, pro jaké případy jsou vlastní zařízení přípustná a pro jaké nikoliv. Pro zvýšení účinku programu je třeba vynutit vstup do BYOD programu u všech, kteří již nyní svá vlastní zařízení k práci používají.

Zaměstnancům využívajícím vlastní zařízení jako náhradu firemního zařízení je nutné vyplácet paušál jako náhradu a toto ošetřit v dodatku pracovní smlouvy. Toto neplatí pro kontraktory.

Není možné podporovat každé BYOD zařízení. Proto se koncept podpory musí změnit na podporu služby. Je třeba zavést uživatelské fórum, na které budou odkázáni uživatelé, kteří mají problémy se svými zařízeními, která spadají mimo rámec podpory služby. Je vhodné mít připraveno několik firemních zařízení k zapůjčení připravených jako náhradu pro účastníky BYOD programu s potížemi, avšak nezaručovat poskytnutí této služby.

Je třeba vyčlenit pracovníka IT oddělení zodpovědného za BYOD. Ten by měl spravovat návod s postupem pro začlenění zájemců do BYOD programu. Podrobnější školení není nutné.

Je třeba zavést interní směrnici, která ošetří BYOD ve firmě. Je nutné zamezit využívání soukromých zařízení k soukromým účelům v pracovní době. Po náběhu BYOD programu je možné interními předpisy umožnit vstup do BYOD nejenom kontraktorům, ale také vlastním zaměstnancům. Momentálně je toto možné pouze na základě bezpečnostní výjimky. Vstup do BYOD programu ze strany zaměstnanců by měl být dobrovolný.

Při najímání kontraktorů je třeba brát v úvahu využití konceptu distribuované virtualizace v BYOD programu, a tedy smluvně zaručit možnost provozování virtuálního stroje na pracovním zařízení najímaného pracovníka.

Proces pro schvalování bezpečnostních výjimek je třeba zachovat z důvodu neočekávaných mezních případů. Využívání výjimek by však nemělo být možné pro případy užití, které se dají řešit pomocí zapojení do BYOD programu. Zároveň je třeba zachovat smlouvu o užívání vlastního zařízení a aktualizovat ji pro potřeby BYOD programu. Bezpečnostní dotazník a zaručení nadřízeného je díky navrženému BYOD programu z procesu připojování uživatelů s neiremními zařízeními možné vypustit.

4.10 Návrh harmonogramu nasazení

Jelikož plánování projektů ve vybrané společnosti na rok 2018 je již uzavřeno, bylo by možné projekt pro nasazení BYOD programu naplánovat nejdříve na rok 2019. Pro projekt by bylo třeba najít implementačního partnera, jelikož Banka pro podobné projekty nemá vlastní volné kapacity.

První fází by byla analýza navrženého řešení napříč různými odděleními. Cílem první fáze by bylo určit konkrétní rozsah potřebných změn pro nasazení

programu. Výstupem první fáze by byl koncept s jasnými požadavky na konkrétní hardware a organizační změny. Projekt je třeba obhájit před vedením společnosti, a je potřeba připravit detailní rozpočet.

Ve druhé fázi je třeba připravit veškeré organizační změny. Připravit paragrafované znění vnitřních směrnic a dalších potřebných dokumentů. V této fázi se taktéž nastaví pravidla pro pilotní provoz.

Třetí fáze zahrnuje nákup potřebného hardware (servery, koncentrátory, firewally...) a nezbytných licencí.

Fáze čtvrtá počítá s instalací, integrací a testováním.

Pátou fází je pilotní provoz pro vybrané uživatele. Po úspěšném vyhodnocení následuje plošné nasazení.

Kapitola 5

Vyhodnocení

V této kapitole je zhodnocena uskutečnitelnost řešení a analyzovány benefity a rizika spojená se zavedením navrženého konceptu.

5.1 Sumarizace navrženého řešení

Vzhledem k povaze problému, zjištěného analýzou uvnitř společnosti, bylo navrženo zvolit rozdílná řešení podle typu zařízení.

