Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra informačních technologií

Studijní program : Aplikovaná informatika

Obor: Informační systémy a technologie

Zavedení BYOD pro notebooky v Telefónica Czech Republic

DIPLOMOVÁ PRÁCE

Student : Bc. David Pokorný

Vedoucí : Ing. Tomáš Bruckner, Ph.D.

Oponent : Ing. Dušan Chlapek, Ph.D.

2014

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze které jsem čerpal.

V Praze dne 6. května 2014 . . . . . .

Bc. David Pokorný

Poděkování

V první řadě chci poděkovat kolegům ze společnosti Telefónica Czech Republic za námět k diplomové práci, poskytnutí podkladů a odborné konzultace, které přispěly ke zvýšení kvality. Zejména chci poděkovat garantovi, panu Janu Černému.

Dále děkuji vedoucímu práce, Ing. Tomáši Brucknerovi, Ph.D., za cenné rady a vstřícný přístup a všem, kteří mě při psaní práce podporovali.

Abstrakt

Práce se zabývá zaváděním programu Bring Your Own Device pro soukromé notebooky zaměstnanců ve společnosti Telefonica Czech Republic. Popisuje způsob řešení pomocí distribuované virtualizace. Na soukromé notebooky je distribuován virtuální firemní počítač se stejným pracovním prostředím, jako mají standardní pracovní stanice společnosti. Řešení problému je zasazeno do reálného prostředí společnosti. Analyzované oblasti pro zavedení a provoz programu BYOD jsou bezpečnostní, technologická, finanční a procesní.

Klíčová slova

BYOD, distribuovaná virtualizace, VMware Player, IT BSC, náklady na virtualizaci, analýza rizik VM, návrh VM, testování VM, procesy BYOD, pravidla BYOD

Abstract

This thesis deals with the implementation of the Bring Your Own Device program for employee's private laptops at Telefonica Czech Republic. It describes the solution using a distributed virtualization. The private laptops are given identical system environments as standard corporate laptops. The solution of the problem is set in the environment of the real corporation. Areas focused on the establishment and operation of the program are security, technology, finance and processes.

Keywords

BYOD, distributed virtualization, VMware Player, IT BSC, virtualization costs, VM risk analysis, VM design, VM testing, BYOD processes, BYOD policy

Obsah

1 Úvod

Bring Your Own Device, česky "přineste si své zařízení", je zavedené pojmenování fenoménu, který se v posledních letech objevil v organizacích po celém světě. Jedná se o používání soukromého zařízení pro pracovní účely. Přináší s sebou řadu výhod, ale i problémů.

Soukromá zařízení se v organizacích postupně objevují řadu let. Ať se jedná o PDA nebo notebooky. Od roku 2011 se začal tento fenomén dynamicky rozrůstat a stal se předmětem řady průzkumů a projektů.

BYOD zastřešuje řadu druhů zařízení. Od chytrých telefonů, přes tablety a netbooky až k notebookům i desktopům "přineseným" do interních sítí společností anebo k nim připojeným prostřednictvím vzdáleného přístupu. Rozvoj BYOD pro chytré telefony je dle (Keyes, 2013) spojován s příchodem Apple iPhone. Apple je jednou ze společností, které táhly rozvoj BYOD kupředu, i díky tabletům Apple iPad, které řada uživatelů používá jako doplněk k desktopům nebo notebookům. Do BYOD oblasti nyní zasahují i výrobci zařízení na platformě Android a výrobci ultrabooků jako je například Intel, který spojuje mobilní technologie s bezpečnostními prvky.

V současnosti je možné se setkat s řadou pohledů na BYOD. Ve světě převládá názor, že BYOD je trend, pro který je přínosné vytvořit pravidla a zahrnout do podnikové strategie IT. Zpřístupňování aplikací uživatelům BYOD probíhá různými způsoby - od úplné transformace do cloudu přes vybudování webového rozhraní, po vývoj specializovaných aplikací pro mobilní platformy. Další z rozšířených možností je vybudování virtuální infrastruktury desktopů uživatelům BYOD. Nejčastěji jsou virtuální desktopy poskytovány na virtualizačním serveru. Možností, jak virtuální desktopy rozšířit mezi uživatele, bez nutnosti budovat infrastrukturu pro virtuální desktopy poskytované na serveru je distribuce virtuálních desktopů přímo do koncových zařízení. O tomto řešení je v současnosti k dispozici velmi málo zdrojů a právě proto se mu tato práce věnuje.

Mezi hlavní výhody BYOD patří zvýšení mobility a flexibility zaměstnanců, které jde ruku v ruce s vyšší produktivitou práce. Díky BYOD mohou uživatelé používat svá oblíbená zařízení, čímž roste i jejich spokojenost.

BYOD se potýká s několika hlavními problémy. Tím prvním a nejčastějším je obava o zachování úrovně bezpečnosti. Druhým problémem je pak fakt, že BYOD přináší více nefinančních přínosů než finančních. Tím je projekt zavedení BYOD náročnější na obhajobu u společností, které se zaměřují na finanční měřítka.

1.1 Cíl práce

Hlavním cílem práce je navrhnout řešení pro zavedení programu BYOD pro notebooky do společnosti Telefónica Czech Republic. Toto řešení využívá distribuce virtuálních strojů pomocí VMware Player/Fusion na soukromé notebooky uživatelů.

Navržené řešení slouží jako příprava pro vytvoření projektového plánu a pro realizaci projektu. Řešení odráží situaci ve společnosti Telefónica Czech Republic, přibližuje přínosy a náklady projektu a připravuje rámcově hlavní procesy a pravidla. Výsledkem práce je otestované modelové řešení distribuce virtuálních počítačů, které pomůže ověřit proveditelnost návrhu.

Vzhledem k velikosti společnosti Telefónica Czech Republic i šíři projektu není cílem popsat podrobně všechny oblasti implementace programu, ale poskytnout pro ni východiska, ze kterých mohou vycházet konkrétní specialisté - např. z oddělení IT provozu, právního, lidských zdrojů, nebo bezpečnosti. Na základě tohoto rámce specialisté rozpracují svoji oblast projektu BYOD pro notebooky.

Seznam cílů:

1. Zpracovat teoretická východiska práce na základě dostupných zdrojů.
2. Charakterizovat prostředí ve společnosti ve vztahu k projektu.
3. Vytvořit rámec pro projekt BYOD pro notebooky.
4. Identifikovat a charakterizovat důvody k realizaci projektu (především finanční, bezpečnostní a zaměstnanecké).
5. Vytvořit a otestovat model technického řešení BYOD pro notebooky.

1.2 Role autora v projektu BYOD pro notebooky

V době vzniku této práce jsem zaměstnancem společnosti Telefónica Czech Republic na pozici stážisty v oddělení informační bezpečnosti.

Zaujal mě koncept projektu BYOD pro notebooky, který připravil kolega z oddělení. Navrhuje distribuovat virtuální prostředí na BYOD notebooky pomocí programu VMware Player. Tomuto konceptu jsem se rozhodl věnovat pozornost a přidal jsem se k týmu, který projekt připravuje. Vzhledem k tomu, že k použití distribuované virtualizace jsem nenašel v souvislosti s BYOD žádné prameny, rozhodl jsem se, že o tomto technickém řešení napíši diplomovou práci. Oproti jiným metodám, jak zpřístupnit pracovní prostředí na BYOD zařízeních, přináší tato levné a jednoduché řešení, které plně nahradí služební notebook.

Od vzniku konceptu jsem se s kolegy zúčastnil řady projektových schůzek i týmových sezení, na nichž jsme jak já, tak kolegové přicházeli s novými nápady a postupně je formovali. Významnou oporou při vstupu do problematiky mi byl garant diplomové práce Jan Černý.

Mojí samostatnou prací jsou kapitoly *1 Úvod*, *2.4 Analýza bezpečnostních rizik*, *2.5 Průzkum mezi zaměstnanci*, *2.6 IT BSC pro projekt BYOD* a *2.7 Náklady*.

Práci týmu jsem prezentoval v kapitolách *2.1 Aktuální stav používání soukromých zařízení*, *2.2 Projekt BYOD pro notebooky* a *2.3 Související projekty*.

V kapitolách *3 Návrh BYOD pro notebooky* a *4 Návrh VM* jsem vycházel z úvah kolegů a přidal i vlastní myšlenky a vše dohromady systematicky shrnul.

1.3 Trendy v BYOD

Jak bylo popsáno v úvodu, BYOD je fenoménem, který se objevuje již několik let. Do popředí se dostává postupně od roku 2011 a v současnosti je častým tématem na ICT konferencích. Tato podkapitola naplňuje cíl práce - *1. Zpracovat teoretická východiska práce na základě dostupných zdrojů* - rozborem aktuální literatury, článků a průzkumů z celého světa.

Některé světové společnosti, např. Intel (Shah, 2013) již na model BYOD postupně přecházejí. Podle průzkumu Gartner (Gartner, 2013) z roku 2012 dokonce 38 % z dotázaných CIO chtělo přejít na tzv. BYOD-only model, tedy že by všechna koncová zařízení bylo možné charakterizovat jako BYOD. V této kapitole jsou identifikovány přínosy BYOD, jeho specifika a problémy na základě zkušeností z praxe - pomocí vyhodnocení průzkumů ve firmách a rozborem aktuálních článků o BYOD.