Bylo navrženo postavit koncepci BYOD na třech základních pilířích a to:

- Technické řešení pro notebooky
- Technické řešení pro mobilní zařízení
- Nastavení dalších opatření

5.2 Uskutečnitelnost navrženého řešení

Z technického hlediska je návrh uskutečnitelný a po odladění technických detailů by z tohoto pohledu nic nebránilo jeho nasazení. Z pohledu obchodního má taktéž smysl, jelikož uskutečněním navržených opatření by se zvýšila bezpečnost informačních a komunikačních systémů zkoumané organizace, přičemž právě vnitřní bezpečnost je vzhledem k jejímu oboru podnikání důležitou součástí korporátní strategie.

5.3 Benefity řešení pro notebooky

Hlavním benefitem řešení pro BYOD notebooky za použití distribuované virtualizace jsou nízké náklady na nasazení a provoz i vysoká flexibilita. Na rozdíl od centralizované virtualizace s sebou nenese vysoké náklady na úložiště,

servery a síťovou infrastrukturu. Stírá známé problémy centralizované virtualizace jako jsou nízká odezva, vysoká citlivost na kvalitu připojení či problémy s provozováním graficky náročných aplikací.

Zároveň však odděluje pracovní prostředí od operačního systému soukromého počítače a zajišťuje tak bezpečnost firemních dat. Velkým benefitem je možnost práce offline při zachování bezpečnosti díky užití virtualizace. Řeší problém s kontraktory a nekontrolovanými zařízeními ve vlastní síti.

Co se týče obecných výhod BYOD, pokud by do programu vstoupilo významné množství zaměstnanců, dá se předpokládat snížení nákladů na IT v rovině snížení nákladů na pořizování firemních zařízení. Dále se dá předpokládat zvýšení spokojenosti u zaměstnanců, kteří by vstoupili do BYOD programu z důvodu nespokojenosti s firemním zařízením. Tyto důvody by však byly pouze vedlejším efektem, hlavním důvodem pro zavedení BYOD programu je nastavení rámce pro existující nefiremní zařízení z důvodu bezpečnosti.

5.4 Rizika nasazení navrhovaného řešení pro notebooky

Největším rizikem nasazení tohoto řešení může být neochota uživatelů přistoupit na tento model, který přináší uživateli nutnost nainstalovat si na své zařízení klientský software a pracovat s ním. U kontraktorů, kteří jsou zaměstnanci partnerských dodavatelských společností, není samozřejmostí povolení virtualizace na jejich pracovních zařízeních a je nutné tuto možnost pro vstup do BYOD programu zajistit. Dále je třeba individuálně řešit licencování nejrůznějšího softwaru, jelikož není možné v návrhu řešení BYOD programu obsáhnout všechny možné kombinace potřebného software a licenčních politik. Z hlediska bezpečnosti řešení odstraňuje aktuální bezpečnostní hrozby spojené s připojováním nefiremních zařízení. Bezpečnost se tak v tomto ohledu zvyšuje a nebyly identifikovány žádné přidané bezpečnostní hrozby.

5.5 Benefity navrhovaného řešení pro mobilní telefony a tablety

Hlavní benefit navrženého řešení pro BYOD mobilní telefony a tablety je vůbec možnost využití konceptu BYOD a tím pádem možnost pracovat kdekoliv. To má potenciál zvýšení produktivity a spokojenosti zaměstnanců. Díky zvoleným licencím a typu nasazení uživatele nijak neomezuje v užívání jejich zařízení a nabízí tak vybalancování pracovního a soukromého života. Důvodem k navržení zavedení konkrétního produktu bylo vysoké zaměření na bezpečnost, které je v bankovním prostředí nejvyšší prioritou.

5.6 Rizika nasazení navrhovaného řešení pro mobilní telefony a tablety

Rizikem může být nedůvěra zaměstnanců k firemnímu softwaru, se schopností kontrolovat jejich soukromé zařízení. Reálný provoz také může ukázat u BYOD zařízení snížení výkonu či snížení výdrže na baterii v určitých konfiguracích. To by znamenalo negativní postoj zaměstnanců k BYOD programu a jeho možný neúspěch.

5.7 Další dopady realizace projektu

Procesní změny nutné k zavedení navrhovaného BYOD programu nejsou nikterak závažné a proto nejsou překážkou k realizaci projektu. Díky nastolení programu pro BYOD je možné nabídnout BYOD některým zaměstnancům a považovat to za pracovní benefit.

Závěr

Cílem této práce bylo navrhnout využití konceptu BYOD ve vybrané bankovní organizaci, a to především s ohledem na jeho zabezpečení. Všechny body zadání byly splněny.

S přihlédnutím k aktuálním trendům v ICT byly definovány klíčové faktory ve využívání nefiremních zařízení. Je zřejmé, že v dnešní době má velká část populace k dispozici svá soukromá zařízení a vzhledem ke zvýšení osobního komfortu a efektivity by někteří zaměstnanci tato zařízení rádi využívali také k pracovním účelům. Dalším častým důvodem zavádění BYOD ve firmách bývá snaha o snížení nákladů na ICT. S příchodem nefiremních zařízení do firemních sítí se ale pojí rizika jakými jsou například snadnější úniky dat, bezpečnostní incidenty nebo komplikovanější správa ICT.

Ve vybrané organizaci byly formou četných konzultací analyzovány požadavky na BYOD. Z hlediska mobilních telefonů a tabletů je požadován především přístup k emailu a kalendáři, případně k dokumentům. V případě notebooků se požadavky liší podle typů uživatele, jedná se o potřeby jako přístup k interním systémům a prostředím, přístup k dokumentům či možnost instalace vlastních aplikací. Požadavkem Banky je zajistit co nejvyšší bezpečnost s co možná nejnižšími náklady.

Nevyhnutelné je využívání nefiremních zařízení pracovníky, kteří nejsou zaměstnanci Banky, ale pracují pro ni na živnostenský list nebo zprostředkovaně. Tato zařízení jsou připojována na základě bezpečnostních výjimek. Jelikož tato zařízení nejsou zkoumanou společností spravována, vyplývá ze stávající praxe bezpečnostní riziko. Existující procesy a hrozby byly analyzovány a jako nejnaléhavější potencionální hrozby byly vyhodnoceny následující: možné porušení bezpečnostních politik, možné zavedení škodlivého software do firemního prostředí či odcizení nebo poškození aktiv společnosti.

Předmětem analýzy byly také různé přístupy k řešení BYOD. Bylo zjištěno, že dostupná řešení je vhodné rozdělit na řešení pro notebooky a na řešení pro chytré telefony a tablety. S použitím studií od renomovaných analytických společností byli vyhodnoceni nejvýznamnější dodavatelé softwaru.

Na základě potřeb vybrané společnosti byla jako řešení pro notebooky zvolena virtualizace, a to specificky centralizovaná. Produktem, který nejlépe splňoval požadavky, se ukázal být Horizon Flex od společnosti VMware. Díky využití tohoto produktu je možné oddělit pracovní a soukromý operační systém. Pracovní operační systém lze plně spravovat a vynutit tak bezpečnostní politiky. Díky tomu jsou potlačeny nejzávažnější hrozby plynoucí ze stávajícího způsobu připojování.

Jako řešení pro mobilní telefony byl navržen Enterprise Mobility Suite od firmy BlackBerry, neboť splňuje požadavky uživatelů tím, že jim umožňuje přístup do firemního emailu, kalendáře a dalších potřebných služeb, zároveň odděluje pracovní a soukromá data a je hodnocen jako nebezpečnější řešení na trhu. Nezávisle na této práci byl během jejího dokončování započat projekt plošného nasazování řešení od BlackBerry do zkoumané organizace. Taktéž byla navržena další opatření nutná pro vznik uceleného BYOD programu.

Navrhované řešení bylo po celou dobu zpracování konzultováno se zástupci vybrané organizace. Bylo ohodnoceno jako vhodné a řešící stávající problémy v oblasti BYOD. V návaznosti na návrh byla stanovena doporučení pro nasazení zvolených produktů.

Díky zmiňovanému řešení by se zvýšila bezpečnost BYOD ve zkoumané organizaci. Tato práce bude jedním ze vstupů pro budoucí projekt pro řešení BYOD ve společnosti.