1.3.1 Světové statistiky

Od roku 2011 zachycují přední světové firmy vývoj v oblasti BYOD a snaží se na něj reagovat. V následujících podkapitolách jsou využity průzkumy poradenských společností CompTIA a Forrester Consulting a technologické společnosti Citrix Systems. Průzkumy jsou doplněny o aktuální poznatky z oblasti BYOD publikované v IT literatuře a články významnějších IT periodik. Je třeba dodat, že se nejedná o vědecké výzkumy a metodika měření nebyla dostatečně prezentována. Přesto poskytují rozhled po fenoménu BYOD ve světě a pomáhají určit, na které otázky BYOD je vhodné se v práci dále zaměřit.

Citrix 2011: IT Organizations Embrace Bring-Your-Own Devices, (Citrix, 2011). Společnost Citrix Systems vydala v roce 2011 průzkum, který provedla mezi svými

zákazníky po celém světě. Reagovala tím na rostoucí trend počtu soukromých zařízení používaných ve firmách.

Společnost Citrix vyvíjí a dodává řešení centralizované virtualizace pracovních stanic na serverech (pomocí VDI[1]). Z toho důvodu mohou být její průzkumy zkreslené ve prospěch firmy. Přesto průzkum obsahuje celkový pohled na BYOD a je možné z něj odhadnout světové trendy z roku 2011.

Forrester Consulting 2012: Key Strategies To Capture And Measure The Value Of Consumerization Of IT, (Forrester, 2012). Společnost Trend Micro, která se zabývá vývojem bezpečnostního software, si v roce 2012 nechala zpracovat šetření z oblasti BYOD od poradenské společnosti Forrester Consulting. Průzkum se zaměřil na firmy z USA a Evropy. Jeho cílem bylo určit hlavní faktory, které táhnou BYOD kupředu, určit metriky, které firmy používají pro měření dopadů BYOD a určit výzvy spojené s tímto programem. Průzkum byl založen jak na online dotazníku, tak i hlubších pětačtyřiceti minutových interview s osobami odpovědnými za BYOD program ve firmách.

CompTIA 2013: In Enterprise Mobility, BYOD is Just the Beginning, (Robinson, 2013). Nezisková organizace CompTIA provedla v roce 2013 průzkum mezi 502 firmami z USA. Průzkum se zaměřuje na problematiku BYOD z globálního pohledu. Zabývá se jak technickým řešením BYOD, tak i důvody k zavedení programu.

Citrix 2013: Citrix Systems Mobility Report: A Look Ahead, (Citrix, 2013). Společnost Citrix přinesla report trendů v oblasti BYOD za rok 2013 a predikci vývoje BYOD v roce 2014. Report je založen na průzkumu mezi 733 zákazníky společnosti napříč celým světem. Respondenty jsou zejména IT administrátoři a IT manažeři z firem různých velikostí i průmyslových odvětví.

Počet firem s BYOD programem

Podle statistiky (Citrix, 2011), kterou vypracovala společnost Citrix Systems, Inc. v roce 2011 na základě celosvětového průzkumu, byl počet zaměstnanců, kteří používali soukromá zařízení pro pracovní účely 28 %. Toto číslo nabíralo vzrůstající trend. V roce 2011 se dle průzkumu firmy rozhodovaly, jak se k tomuto rozrůstajícímu se fenoménu mají postavit. Firmy do roku 2011 zaujímaly postoj mezi popíráním existence fenoménu BYOD a zakazováním používání BYOD zařízení. V roce 2011 zaujímalo jasně daný postoj k BYOD zařízením pouze 44 % respondentů. 94 % respondentů ale mělo v plánu zavedení oficiálních pravidel pro BYOD do poloviny roku 2013.

Z pohledu počtu BYOD zařízení v roce 2011 byly podle (Citrix, 2011) v popředí indické firmy s téměř 34 % zaměstnanci pracujícími na soukromých zařízeních. Oproti tomu nejméně používali soukromá zařízení zaměstnanci ve Velké Británii.

---

[1] VDI = Virtual Desktop Infrastructure, infrastruktura pro virtuální desktopy

V oblasti zavedení BYOD programu do firemního prostředí mají nejčastěji program zaveden firmy z USA (56 %). Proti tomu nejméně často firmy ve Velké Británii, kde je podíl 37 % firem. Celosvětový průměr je 44 %.

Podle výzkumu CompTIA (Robinson, 2013) v roce 2013 poskytovalo 58 % firem zaměstnancům firemní zařízení a zároveň jim nechávalo možnost používat zařízení soukromá.

Na to, že BYOD je rychle rostoucím fenoménem, poukazuje v průzkumu CompTIA (Robinson, 2013) fakt, že v roce 2013, kdy průzkum proběhl, mělo 24 % firem z USA zavedená pravidla pro BYOD, zatímco o rok dříve to byla pouze 2 %.

V roce 2013 mělo podle průzkumu Citrix nastavenu strategii pro BYOD zařízení 66 % firem. Pro poskytování mobilních aplikací mělo strategii 56 % firem a pro přístup k datům v k cloudu a sdílených složkách pouze 41 %.

Z výše uvedených statistik vyplývá, že od roku 2011, kdy firmy poznávaly fenomén BYOD, došlo do roku 2013 k přejímání BYOD jako formalizovaného modelu, který má jasně stanovená pravidla, procesy, legislativu i metriky. Řada firem v modelu BYOD vidí budoucnost a postupně ho rozšiřují, buď jako doplněk k zařízením dodávaným firmou nebo jako náhradu firemních zařízení.

Druhy BYOD zařízení a jejich podpora

Průzkumy se zabývaly druhy soukromých zařízení, které firmy nejčastěji podporovaly ve svých BYOD programech.

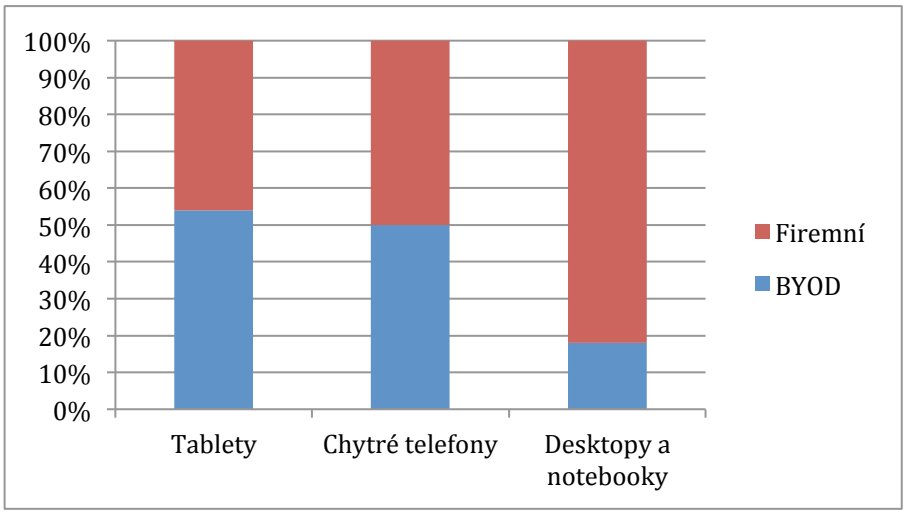
V roce 2011 byly mezi respondenty Citrix (Citrix, 2011) zastoupeny chytré telefony 29 %, notebooky 38 % netbooky 6 %, tablety 8 % a PC 17 %.

IT oddělení dle průzkumu Citrix v roce 2011 poskytovala pro soukromá zařízení podporu v překvapivě vysoké míře. Podporu soukromých chytrých telefonů zajišťovalo 42 % firem, 25 % firem pak podporu tabletů, téměř 50 % firem podporu notebooků, 35 % firem podporu netbooků a kolem 55 % podporu soukromých desktopů.

Z výsledků průzkumu Forrester (Forrester, 2012) vyplývá, že v roce 2012 má 60 % firem implementovaný program BYOD pro chytré telefony, 47 % pro tablety, 47 % pro notebooky a 36 % pro domácí počítače zaměstnanců.

V průzkumu, který realizovala v roce 2013 společnost Citrix, dominovaly BYOD zařízením tablety, kterých bylo 54 % BYOD ze všech tabletů ve firmách. Chytré telefony v programu BYOD tvořily 50 %. V BYOD programu bylo také 18 % desktopů a notebooků. Podle odhadu společnosti Citrix bude poměr BYOD notebooků v roce 2014 znatelně růst, až na 25 % - tedy každý čtvrtý desktop nebo notebook v dotazovaných firmách bude soukromý a zařazený v programu BYOD. BYOD pro notebooky se bude stávat stále rozšířenějším modelem poskytování IT služeb.

Uvedené průzkumy není bohužel možné spolu propojit a získat ucelený obraz v průběhu let 2011 až 2013. Přesto z nich vyplývá, že v poslední době jsou mezi BYOD zařízeními nejčastěji zastoupené chytré mobilní telefony a tablety (oba přes 50 %). Pro tuto práci je zajímavý rostoucí trend poměru soukromých notebooků vůči služebním, který v průzkumu Citrix 2013 činí 18 % a společnost Citrix předpokládá nárůst na 25 % v roce 2014. BYOD se tedy netýká pouze mobilních platforem, ale je také otázkou počítačů. Zastoupení BYOD zařízení na celkovém počtu zařízení ve firmách respondentů je zobrazeno na následujícím grafu.