Literatura

[1] Consumer Barometer [online]. April 2015, [Cit. 01-03-2017]. Dostupné z: https://www.consumerbarometer.com/en/about/

[2] BYOD - Prozkoumat - Trendy Google [online]. [Cit. 01-03-2017]. Dostupné z: https://trends.google.com/trends/explore?q=BYOD

[3] BYOD po česku – pouze 7 % firem vítá využití soukromých počítačů zaměstnanců [online]. September 2016, [Cit. 20-03-2017]. Dostupné z: http://ictrevue.ihned.cz/c3-65456950-0ICT00_d-65456950-byod-po-cesku-pouze-v-7-firem-vita-vyuziti-soukromych-pocitacu-zamestnancu

[4] 2016 State of the Endpoint Report [online]. April 2016, [Cit. 20-03-2017]. Dostupné z: http://www.countertack.com/2016-state-of-the-endpoint-report

[5] Mobile & tablet operating system market share in Czech Republic | StatCounter Global Stats [online]. June 2016, [Cit. 01-03-2017]. Dostupné z: http://gs.statcounter.com/os-market-share/mobile-tablet/czech-republic/

[6] Operating system market share Worldwide | StatCounter Global Stats [online]. [Cit.01-03-2017]. Dostupné z: http://gs.statcounter.com/os-market-share/

[7] Shackleford, D.: *Virtualization Security: Protecting Virtualized Environments*. Sybex, první vydání, 11 2012, ISBN 9781118288122.

[8] Technology brief... [online]. April 2016, [Cit. 20-04-2017]. Dostupné z: http://jgoldassociates.com/Technology_Brief/Technology_Brief_April_2016.pdf

[9] Crook, S. K.: Worldwide Enterprise Mobility Management Software Market Shares, 2014: Fragmentation Continues, But the Dust Is Starting to Settle [online]. June 2015, [Cit. 07-02-2017]. Dostupné z: http://www.air-watch.com/resources/analyst-reports/idc-worldwide-enterprise-mobility-management-software-market-shares-2014/download/

[10] Hochmuth, P.: Worldwide Enterprise Mobility Management Software Market Shares, 2015: Consolidation of Vendors and Market Share Changes the Landscape [online]. May 2016, [Cit. 07-02-2017]. Dostupné z: http://www.air-watch.com/downloads/resources/US40430516e_VMware.pdf

[11] Smith, R.; Taylor, B.; Silva, C.; aj.: Magic Quadrant for Enterprise Mobility Management Suites [online]. June 2016, [Cit. 26-02-2017]. Dostupné z: https://www.gartner.com/doc/reprints?id=1-390IMNG&ct=160608&st=sb

[12] Johnson, D. K.: The Forrester Wave: Server-Hosted Virtual Desktops (VDI), Q3 2015 [online]. 2015, [Cit. 20-01-2017]. Dostupné z: http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/view/vmware-horizon-vs-microsoft-quick-look.pdf

[13] Young, R.; Laing, D.: IDC MarketScape: Worldwide Virtual Client Computing Software 2016 Vendor Assessment [online]. November 2016, [Cit. 20-02-2017]. Dostupné z: http://campaign.vmware.com/imgs/GlobalCampaigns/39249/IDC_MarketScape_Worldwide_Virtual_Client_Computing_Software_2016_Vendor_Assessment.pdf

[14] Morris, A.: *VMware Horizon FLEX Solution Brief [online]*. VMware, [Cit. 01-02-2017]. Dostupné z: http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-horizon-flex-solution-brief-mirage-fusion-player.pdf

[15] Girard, J.; Zumerle, D.; Smith, R.: Critical Capabilities for High-Security Mobility Management [online]. August 2016, [Cit. 20-04-2017]. Dostupné z: https://www.gartner.com/doc/reprints?id=1-3GSO3TQ&ct=160902&st=sb

[16] Coltoff, P. D.; De Nike, K.; White, C.; aj.: *VMware Horizon FLEX Deployment Considerations [online]*. VMware, [cit. 01-05-2017]. Dostupné z: http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-horizon-flex-deployment-considerations.pdf

[17] BlackBerry: *BlackBerry UEM - 12.6 [online]*. [cit. 10-05-2017]. Dostupné z: http://help.blackberry.com/en/blackberry-uem/current/

[18] Hallock, Z.; Johnston, J.; Macias, F.; aj.: *Cisco Unified Access (UA) and Bring Your Own Device (BYOD) CVD [online]*. Cisco Systems, August 2014, [cit. 01-02-2017]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.html

[19] Báčová, P.: Chytré telefony zvyšují počet uživatelů internetu [online]. May 2016, [Cit. 01-03-2017]. Dostupné z: https://www.czso.cz/csu/czso/chytre-telefony-zvysuji-pocet-uzivatelu-internetu