Obrázek 1-3-1-1: Zastoupení BYOD zařízení ve světových firmách. Zdroj: (Citrix, 2013)

Hybné faktory BYOD

Průzkumy se pokusily identifikovat hybné faktory pro rozvoj BYOD do firem. Hlavním faktorem, který táhl BYOD kupředu byla podle respondentů Citrix v roce 2011 (Citrix, 2011) stále větší technická zdatnost uživatelů, kteří chtějí pracovat na oblíbených zařízeních. Mezi hlavní faktory dále patřila potřeba přilákání talentů a mladých zaměstnanců zatraktivněním prostředí pomocí BYOD. Hybným faktorem byla také potřeba různorodých zařízení, která by podporovala specifické potřeby uživatelů (např. tablet pro obchodní zástupce) a tím by zefektivnila jejich práci i mimo kancelář. Dalšími faktory jsou úsporné programy firem, které v BYOD vidí ušetřené náklady za IT podporu a správu zařízení, zrychlení náboru nových zaměstnanců a formování samoobslužné IT podpory.

Z průzkumu lze učinit závěr, že hlavními hybnými faktory jsou rostoucí technická zdatnost zaměstnanců, preference oblíbených nebo speciálně přizpůsobených zařízení i motivace v možné úspoře nákladů.

Oddělení spolupracující na programu

Průzkum (Citrix, 2011) ukazuje podíl oddělení firem na formování pravidel BYOD. U 94 % respondentů se podílelo na formování IT oddělení, ve 39 % případů oddělení

lidských zdrojů, ve 35 % právní oddělení a ve 29 % finanční oddělení. U malého množství organizací (do 18 %) se na formování BYOD pravidel podílely odborové organizace se zástupci uživatelů a správa budov.

Při implementaci programu BYOD využily firmy dotázané v průzkumu Forrester Consulting (Forrester, 2012) v 86 % případů kapacity IT oddělení, ve 40 % případů podporu senior managementu, 31 % firem využilo oddělení síťové infrastruktury, 28 % technické oddělení, 25 % pak oddělení pro zadávání zakázek. V nižší míře firmy využívaly oddělení právní, správy telekomunikací a externí dodavatele v oblasti IT infrastruktury, consultingu a poskytování telekomunikačních služeb.

Z výsledku průzkumů lze usuzovat, že BYOD je komplexní program, který procesně ovlivní organizaci napříč odděleními. Počet zapojených oddělení závisí i na velikosti organizace. Samozřejmostí je zapojení IT oddělení, mimo jiné z důvodu technického řešení BYOD, dále oddělení lidských zdrojů kvůli úpravě pracovněprávních vztahů a vyplácení příspěvků, finanční (případně i daňové) oddělení pro schválení nákladových modelů BYOD a příspěvků a právní pro schválení nových smluv a požadavků.

Očekávané přínosy

V roce 2011 byly podle průzkumu (Citrix, 2013) benefity, které respondenti nejčastěji dovodili z provozu BYOD nebo které předpokládají, zejména vyšší spokojenost zákazníka, nárůst pracovní produktivity, vyšší mobilita, flexibilnější pracovní prostředí a snížení nákladů na IT podporu. Tyto přínosy pozorovalo více než 35 % respondentů. Oproti tomu pouze necelých 25 % firem shledalo v BYOD prostředek pro zajištění vyšší úrovně business continuity.

Podle průzkumu Forrester Consulting (Forrester, 2012) jako hlavní faktory pro zavedení BYOD uváděly firmy v největší míře (90 %) zvýšení produktivity práce svých zaměstnanců, 63 % firem uvedlo zpřístupnění firemního obsahu zaměstnancům mimo kancelář. Pro 52 % bylo motivem dovolit uživatelům používat soukromé tablety a chytré telefony k práci. 40 % firem spatřovalo významnými úspory v nákladech - ať na správu zařízení nebo na zařízení samotná.

V průzkumu CompTIA (Robinson, 2013) z roku 2013 uvádí 53 % firem mezi hlavní důvody zavedení BYOD programu nárůst produktivity díky vyšší mobilitě a flexibilitě. Mezi další důvody patřil fakt, že svá soukromá zařízení znají zaměstnanci lépe než firemní a vybírají si je tak, aby jim vyhovovala. Dle (Robinson, 2013) je výhodnější, když firmy nechají používat zaměstnance zařízení, která jim vyhovují, místo jednoho druhu poskytovaného IT oddělením firmy.

Vyhodnocení přínosů a nákladů BYOD programu

Společnost Forrester Consulting ve svém reportu uvádí zkušenosti respondentů s reálnými přínosy programu BYOD. Šetření zahrnuje veškerá zařízení BYOD - chytré telefony, tablety i notebooky, případně soukromé desktopy. Vybrány jsou pouze některé přínosy. Jejich úplný výčet je uveden v příloze A.1.

Firmy, které měřily produktivitu zaměstnanců (43 % všech respondentů) v 82 % zaznamenaly zvýšení jejich produktivity. Zvýšená produktivita je tak nejčastěji dosahovaným přínosem BYOD programu. Firmy, které zavedly BYOD také v 69 % zaznamenaly zvýšení příjmů (zde se jedná o metriku, kterou ovlivňuje velmi mnoho faktorů a nelze říci, jaký v ní má BYOD podíl, pozn. autora).

V oblasti softwarových licencí měřilo náklady 60 % respondentů. Jejich zvýšení zaznamenalo 51 %. Z toho lze usuzovat, že BYOD přinesl vyšší využívání licencí. Snížení nákladů na licence zaznamenalo 41 % firem.

U nákladů na správu a údržbu koncových zařízení, které měřilo 59 % firem, zaznamenalo pouze 38 % nárůst a 43 % jejich snížení. Z toho lze usuzovat, že zaměstnanci využívali ve vyšší míře soukromá zařízení a nepotřebovali firemní. Náklady na výměnu zařízení se v 59 % firem snížily. 60 % firem narostly po zavedení BYOD hovory na helpdesk.

Výrazně rostly náklady na zajištění bezpečnosti (63 % na zabezpečení zařízení a 66 % na zabezpečení aplikací) a přenos dat (50 %). V souvislosti se správou mobilních zařízení vynaložilo 60 % firem vyšší náklady na MDM.

V souvislosti s BYOD programem k výraznému zvýšení vyplácení náhrad a bonusů. Nárůst zde zaznamenalo 59 % firem. Pokles nákladů na vzdělání a trénink v 45 % firmách podporuje existenci benefitu vzdělanějších zaměstnanců schopných spravovat svá zařízení samostatně.

Výsledek ukazuje, že BYOD často přispívá ke zvýšení produktivity zaměstnanců a k ušetření části nákladů za správu koncových zařízení. Oproti tomu může znamenat nárůst nákladů na bezpečnost, na vyplácení náhrad a na licence.

Nejčastější aktivity spojené s BYOD

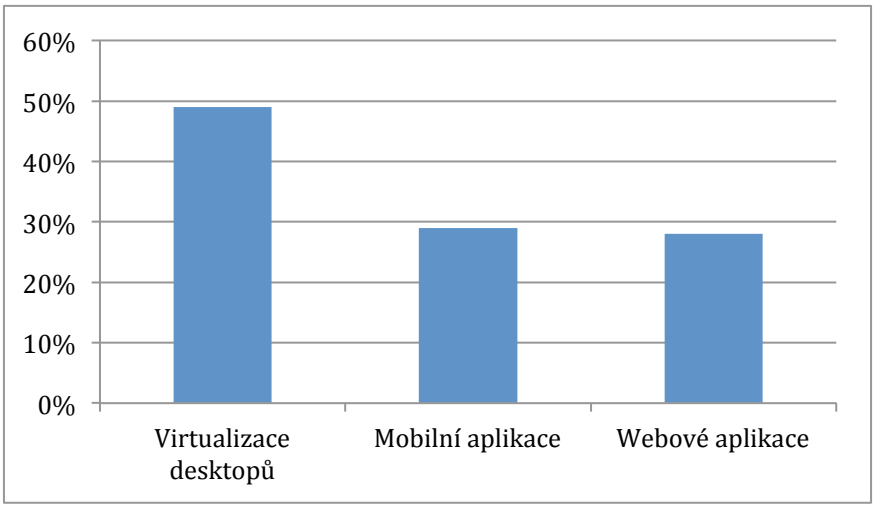
Průzkum Forrester Consulting (Forrester, 2012) se zaměřil na oblasti aktivit spojených se zavedením BYOD programu do firem. Podle výsledků 46 % firem v rámci BYOD zavedlo dokument s pravidly programu a vyžaduje od zaměstnanců jeho přijetí a dodržování, 38 % firem zavedlo příspěvky zaměstnancům za používání soukromých zařízení, 37 % firem pak vyvinulo rozsáhlejší pravidla pro použití dat a aplikací v BYOD a 34 % firem se zabývalo bezpečností BYOD programu. Méně často se pak firmy zaměřovaly na náhrady za datové a hlasové tarify, vytvoření pracovních skupin napříč odděleními, ustavených k formování

pravidel BYOD. Pouze 22 % firem nechalo vypracovat právní analýzu pravidel a bezpečnostních opatření BYOD programu.

Technické zajištění

Podniky volí pro BYOD různé strategie, které průzkum CompTIA (Robinson, 2013) zmapoval. Nejvíce firem (49 %) volí strategii implementace virtuálních desktopů - VDI, tedy serverové poskytování virtuálních strojů. Téměř třetina firem se vydalo cestou vývoje mobilních aplikací na míru pro své business systémy a 28 % firem zvolilo strategii zpřístupnění business aplikací přes rozhraní webového prohlížeče. Průzkum poukazuje na to, že díky postupnému přechodu IT služeb do cloudu z důvodu podpory BYOD uživatelů bude možné lépe řídit náklady na IT služby a uživatelé budou moci využívat svůj přístup z různých zařízení.

Následující graf ukazuje, kolik procent z dotázaných firem implementovalo jaké druhy technického zajištění přístupu k IT službám pro BYOD zařízení.



Obrázek 1-3-1-2: Formy realizace přístupu pro BYOD. Zdroj: (Robinson, 2013)

Průzkumy neuvádějí možnost využít pro dodání pracovního prostředí řešení distribuované virtualizace, které je dále v této práci navržené.

BYOD aplikace

Report (Citrix, 2013) uvádí, že podíl Windows-based aplikací pro čerpání firemních IT služeb postupně klesá ve prospěch SaaS, HTML5/Web a mobilních aplikací. Přesto jsou Windows-based aplikace v roce 2013 zastoupeny dominantně 64 % a Citrix očekává ke konci roku 2014 jejich pokles na 54 %.

V současnosti jsou podle průzkumu mezi IT službami, čerpanými z mobilních zařízení nejčastěji e-mail, kalendář a adresář, dále různé druhy business aplikací, přístup ke sdíleným složkám a nástrojům pro spolupráci.

Přestože zastoupení aplikací založených na operačním systému Windows klesá, tvoří nadále významnou skupinu. Přechod IT služeb na jiné platformy může být problematický. Přesto je možné očekávat, že toto procento bude i nadále klesat. Vysoké zastoupení Windows-based aplikací je možné v BYOD řešit virtualizací fyzických Windows stanic a jejich zpřístupnění ve VDI, případně je distribuovat na koncová zařízení jako virtuální stroje.

Zpřístupnění BYOD skupinám uživatelů

Průzkum Citrix 2011 se zabýval i otázkou, kterým skupinám uživatelů zpřístupňují firmy BYOD program. Je zřejmé, že pro některé pracovní pozice je BYOD program velmi přínosný (např. u obchodních zástupců) a naopak u některých pozic je nežádoucí, aby zaměstnanci pracovali na BYOD zařízeních (z důvodu práce s citlivými daty nebo např. v call centrech, kde jsou počítače speciálně upraveny).

Z průzkumu (Citrix, 2011) vyplývá, že nejčastěji firmy povolovaly BYOD mobilním zaměstnancům (přes 60 %), specialistům (téměř 40 %) a zaměstnancům, pracujícím na dálku (téměř 45 %). Nejméně často pak firmy povolovaly BYOD plošně všem zaměstnancům (pouze 9 %) nebo pracovníkům zákaznické podpory a call center (do 25%).

Z odpovědí respondentů vyplývá, že je třeba přístup zaměstnanců do BYOD programu řídit. Program je sice možné uplatnit u velkého procenta zaměstnanců, ale je třeba vždy určit skupiny uživatelů, kterým bude povolen a kterým zakázán. Je možné, že zaměstnanci na některých pracovních pozicích budou mít dovoleno využívat pouze část BYOD programu (např. BYOD pro chytré telefony jim bude povolen, zatímco BYOD pro notebooky zakázán).

Očekávaná součinnost uživatelů

Další část průzkumu Citrix z roku 2011 (Citrix, 2011) identifikovala činnosti, které v rámci programu BYOD očekávaly firmy od svých zaměstnanců. Odpovědi respondentů nejsou jednoznačné. Kolem poloviny firem očekávalo, že si zaměstnanci BYOD zařízení sami koupí a připraví do provozu. Přibližně 40 % firem od svých zaměstnanců očekávalo, že si sami zajistí podporu zařízení. A pouze třetina očekává, že budou zaměstnanci na zařízení zajišťovat antivirovou ochranu.

Tato část otevírá otázku vyjasnění práv a povinností zaměstnance a zaměstnavatele v BYOD programu. Významnější shoda respondentů je u pořízení BYOD zařízení, jeho uvedení do provozu a zajištění podpory. Zde přibližně polovina firem nechává tyto činnosti na zaměstnanci. Ostatní činnosti je třeba určit, ale v průzkumu se názory respondentů různí a nelze z nich vycházet.

Poskytování a výše finančního příspěvku

V roce 2011 respondenti průzkumu společnosti Citrix (Citrix, 2011) uvedli, že v oblasti finanční podpory plánuje poskytnout 41 % firem příspěvek srovnatelný s ušetřenými náklady na nákup a správu zařízení, 31 % alespoň část těchto nákladů a ostatních 28 % firem neuvažovalo o finanční podpoře zaměstnanců v BYOD programu vůbec. Z výsledků dále vyplývá, že nejvíce firmy finančně podporují BYOD v Indii a Německu. Nejméně pak ve Velké Británii a Nizozemsku.

Důvodem rozdílné výše finanční podpory jsou i různé implementace BYOD programu v konkrétních firmách. Je pravděpodobné, že pokud BYOD zařízení je náhradou firemního, bude příspěvek vyšší než v případě, že BYOD je doplňkem k firemnímu zařízení.

Obavy z BYOD programu

Respondenti průzkumu (Citrix, 2011) byli v souvislosti s BYOD nejčastěji znepokojeni možnými bezpečnostními problémy (více než 50 %) a ve více než 40 % případů i možnými problémy s podporou BYOD zařízení a náklady na zavedení BYOD programu.

Z průzkumu Forrester (Forrester, 2012) vyplývá, že za hlavní překážky respondenti považovali bezpečnostní rizika, problematickou implementaci se stávajícími systémy, získání podpory u managementu a v menší míře i problematiku finanční obhajoby BYOD programu z důvodu převažujících nefinančních přínosů.

Bezpečností BYOD bylo v roce 2013 podle průzkumu Citrix (Citrix, 2013) velmi znepokojeno 58 % respondentů. Oproti tomu pouze 13 % respondentů nebylo bezpečností BYOD znepokojeno vůbec.

Nejčastěji převažují obavy v oblasti bezpečnosti. Respondenti se shodují, že BYOD zařízením hrozí vyšší rizika krádeže, ztráty dat nebo technických problémů. Vážným problémem může být i integrace BYOD zařízení ve stávajícím firemním prostředí.

1.3.2 Přínosy programu BYOD

Podle článku (Norsa, 2013) jsou hlavními přínosy BYOD zvýšení pracovní mobility uživatelů, větší pracovní nasazení mimo pracovní dobu, rychlejší komunikace a uspokojení zaměstnanců tím, že pracují na oblíbeném zařízení. Znatelné jsou úspory nákladů IT. Se vzrůstající mobilitou klesají i náklady na pracovní místa díky možnosti práce z libovolného místa, např. homeworking.

Článek dodává, že je těžké vyjadřovat benefity pouze finančními měřítky, protože úspora nákladů na služby IT oddělení tvoří pouze část z mnoha přínosů BYOD.

Výhodou zavedení BYOD by měl být podle (Norsa, 2013) i fakt, že se jedná o projekt, který zasáhne všechny uživatele, tedy i uživatele z tzv. business oblasti a nejen technicky orientované profese. To pomáhá s propagací projektu.

V článku ComputerWeekly (Ashford, 2012) jsou uvedeny mezi dalšími benefity i technicky zdatnější zaměstnanci. BYOD mezi zaměstnanci podporuje kreativitu a inovace tím, že sami iniciativně přebírají nové technologie.

BYOD ve společnosti Intel

Agam Shah (Shah, 2013) se zabývá ve svém článku na CIO.uk benefitem zvýšené produktivity práce ze zavedení BYOD programu. Článek popisuje stav ve společnosti Intel Corporation, která zavedla program BYOD. Její CIO Kim Stevenson tvrdí, že každý zaměstnanec průměrně díky BYOD ušetřil 57 minut v každém pracovním dni. Intel svůj program BYOD modeloval právě pro zvýšení produktivity, potenciálními úsporami se zabýval okrajově. V roce 2013 má Intel 23 500 mobilních BYOD zařízení (což je oproti roku 2011 nárůst o 38 %). Společnost se vydala cestou vývoje mobilních aplikací. V roce 2013 měl 41 vlastních mobilních aplikací a 16 ověřených aplikací třetích stran pro provoz na BYOD zařízeních. Takovými aplikacemi jsou například rychlé posílání zpráv, nástroje pro spolupráci a organizování, či pro rychlé schvalování požadavků. Pro přístup k aplikacím provozuje Intel privátní cloud, na kterém podporuje řadu zařízení a využívá jejich funkce, jako informace o poloze apod. BYOD program je ve společnosti Intel zaměřen na chytré telefony, drobnou část zaujímají tablety a notebooky.

Zvláštní pozornost začíná Intel věnovat ultrabookům. Zahrnuje je do svého programu BYOD. Pro přístup k IT službám ultrabooky využívají aplikace založené na cloudových technologiích. K zabezpečení pak využívá svoji technologii VPro, umožňující vzdálenou správu a dohledání či smazání ultrabooku. Zajímavé je nasazení víceúrovňového modelu bezpečnosti pro BYOD zařízení. Model podle uživatele, polohy a druhu zařízení povoluje přístup k různým informacím a službám.

Uvedené články korespondují s průzkumy z předchozí kapitoly, kdy mezi hlavní přínosy BYOD nejčastěji uvádějí zvýšení produktivity zaměstnanců, vyvolané zvýšením jejich flexibility, mobility, spokojenosti a rychlejší reakce. Zdroje se shodují, že ušetřené náklady na IT jsou dalším přínosem BOYD, který je však méně významný než zvýšení produktivity zaměstnanců.

1.4 Dopady programu BYOD na firemní prostředí

Tato podkapitola naplňuje cíl - *1. Zpracovat teoretická východiska práce na základě dostupných zdrojů* - tím, že rozborem aktuálních zdrojů zachycuje problematiku dopadů

zavedení programu BYOD na firemní prostředí. Podkapitola také pomáhá naplnit cíl - *3. Vytvořit rámec pro projekt BYOD pro notebooky*.