[20] BYOD - definition of BYOD in English | Oxford Dictionaries [online]. [Cit. 05-03-2017]. Dostupné z: https://en.oxforddictionaries.com/definition/BYOD

[21] BYOD Meaning in the Cambridge English Dictionary [online]. [Cit. 05-03-2017]. Dostupné z: http://dictionary.cambridge.org/dictionary/english/byod

[22] BYOD – Bring Your Own Device – Free Gartner Research [online]. [Cit. 05-03-2017]. Dostupné z: http://www.gartner.com/it-glossary/bring-your-own-device-byod

[23] Thomas Struthers, P. L.: Understanding the BYOD landscape [online]. 2013, [Cit. 01-02-2017]. Dostupné z: https://www2.deloitte.com/uk/en/pages/technology-media-and-telecommunications/articles/understanding-the-bring-your-own-device-landscape.html

[24] Stagliano, T.; DiPoalo, A.; Coonnelly, P.: The Consumerization of Information Technology. *Graduate Annual*, ročník 1, č. 1, 2013: str. 10.

[25] Houser, P.: BYOD přináší firmám vyšší produktivitu i bezpečnostní rizika [online]. April 2016, [Cit. 20-03-2017]. Dostupné z: http://archiv.ihned.cz/c1-65235190-byod-prinasi-firmam-vyssi-produktivitu-i-bezpecnostni-rizika

[26] Koch, H.; Zhang, S.; Giddens, L.; aj.: Consumerization and IT Department Conflict. In *Thirty Fifth International Conference on Information Systems*, Auckland, 2014.

[27] Diblík, J.; Zahradníček, P.: Právní aspekty BYOD (Bring Your Own Device) a jeho praktická využitelnost v českých společnostech [online]. January 2017, [Cit. 01-04-2017]. Dostupné z: http://www.pravniprostor.cz/clanky/pracovni-pravo/pravni-aspekty-byod-bring-your-own-device-a-jeho-prakticka-vyuzitelnost-v-ceskych-spolecnostech

[28] Marc, P.: Rady jak vyzrát na home office. Chystaná regulace víří největší emoce [online]. April 2017, [Cit. 20-04-2017]. Dostupné z: http://www.e15.cz/finexpert/vydelavame/rady-jak-vyzrat-na-home-office-chystana-regulace-viri-nejvetsi-emoce-1330808

[29] AleFIT MAB Keeper a AleFIT Office Locator [online]. October 2016, [Cit. 01-02-2017]. Dostupné z: https://www.alef.com/alefnula/alefit-mab-keeper-a-alefit-office-locator.c-269.html

[30] Claudio Neiva, L. O.: Market Guide for Network Access Control [online]. March 2016, [Cit. 02-03-2017]. Dostupné z: https://www.gartner.com/doc/reprints?id=1-3I8W2V2&ct=160922&st=sb

[31] Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). January 2015, [Cit. 01-05-2017]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-316/zneni-20150101

[32] Křížný prodej (Cross-selling) [online]. December 2016, [Cit. 01-03-2017]. Dostupné z: https://managementmania.com/cs/krizovy-prodej-cross-selling

[33] Mac* vs. PC Debate [online]. June 2016, [Cit. 01-03-2017]. Dostupné z: http://www.intel.com/content/www/us/en/tech-tips-and-tricks/pc-vs-mac-the-big-debate.html

[34] Schön, O.: Android předběhne Windows jako nejpoužívanější systém na webu, v Česku mu brání drahá data [online]. March 2017, [Cit. 20-04-2017]. Dostupné z: http://tech.ihned.cz/internet/c1-65653000-android-predbehne-windows-jako-nejpouzivanejsi-system-na-webu-v-cesku-mu-brani-draha-data

[35] macOS – What is macOS [online]. [Cit. 01-03-2017]. Dostupné z: https://www.apple.com/macos/what-is/

[36] Smartphone - Gartner IT Glossary [online]. [Cit. 01-03-2017]. Dostupné z: http://www.gartner.com/it-glossary/smartphone/

[37] Nokia malware report shows smartphones now account for 60% of infections in the mobile network [online]. March 2016, [Cit. 20-04-2017]. Dostupné z: http://www.nokia.com/en_int/news/releases/2016/03/01/nokia-malware-report-shows-smartphones-now-account-for-60-of-infections-in-the-mobile-network