Program BYOD reaguje z části na existující fenomén používání soukromých zařízení ve firmách, pro který zavádí pravidla, a z části mění firemní prostředí novým způsobem. Změny spojené se zavedením BYOD programu se dotknou jak práce zaměstnanců, tak firemních procesů a pravidel. V řadě případů přináší program BYOD i celkovou změnu filozofie, se kterou zaměstnanci zařízení používají. Od hardware, který jim byl přidělen a byl kompletně firemní, přesouvá BYOD firemní prostředí do soukromého hardware zaměstnanců, který si sami zvolili. Zařízení tak přestává být pracovním nástrojem poskytnutým zaměstnavatelem a začíná být součástí zaměstnancovy vlastní identity, která podléhá jeho potřebám a preferencím. Patrné to je například u zařízení výrobce Apple, který vytváří tzv. imagové produkty, jak uvádí i (Keyes, 2013), a se kterými se řada uživatelů ztotožňuje.

BYOD program ovlivní řadu interních procesů. Ovlivněny jsou procesy oddělení, která identifikovaly průzkumy v kapitole 1.3 a která se podílejí na zavádění BYOD. Zejména se jedná o IT oddělení a oddělení lidských zdrojů, jejichž procesy jsou programem BYOD ovlivněny v největší míře.

1.4.1 Dopady na IT procesy

Dopady na IT procesy tvoří jednu z nejvýznamnějších změn při zavedení BYOD. Jako model, podle kterého jsou dopady přiblíženy, je využit ITIL v3. Ten je založen na životním cyklu služeb a využívá ho k řízení IT řada významných společností.

(NORSA, 2013) ve svém článku v CIO na fakt, že zavedení BYOD ovlivní služby řízené pomocí ITIL v3, upozorňuje. BYOD se podle něj promítne do všech životních cyklů ITIL. Pro firmu to znamená zvážit všechny důsledky BYOD a upravit podle nich dotčené IT procesy. Vzhledem k tomu, že podoba BYOD programu může být různá v každé firmě (od podpory soukromých mobilních telefonů až po široké zpřístupnění firemních služeb na různých druzích zařízení včetně notebooků), dotkne se zavedení BYOD programu IT procesů v různé míře.

Podle (NORSA, 2013) by měl být BYOD zaveden v ITIL katalogu služeb včetně nadefinovaných podmínek poskytování služby, SLA[2]. Zároveň by měl vzniknout v rámci katalogu přehled o zaměstnancích, kteří přistoupili na podmínky BYOD a tuto službu čerpají.

Ze článku (ProActive, 2013), publikovaného v roce 2013 australskou společnosti ProActive, která se zabývá implementací ITIL, vyplývá, že pouze 11 % firem je schopno

[2] SLA = Service Level Agreement, smlouva o úrovni poskytované služby.

zcela identifikovat zařízení, která přistupují do firemní sítě. Z dotázaných CIO si 34 % myslí, že jejich zaměstnanci přistupují do sítě i ze soukromých zařízení a 68 % zaměstnanců to ve skutečnosti i neoficiálně dělá. Bezpečnostní rizika, která z tohoto stavu vyplývají, jsou podle (ProActive, 2013) důvod k implementaci pravidel BYOD do systému řízení informatiky ITIL.

Společnost ProActive se dále ve svém článku obecně zabývá dopady BYOD na jednotlivé části knih ITIL v3. V této práci jsou uvedeny pro přiblížení dopadů na interní procesy. Neslouží jako přesné mapování, které pokrývá systematicky všechny oblasti ITIL, ale poskytuje souhrnný a zjednodušený pohled na věc.

ITIL - Service Strategy

První kniha ITIL v3 životního cyklu IT služeb Service Strategy se zabývá IT Governance. Její největší přínos je pro osoby na řídících pozicích jako CIO. Poskytuje celkový pohled na management IT služeb. Článek (ProActive, 2013) doporučuje v souvislosti s BYOD analyzovat následující oblasti:

- formy poskytování BYOD služeb,
- skupiny uživatelů, kterým bude BYOD poskytován,
- zachování úrovně business požadavků a výstupů,
- IT služby zpřístupněné pro BYOD,
- správa BYOD zařízení,
- poplatky za vybavení a aplikace,
- úroveň uživatelské podpory poskytované IT oddělením.

V rámci procesu **Service Portfolio Management** je nutné vytvoření modelu poskytování IT služeb pro BYOD.

Proces **Financial Management** je zavedením programu BYOD také ovlivněn. V rámci něj je třeba definovat nákladové modely platné pro konkrétní podobu BYOD programu. Nákladové modely je možné, jak uvádí (ProActive, 2013), využít při následném modelování business case, rozpočtování a jako podklad pro fakturaci za služby.

ITIL - Service Design

Druhá kniha ITIL v3 životního cyklu IT služeb Service Design se zabývá návrhem služeb tak, aby dokázaly uspokojit současné i budoucí požadavky businessu.

V procesu **Information Security Management** je nutné nadefinovat nové bezpečnostní standardy pro zařízení BYOD. Dále upravit nové povinnosti uživatelů, kteří mohou být v pozici administrátora svého zařízení a měli by dodržovat požadavky na správu koncových stanic.

Podstatným aspektem bezpečnosti, jak dodává (ProActive, 2013), je právní oblast. Uživatel BYOD by se měl zavázat k plnění svých povinností (jako jsou správa hardware, udržení aktualizovaného systému a software, provozování bezpečnostního software - pozn. autora). Uživatelé by měli prokázat svoje znalosti absolvováním školení a závěrečné zkoušky.

Program BYOD znamená zanesení nových IT služeb do katalogu, který je popsán v procesu **Service Catalogue Management**. Součástí popisu BYOD IT služeb je i vytvořený postup jejich získání a podmínky jejich čerpání.

Pokud BYOD znamená dodatečné nároky na kapacitu zaměstnanců nebo infrastruktury, je třeba toto zohlednit v procesu **Capacity Management**. Konkrétně se může jednat o dodatečné zaměstnance pro správu soukromých zařízení, rozšiřování přenosových kapacit pro vzdálená připojení přes VPN nebo přes interní Wi-Fi.

V případě, že zavedení a provoz BYOD znamená zavedení nového dodavatele, je třeba tento fakt zohlednit v procesu **Supplier Management**. Může se jednat o nového dodavatele řešení pro virtualizaci, správu mobilních zařízení, případně o dodavatele kompletně outsourcovaných řešení pro BYOD.

ITIL - Service Transition

Třetí kniha ITIL v3 životního cyklu IT služeb Service Transition se zabývá zaváděním navržených služeb do produkčního prostředí.

V procesu **Change Management** je nutné zohlednit změny v IT infrastruktuře, reportingu, pravidlech poskytování IT služeb nebo v bezpečnostním modelu.

Proces **Knowledge Management** by měl podporovat zavedení samoobsluhy pro uživatelskou podporu, která by zpřístupnila uživatelům znalosti potřebné ke správě BYOD zařízení. Dále by mělo být zváženo publikování návodů a zavedení BYOD fóra a platformy typu Wiki.

ITIL - Service Operation

Čtvrtá kniha ITIL v3 Service Operation se zabývá samotným provozem služeb. Jejím cílem je zajistit provozování služeb ve sjednané kvalitě.

V oblasti provozu by měl service desk dostat jasné postupy, jak postupovat v případě požadavku, vztahujícímu se k BYOD programu. Zadokumentováno by mohlo být, i které služby čerpal uživatel BYOD od třetích stran.

V procesu **Access Management** je třeba nadefinovat uživatelům povolení přístupu k IT službám a zdrojům.

ITIL - Continual Service Improvement

Poslední kniha ITIL v3 Continual Service Improvement, se zabývá stálým vylepšováním IT služeb.

Pro program BYOD to znamená zavedení nových metrik, jejich měření a kontrolu naplňování.

1.4.2 Dopad na procesy oddělení lidských zdrojů

Dopady zavedení BYOD na procesy oddělení lidských zdrojů se zabývá (Keyes, 2013) ve své knize. BYOD se do lidských zdrojů promítá v poměrně širokém rozsahu. V souvislosti s tím je potřeba například:

- revidovat postupy při přijímání nových zaměstnanců,
- nastavit nové motivační programy,
- zavést náhradu za opotřebení vlastního pracovního nástroje,
- revidovat pracovní smlouvy a vytvořit nové dodatky,
- nastavit postupy pro zařazení a vyřazení zaměstnance z BYOD programu.

Procesy oddělení lidských zdrojů nejsou pro tuto práci primární oblastí. Příklady dopadů na lidské zdroje jsou zde uvedeny jako ilustrace šíře BYOD. Práce se však v první řadě zaměřuje na IT procesy.

1.5 Virtualizace pracovních stanic

Podkapitola naplňuje cíl - 1. Zpracovat teoretická východiska práce na základě dostupných zdrojů - v oblasti problematiky virtualizace.

Využití virtualizace je jedním z možných technických prostředků, kterými jsou zpřístupněny IT služby uživatelům BYOD. Jak vyplynulo z průzkumů uvedených v kapitole 1.3, ve firmách stále dominují aplikace založené na operačním systému Windows (v roce 2013 jich bylo 64 %) a pravděpodobně i z tohoto důvodu 49 % firem využívá VDI ke zpřístupnění pracovního prostředí uživatelům BYOD.

Virtualizace představuje dle (Shackleford, 2013) abstrakci výpočetních zdrojů z fyzické hardwarové vrstvy. Při virtualizaci je hostitelský systém využit k tomu, aby vhodným způsobem zpřístupnil virtualizované vrstvy hostovanému systému běžícím ve virtuálním

stroji (VM[3]). VM je v hostitelském systému reprezentována skupinou souborů, ve kterých je uložena konfigurace, paměť i disk hostovaného systému.

Pro zpřístupnění zdrojů VM jsou využívány různé softwarové platformy. (Shackleford, 2013) uvádí mezi nejčastější serverové VMware ESXi, Microsoft Hyper-V, Citrix XenServer a Red Hat KVM.

K většímu rozvoji virtualizace dochází mimo jiné díky dostupnému výkonnějšímu hardware, který má dostatek kapacity pro provoz více hostovaných systémů současně. Dnes běžně dostupné procesory mají zabudovanou podporu virtualizace. Tento trend se v posledních letech přenáší od serverových platforem k osobním počítačům. Příkladem jsou virtualizační technologie Intel VT-x a AMD AMD-V.

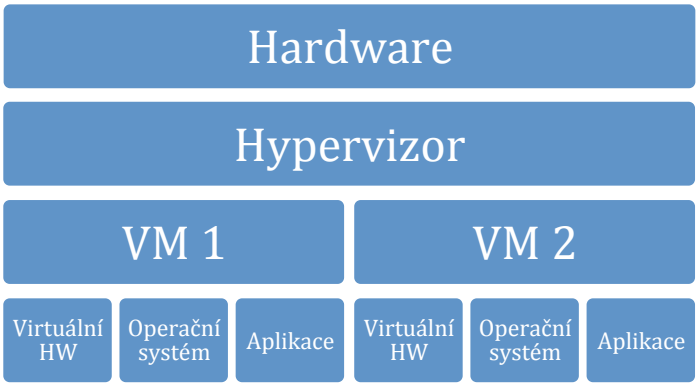
1.5.1 Architektura virtualizace

Virtualizační řešení se, jak uvádí (Shackleford, 2013), skládá ze základních komponent - fyzického hardware, hypervizoru, a virtuálních strojů (hostovaných systémů). Hypervizor, který řídí přístup k fyzickému hardware, může být postaven přímo na hardwaru jako tzv. bare metal a nebo nainstalovaný jako aplikace nad běžnými operačními systémy.

Hypervizor I. typu (bare metal)

Hypervizory I. typu obsahují jednoduchý operační systém a instalují se přímo na hardware hostitele. Hypervizor má rozšířený přístup k hardware oproti hypervizorům II. typu. V modelu úrovní privilegií procesorů architektury x86 (Ring 0 - Ring 3) využívá hypervizor I. typu všechny úrovně, tedy od Ring 0 určené pro jádro systému po Ring 3 určené pro uživatelské operace a spouštění aplikací.

Příkladem takového hypervizoru je VMware ESXi.



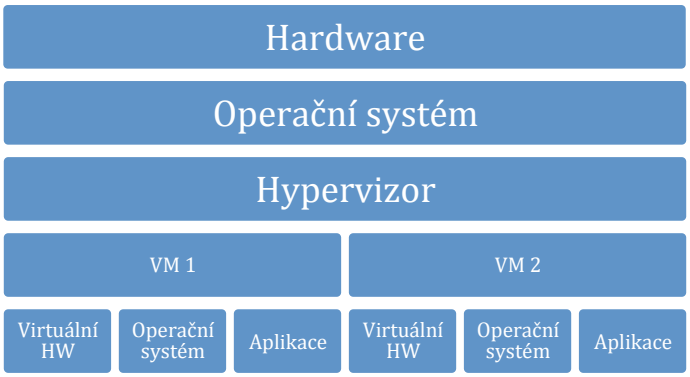
Obrázek 1-5-1-1: Architektura hypervizoru I. typu. Zdroj: (Shackleford, 2013)

[3] VM = Virtual Machine

Hypervizor II. typu (aplikační)

Hypervizory II. typu jsou vyvinuty ve formě aplikace pro operační systém. Nejčastěji jsou podporovány systémy typu Windows, OS X a Linux. Hypervizory II. typu se instalují přímo do operačního systému hostitele. Hypervizor má omezený přístup k hardware oproti hypervizorům II. typu. V modelu úrovní privilegií procesorů architektury x86 je hypervizor II. typu integrován pouze v Ring 3 určené pro spouštění aplikací a ostatní vrstvy jsou mu zprostředkovány virtuálně.

Příkladem takového hypervizoru je VMware Workstation.



Obrázek 1-5-1-2: Architektura hypervizoru II. typu. Zdroj: (Shackleford, 2013)

Síťová architektura

K hypervizorům I. a II. typu se typicky váže i rozdílná síťová architektura. Zatímco hypervizory I. typu jsou provozovány ze své podstaty pouze na serverech a pro provoz virtuálních pracovních stanic používají VDI, pak hypervizory II. typu mohou být provozovány jak na serveru, tak na stanici klienta. VMware v případě hypervizorů II. typu hovoří o tzv. Personal Desktop Virtualization, tedy virtualizaci na osobních počítačích.

1.5.2 Známé hrozby ve virtualizovaném prostředí

Na úvod je třeba zdůraznit, že hostovanému systému hrozí úplně stejná rizika, jako kdyby nebyl provozován virtuálně. Zde uvedené hrozby se týkají problémů spojených s virtualizací.

U virtualizace je možné se setkat se specifickými zranitelnostmi. Nejčastěji uváděnými hrozbami jsou krádež VM, vyzrazení dat VM, proniknutí do VM běžící paralelně, nebo zanesení tzv. virtualization aware malware[4].

Následující hrozby přibližují (Shackleford, 2013) ve své knize.

[4] Virtualization aware malware je malware, který mění své chování podle toho, zda je spuštěn ve virtuálním prostředí.

Provozní hrozby

Provozní hrozby působí při provozování virtuálního prostředí a jsou způsobeny lidským faktorem. Může se jednat o nehodu, lidskou chybu nebo zlý úmysl.

Neřízené vytváření VM je první hrozbou, kterou uvádí (Shackleford, 2013). Nové VM mohou být velmi snadno nasazeny během minut. To může v některých případech vést až k rychlému nasazování neprověřených a neotestovaných stanic. Jedna slabě zabezpečená VM může znamenat bezpečnostní slabinu, která ohrožuje celé prostředí. K neřízenému vytváření VM dochází častěji ve firmách s nižší úrovní zralosti procesů.

Nízká transparentnost virtuálního prostředí je dalším druhem hrozby. V praxi se IT oddělení zaměří na monitorování serverů a fyzické infrastruktury. Ve skutečnosti je virtuální infrastruktura zranitelná ve srovnatelné míře, jako fyzická. Virtuální sítě mají také své switche a routery, které je třeba řídit. Automatizované nástroje jsou často nastaveny pro práci s fyzickou sítí a do virtuální sítě nemají přístup. Virtuální síťový provoz mezi více VM v jednom hypervizoru je třeba také monitorovat. Může zde docházet k únikům dat nebo k problémům s výkonem.

Nedostatečná pravidla pro rozdělení odpovědnosti mohou způsobit vytvoření prostředí, ve kterém nejsou jasně rozděleny pravomoci mezi správci aplikací, sítí a systémů. Může být problematické při sporu mezi společností, zaměstnanci a dodavateli. Opatřením může být vytvoření pravidel pro správu VM a pevné dodržování principů change a configuration managementu (známého z ITIL v3).

Krádež VM

Další hrozbou, která na VM působí, je možnost krádeže. Ta je ulehčena tím, že celý hostovaný systém je zabalen ve VM, která je v hostitelském systému reprezentována několika soubory. Krádež VM nemusí být ani zaznamenána, protože ji lze provést pouhým překopírováním souborů. VM lze ukradnout získáním přístupu do hostitelského systému. Možností ochrany je např. aplikování pravidel řízení přístupů, nebo logování. Úniku dat je možné také zabránit šifrováním VM.

Hrozby malware

Od roku 2006 se začaly objevovat škodlivé programy jako boti, červi, rootkity, které dokázaly zjistit, zda běží ve fyzickém nebo virtuálním prostředí a tomu přizpůsobily své chování. Pokud malware zjistí, že běží ve virtuálním prostředí, změní své chování. To může být i takové, že malware nebude dělat nic z důvodu, že řada antivirových společností používá k analýze malware virtuální prostředí a malware se tímto maskuje.

VM Escape

VM Escape by bylo možné do češtiny přeložit jako útěk z virtuálního stroje. To vystihuje podstatu hrozby, tedy vystoupení z izolovaného prostředí VM do prostředí hypervizoru nebo hostitelského systému. Jedná se o velmi závažnou hrozbu, kdy útočník pronikne do důvěryhodného prostředí. To způsobí narušení bezpečnosti pro celý virtuální systém, tedy všechny hostované VM, systémové prostředí hypervizoru, případně i hostitelského OS v případě použití hypervizoru II. typu.

VM Escape je málo prozkoumanou hrozbou. Návrháři virtualizačních technologií si uvědomují závažnost této hrozby a tak jsou bezpečnostní mechanizmy silné a není snadné VM Escape provést. Většina doposud úspěšných útoků využila k VM Escape zanesení škodlivého kódu jak do hostitelského systému, tak do systému hostovaného. Nejzávažnější forma čistého VM Escape útoku by se však odehrávala pouze ze strany hostovaného systému.

Directory Traversal Attack, útok průchodu mezi adresáři je popsán od roku 2007. Je jedním z druhů VM Escape. Zranitelnost se týkala VMware Workstation a její funkce sdílení adresářů mezi hostovaným a hostitelským systémem. Kvůli chybě v interpretaci názvů souborů mohlo dojít po zanesení malware do VM k zápisu souborů do hostitelského systému pod právy uživatele. To v případě uživatele, který spouštěl hypervizor VMware Workstation pod administrátorskými právy mohlo znamenat vážné ohrožení bezpečnosti hostitelského systému.