[38] Nokia Threat Intelligence Report – H2 2015 [online]. March 2016, [Cit. 20-04-2017]. Dostupné z: http://resources.alcatel-lucent.com/asset/193174

[39] Ethernet Definition from PC Magazine Encyclopedia [online]. [Cit. 01-03-2017]. Dostupné z: http://www.pcmag.com/encyclopedia/term/42781/ethernet

[40] Wi-Fi Definition from PC Magazine Encyclopedia [online]. [Cit. 01-03-2017]. Dostupné z: http://www.pcmag.com/encyclopedia/term/54444/wi-fi

[41] Paul Ferguson, Geoff Huston: What Is a VPN? – Part I. *The Internet Protocol Journal*, ročník 1, č. 1, 1998.

[42] Mobile device management [online]. February 2012, [Cit. 07-03-2017]. Dostupné z: http://www.systemonline.cz/sprava-it/mobile-device-management.htm

[43] Keen, M.: Nokia malware report shows smartphones now account for 60% of infections in the mobile network [online]. January 2013, [Cit. 07-03-2017]. Dostupné z: https://www.ibm.com/developerworks/community/blogs/mobileblog/entry/got_mam_mobile_application_management_in_your_2013_mobile_menu25?lang=en

[44] Valerio, P.: AirWatch Consolidates EMM Leadership in Latest IDC Report [online]. June 2016, [Cit. 07-02-2017]. Dostupné z: https://theictscoop.com/airwatch-consolidates-emm-leadership-in-latest-idc-report-6622602febde

[45] Guide To VDI: Evaluating Top Vendors [online]. [Cit. 20-01-2017]. Dostupné z: http://byod.cioreview.com/vendors/most-promising-byod-solution-providers-2016.html

[46] Cheng, L.; Sliwinski, H.: VMware Completes Acquisition of AirWatch [online]. February 2014, [Cit. 20-05-2017]. Dostupné z: http://ir.vmware.com/overview/press-releases/press-release-details/2014/VMware-Completes-Acquisition-of-AirWatch/default.aspx

[47] BlackBerry Completes WatchDox Acquisition [online]. May 2015, [Cit. 20-05-2017]. Dostupné z: https://global.blackberry.com/en/company/newsroom/press?id=1946553

[48] BlackBerry Completes WatchDox Acquisition [online]. November 2015, [Cit. 20-05-2017]. Dostupné z: https://global.blackberry.com/en/company/newsroom/press?id=1998017

[49] Cisco Completes Acquisition of Meraki [online]. December 2012, [Cit. 20-05-2017]. Dostupné z: https://newsroom.cisco.com/press-release-content?articleId=1118649

[50] Historic Dell and EMC Merger Complete; Forms World's Largest Privately-Controlled Tech Company [online]. September 2016, [Cit. 20-05-2017]. Dostupné z: https://www.emc.com/about/news/press/2016/20160907-01.htm

[51] Berry, R.: Citrix XenDesktop/XenApp: What is HDX? It's not just ICA! [online]. 2014, [Cit. 20-04-2017]. Dostupné z: https://www.citrix.com/blogs/2014/08/18/citrix-xendesktopxenapp-what-is-hdx-its-not-just-ica/

[52] Why choose Citrix over VMware infographic [online]. 2016, [Cit. 09-02-2017]. Dostupné z: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/why-choose-citrix-over-vmware-infographic.pdf

[53] Three areas where Citrix XenApp and XenDesktop outperform VMware Horizon [online]. 2016, [Cit. 09-02-2017]. Dostupné z: https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/three-areas-where-citrix-xenapp-and-xendesktop-outperform-vmware-horizon.pdf

[54] Federal Information Processing Standards (FIPS) [online]. [Cit. 10-05-2017]. Dostupné z: http://www.vmware.com/security/certifications/fips.html

[55] Produkty společnosti VMware [online]. [Cit. 09-02-2017]. Dostupné z: http://www.vmware.com/cz/products.html

[56] Why VMware Horizon Is Better Than Citrix XenDesktop [online]. [Cit. 09-02-2017]. Dostupné z: http://digital.leadmagz.com/ingrammicro/VMware/VMware_Why_Horizon_over_Citrix_Whitepaper.pdf

[57] VMware Horizon 7, Horizon Air, and Horizon FLEX advantages over Microsoft RDS and Azure RemoteApp [online]. September 2016, [Cit. 09-02-2017]. Dostupné z: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/forrester-wave-server-hosted-virtual-desktops-q3-2015.pdf