Skupina IntelGuardians v roce 2007 přišla s několika nástroji, pomocí kterých je možné provést Directory Traversal Attack. Všechny byly zaměřeny na virtualizační platformu VMware:

- **VMchat** - v prvním případě byla využita zranitelnost komponenty VMchat, kterou VMware hypervizor používá pro komunikaci mezi hypervizorem a VM. Útok nepotřebuje zanesení škodlivého kódu a nemá vliv na síťové prostředky.
- **VMcat** - je nástroj pro přenášení vstupů a výstupů typu stdin/stdout po komunikačním kanálu vytvořeném komponentou VMchat. Může být použit k přenášení příkazů shellu mezi hostitelem a hostem.
- **VM Drag-n-Sploit** - využívá zranitelnosti komponenty hosta VMwareService.exe, která slouží k funkci Drag and Drop mezi hostem a hostitelem ve VMware Workstation. Pomocí nástroje je možné monitorovat i pozměnit komunikaci mezi VM a hypervizorem.
- **VMftp** - jednalo se o útok, který umožnil z jakéhokoliv hostovaného systému na jakékoliv úrovni práv číst a zapisovat do souborového systému hostitele. K uskutečnění útoku bylo třeba, aby bylo zapnuté sdílení adresářů a alespoň jeden adresář byl sdílen.

Directory Traversal Attack uskutečnili v roce 2008 i vývojáři z Core Security, která vyvíjí známý nástroj pro penetrační testování Core Impact. Objevili zranitelnost VMware Workstation a příbuzných produktů ve funkci Sdílené Adresáře. Díky útoku bylo možné z VM číst a zapisovat do celé adresářové struktury hostitelského systému.

Další zranitelnosti virtualizačních technologií byly popsány na úrovni virtualizačních funkcí procesorů jako AMD-V procesorů AMD a VT-x procesorů Intel. Zranitelnosti na úrovni instrukcí procesorů jsou obecně náročnější na odhalení a mohou mít vysoké dopady.

Dle (Shackleford, 2013) byl v roce 2009 poprvé proveden útok typu buffer overflow, který pomocí přetížení ovladače ve VM způsobil spuštění vloženého kódu pod hypervizorem. Jednalo se do roku 2013 o útok nejbližší VM Escape vedený pouze z hostovaného systému. V roce 2010 společnost VMware oznámila řadu odhalených zranitelností většího rozsahu na svých virtualizačních platformách. Vydala 40 CVE[5], které převzali a aplikovali uživatelé VMware produktů. Jednalo se například o vzdáleně způsobené DoS, spuštění kódu, nebo eskalace práv.

Je třeba uvést, že s bezpečností neměly problém pouze produkty VMware, ale i konkurenční Citrix XenServer nebo Microsoft Hyper-V. Zranitelnostem VMware je věnováno více prostoru jak z důvodu jejich rozšíření, tak návaznosti na tuto práci. Většina uvedených útoků využívala zranitelnosti rozšířených funkcionalit VMware Workstation, jako jsou sdílení schránky, sdílení souborů nebo povolení drag and drop. Tyto funkce je možné zcela zakázat a tím se uvedeným zranitelnostem vyhnout.

1.5.3 VMware Workstation 10

VMware Workstation 10 je virtualizační platformou pro provozování virtuálních strojů na běžných operačních systémech. Funguje jako hypervizor II. typu.

Mezi přímé konkurenty VMware Workstation patří Oracle VirtualBox, Parallels Desktop a Microsoft Virtual PC.

Jak uvádí VMware na svých stránkách (VMware, 2014), Workstation 10 má zjednodušenou verzi Player 6 pro nekomerční použití, Player Plus 6 pro komerční použití a Fusion 6 pro komerční i nekomerční použití v systémech OS X. Rozšířenou verzí pro systém OS X je Fusion Pro 6, která funkcionalitou odpovídá produktu Workstation. Workstation a Player jsou dostupné pro systémy Linux, Unix a Windows, Fusion pro Linux a OS X. Většina textu v této práci se zabývá funkcemi shodnými ve všech těchto produktech a proto při zmínění VMware Workstation platí tvrzení i v produktech Player a Fusion.

[5] Common Vulnerabilities and Exposures - společných zranitelností a ohrožení

Kompatibilita s operačními systémy

Pro instalaci hypervizoru je v případě Workstation 10 vyžadován operační systém Microsoft Windows XP SP3, Vista, 7 nebo 8 ze systémů pro koncové stanice. Podporované serverové systémy Microsoft jsou Windows Server 2003, Windows Server 2008 a Windows Server 2012. Z Linuxových systémů to jsou aktuální verze distribucí OpenSUSE (SUSE Linux), CentOS, Ubuntu, Red Hat Enterprise a další. Podpora systémů Apple OS X je zajištěna aplikací VMware Fusion 6, která svou funkcionalitou odpovídá aplikaci Player 6 nebo Workstation 10 v případě Fusion Pro 6. Fusion má podporu specifických funkcí prostředí OS X, jako zálohování Time Machine, rozdílná práce se soubory apod. Podporovány jsou jak 32 bitové, tak 64 bitové verze.

Škála hostovaných systémů není omezena. VMware vydává seznam kompatibilních OS, pro které jsou vytvořeny ideální profily virtuálního hardware, testována funkčnost a výkon. Ze systémů Microsoft jsou to Windows 2000 a novější, z linuxových distribucí jsou to Ubuntu 8.04 a novější, CentOS 5.10 a novější, Debian GNU/Linux 5.0 a novější, dále novější verze distribucí Red Hat, Fedora, SUSE a Oracle Linux. Z dalších systémů to jsou Sun Solaris a FreeBSD[6].

Kompatibilita s virtualizačními technologiemi

Kompatibilita s ostatními produkty VMware je na vysoké úrovni. VM vytvořenou ve Workstation je možné provozovat na serveru VMware ESX (ESXi) i na koncových zařízeních (Shackleford, 2013). VMware dodává ke svým řešením zdarma nástroje pro konverzi, jako OVF Tools pro export do tzv. virtuálních appliancí, tedy virtuálních strojů zabalených v jediném souboru, který odpovídá standardům a je možné ho spustit i na konkurenčních hypervizorech.

Kompatibilita s konkurenčními produkty je omezená. Přenos VMware VM na konkurenční stanice probíhá buď přes otevřené formáty OVF a OVA nebo s použitím nástrojů pro konverzi. Není možné převést kompletní konfiguraci VMware VM, protože obsahuje funkce, které konkurenční hypervizory nepodporují. Mezi takové funkce patří vytváření VM v tzv. restricted módu, který zajišťuje ochranu konfigurace VM před neoprávněnými změnami.

Porovnání funkcí Workstation a Player

Workstation (Fusion Pro) a Player (Fusion) mají společný hypervizor a je možné mezi nimi přenášet VM bez nutnosti konverze. Liší se pouze funkcionalitou. Nejpodstatnější rozdíly shrnuje tabulka na následující stránce.

---

[6] Úplný seznam kompatibility operačních systémů s produkty VMware je k dispozici na webových stránkách "http://www.vmware.com/resources/compatibility".

Tabulka 1-5-3-1: Porovnání VMware Workstation 10 a Player 6. Zdroj: (VMware, 2014)

Funkcionalita	**Player (Plus) 6**	**Workstation 10**
Funkce hypervizoru	ANO	ANO
Spouštění VM v restricted módu	ANO	ANO
Vytváření VM v restricted módu	NE	ANO
Klonování VM	NE	ANO
Vytváření snapshotů (snímků stavu běžící VM)	NE	ANO
Poskytování VM po síti klientům	NE	ANO
Konverze fyzického systému do virtuálního	NE	ANO

Složení VM

VM se skládá z několika souborů, které jsou pro VMware produkty specifické. Složení popisuje (Shackleford, 2013) a je patrné ze schématu na *obrázku 1-5-3-1*.

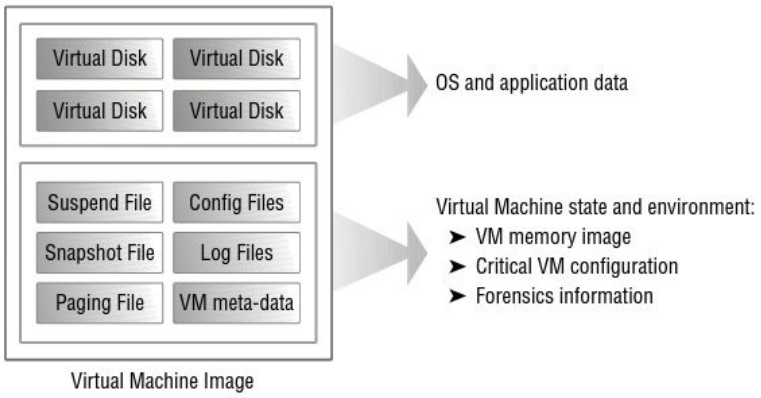
Hlavním souborem je <název_VM>.vmx. Obsahuje konfiguraci VM - od emulovaného hardware po aktivaci speciálních funkcí, jako povolení sdílení schránky nebo souborů VM s hostitelem. Soubor je v textové podobě, takže je možné editovat detailní nastavení parametrů VM pomocí textového editoru. Pokud je VM zašifrována přes funkci šifrování ve VMware Workstation, je zašifrován i soubor <název_VM>.vmx.