[58] Oracle VM VirtualBox 5.0 Overview [online]. March 2016, [Cit. 09-02-2017]. Dostupné z: http://www.oracle.com/us/technologies/virtualization/oracle-vm-virtualbox-overview-2981353.pdf

[59] Francis, D.: Guide To VDI: Evaluating Top Vendors [online]. February 2015, [Cit. 20-01-2017]. Dostupné z: http://www.networkcomputing.com/storage/guide-vdi-evaluating-top-vendors/1908233543/page/0/1

[60] Lockwood, M.: Is VMware's Horizon FLEX the answer to BYOD? [online]. October 2014, [Cit. 20-01-2017]. Dostupné z: http://blogs.gartner.com/mark-lockwood/2014/10/14/is-vmwares-horizon-flex-the-answer-to-byod/

[61] GFE Comparison - Canada [online]. [Cit. 20-04-2017]. Dostupné z: https://ca.blackberry.com/enterprise/gfe-comparison

[62] BlackBerry: *BlackBerry Enterprise Mobility Suite [online]*. [cit. 10-05-2017]. Dostupné z: https://global.blackberry.com/content/dam/blackberry-com/PDF/enterprise/ds-blackberry-enterprise-mobility-suite.pdf

[63] BlackBerry: *Determining what licenses you need - BlackBerry UEM – 12.6 [online]*. [cit. 10-05-2017]. Dostupné z: http://help.blackberry.com/en/blackberry-uem/12.6/licensing/dhd1465315353877.html

Příloha **A**

Seznam použitých zkratek

BYOD Bring your own device – Nefiremní zařízení používané k práci

IT Informační technologie

AMA Advanced Measurement Approach – Způsob řízení rizik

MAC adresa Media Access Control adresa – Jednoznačný identifikátor síťového zařízení

WiFi Standard pro bezdrátové sítě

MAB MAC Authentication Bypass – Způsob autentifikace obcházející 802.1x

VLAN Virtual Local Area Network – Virtuální lokální síť

ACL Access Control List – Sada oprávnění v rámci sítě

ISE Identity Service Engine – NAC nástroj od společnosti Cisco

RADIUS Remote Authentication Dial-In User Service – Protokol pro síťtovou autentifikaci

VPN Virtual Private Network – Způsob přiojování k soukromé síti skrze síť veřejnou

PIM Personal Information Management – Software pro správu osobních informací a organizaci času

DaaS Desktop as a Service – Desktop jako služba

EMM Enterprise Mobile Management – Balík software pro správu mobilních zaízení

MDM Mobile Device Management – Software pro správu mobilního zařízení

MAM Mobile Application Management – Software pro správu podnikových aplikacích pro mobilní zařízení

MCM Mobile Content Management – Software pro správu na mobilních zařízeních

IAM Identity and Access Management – Software pro správu identit

EFSS Enterprise File Synchronization and Sharing – Software pro sdílení souborů

VCC Virtual Client Computing – Klientský software pro virtualizaci

VDI Virtual Desktop Infrastructure – Technologie pro virtualizaci desktopů

VM Virtual Machine – Virtuální stroj

IIS Internet Information Services – Webový server od společnosti Microsoft

API Application programming interface – Aplikační rozhraní

SSL Secure Sockets Layer – Protokol pro zabezpečení komunikace po síti

Příloha **B**

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF

Příloha C

HW požadavky VMware Horizon FLEX

C.1 Horizon FLEX Server

- Minimum CPU: 1 Quad-Core Processor or 2 vCPUs
- 2.26GHz Intel core speed or equivalent
- Minimum 512MB /Recommended 4GB
- Disk: 10GB+ /Recommended 40GB+
- Windows 2008 R2, Windows 2012 and above
- .NET 3.5 SP1 and above
- IIS 7.0+ with II6 Management Compatibility and ASP.Net

C.2 VMware Mirage Server

- Minimum 4 vCPU, Recommended 8 vCPU
- Minimum 8GB RAM, Recommended 16GB
- 146GB Free Disk Space
- Windows 2008 R2, Windows 2012 and above
- .NET 3.5 SP1 and above
- IIS 7.0+ with II6 Management Compatibility and ASP.Net