Druhým důležitým souborem je <název_VM>.vmdk, což je konfigurační soubor s nastavením disků, které VM používá. Patří k němu soubory <název_VM>-flat.vmdk pro celý disk v jednom souboru nebo <název_VM>-s001.vmdk pro disk rozdělený do více souborů (tzv. Sparse). Konfigurační soubor je textový a obsahuje cesty k diskům a další významné informace. V případě zapnutého šifrování VM je soubor VMDK zašifrován.

<název_VM>.nvram je BIOS virtuálního stroje. VMware používá BIOS platformu Phoenix. Tento soubor se podle (Shackleford, 2013) při každém spuštění VM znovu vytváří.

<název_VM>.log a vmware.log jsou soubory s protokolem. Obsahují logovací zprávy na úrovni nastavené v konfiguraci VM.

Ve VM se vyskytují i další soubory, které slouží jako stránkovací soubory, jako tzv. snapshoty nebo soubory pro obnovení z hybernace.



Obrázek 1-5-3-1: Soubory tvořící VM, Zdroj: (Shackleford, 2013, str. 187)

VMware Tools

VMware Tools jsou dostupné pro podporované hostované operační systémy ve formě instalačního balíčku, který je možné nainstalovat do hostovaného systému buď běžným způsobem pomocí instalačních souborů aplikace nebo zjednodušeným způsobem přímo z menu hypervizoru Workstation nebo Player/Fusion. Dostupné jsou i tzv. OSP balíčky[7] pro podporované systémy. Podrobné informace uvádí VMware v manuálu Installing and Configuring VMware Tools (VMware, 2012).

Tools obsahují ovladače pro zajištění vyšší kompatibility hostovaného systému s hypervizorem a s hostitelským systémem. Jedná se o ovladače:

- grafické karty a zobrazení,
- ovladač disku SCSI,
- síťového rozhraní,
- zvukového rozhraní,
- periferií jako jsou myš, můstek pro tiskárny hostitele,
- ACPI (management napájení),
- paměti.

VM Tools zprostředkovávají kompatibilitu speciálních funkcí jako:

- posílání zpráv mezi hostovaným OS a hypervizorem,
- spouštění skriptů,
- integrace ukazatele myši,
- poskytování API,
- automatická úprava rozlišení obrazovky,

[7] OSP = Operating System Specific Package

- drag and drop,
- sdílení schránky,
- sdílení souborů.

Základem nainstalovaných VMware Tools je démon spouštěný při startu hostovaného systému. V různých systémech má různou podobu:

- vmtoolsd.exe ve Windows,
- vmware-tools-daemon v OS X,
- vmtoolsd v Linuxových, Unixových a FreeBSD systémech.

Distribuce VM

Virtuální stanice mohou být ve VMware distribuovány buď prostým zkopírováním souborů VM, tak pomocí exportu tzv. virtuální appliance do standardizovaného formátu OVA či OVF, případně mohou být staženy z virtualizačního serveru.

Nejjednodušším a funkčním řešením je komprimace složky VM do zip souboru a jeho následné zkopírování buď přímo do nového prostředí nebo na souborový server k pozdějšímu stažení. Toto řešení funguje v případě přenosu mezi VMware Player, Workstation a Fusion. Jeho výhodou je jednoduchost a zachování formátu VM bez nutnosti konverze - s tím je spojeno zachování všech nastavených parametrů VM, i těch, které jsou platné pouze pro VMware produkty. Nevýhodou je nemožnost otevřít VM v jiném hypervizoru než VMware.

Další možností je VM exportovat z formátu VMware do formátu OVF, což je otevřený formát pro virtuální stroje. OVF virtuální stroj je možné zabalit do jediného souboru OVA, který je pak možné snadno kopírovat nebo vystavit na souborový server ke stažení. Výhodou otevřeného formátu je přenositelnost mezi různými hypervizorovými platformami, např. z VMware Workstation do Oracle Virtual Box. Nevýhodou je ztráta některých konfiguračních parametrů specifických pro VMware produkty.

2 Analýza pro program BYOD v TCZ

Telefónica Czech Republic, a.s. je telekomunikační operátor v ČR se 100% vlastněnou dceřinou společností Telefónica Slovakia, s.r.o. Subjekt vznikl sloučením společností Český Telecom a Eurotel pod společnost Telefónica Czech Republic, a.s., vlastněnou finanční skupinou Telefónica, S.A. Řadí se mezi velké firmy s více než 5 000 zaměstnanci. Na konci roku 2013 koupila Telefónicu Czech Republic česká investiční skupina PPF. V době vzniku této práce docházelo postupně ke změnám ve vedení společnosti, jejím řízení a projektech. Tato práce je zasazena do prostředí podniku před převzetím skupinou PPF.

Telefonica Czech Republic, a.s. (dále TCZ) se rozhodla implementovat určité prvky programu BYOD. Projekty, které bezprostředně s BYOD souvisí, jsou Mobile Device Management pro správu mobilních zařízení, L2 Security pro řízení přístupu do vnitřní sítě a program BYOD pro notebooky. Autor práce je členem týmu, který projekt BYOD pro notebooky připravuje.

TCZ má správu IT outsourcovanou do externí firmy Telefónica Global Technology (TGT). Společnost TGT vznikla oddělením provozního IT útvaru od TCZ a oba právní subjekty spolu úzce spolupracují. Pro zjednodušení je v této práci pro společnost TGT užíván termín "IT oddělení".

Zaměstnanci TCZ stále častěji preferují svá oblíbená zařízení založená na různých platfomách (od Android a iOS tabletů po vlastní Windows, Linux nebo OS X notebooky). Tato zařízení používají k práci a připojují je do sítě. To znamená zvýšené bezpečnostní riziko, protože se jedná o neznámá zařízení, která nemusí odpovídat bezpečnostním požadavkům společnosti. Vzhledem k velikosti firmy a jejímu technologickému zaměření se jedná o přirozený vývoj, zaznamenaný ve firmách po celém světě. BYOD fenomén přináší novou výzvu, na kterou společnost TCZ reaguje.

2.1 Aktuální stav používání soukromých zařízení

Tato podkapitola naplňuje cíl - *2. Charakterizovat prostředí ve společnosti ve vztahu k projektu* - rozborem aktuálního stavu v oblasti připojených zařízení do vnitřní sítě. Zároveň i podporuje naplnění cíle - *4. Identifikovat a charakterizovat důvody k realizaci projektu* - vymezením stávajících rizik.

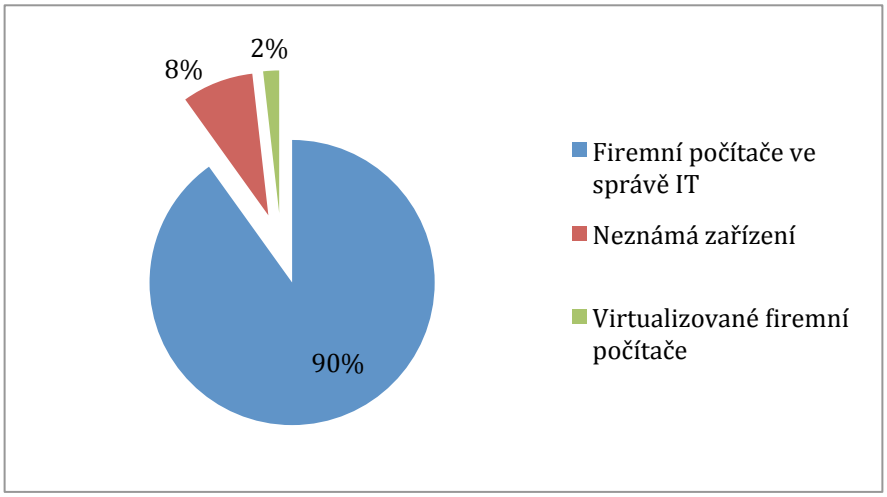
V TCZ se tak jako ve světě projevuje trend používání soukromých zařízení v práci. V současné době nemá TCZ cílená pravidla přímo pro BYOD. Používání soukromých zařízení se řídí obecnými pracovními předpisy, zejména bezpečnostním řádem.

IT oddělení a oddělení bezpečnosti pravidelně monitorují vnitřní síť společnosti a vyhodnocují data o připojených zařízeních, včetně detekovaných bezpečnostních událostí. Z nich vyplývá následující kapitola, která přibližuje stav používání soukromých zařízení v síti, využívání veřejných cloudových služeb a incidenty způsobené neznámými zařízeními.

Uvedené informace jsou uvedeny záměrně na nízké úrovni detailu z důvodu utajení citlivých údajů a v této práci slouží k obecnému přiblížení stavu ve společnosti.

2.1.1 Připojená soukromá zařízení

Na základě vyhodnocení dat pořízených při monitoringu sítě IT oddělením a oddělením bezpečnosti bylo zjištěno, že jsou v síti připojena neznámá zařízení. Ta nemusí znamenat zvýšené riziko, pokud se jedná o technologická zařízení mimo hlavní evidenci IT oddělení spravovaná v souladu s bezpečnostními pravidly. Dále se může jednat o testovací zařízení z různých projektů, případně zařízení externích pracovníků, která nejsou v evidenci IT. Část z identifikovaných neznámých zařízení tvoří i soukromá zařízení zaměstnanců (notebooky, tablety i mobily). Tato zařízení mohou znamenat zvýšené riziko pro bezpečnost sítě, protože není zajištěn jejich soulad s bezpečnostními pravidly. Za povšimnutí stojí v souvislosti s projektem BYOD pro notebooky i fakt, že IT oddělení identifikovalo významný počet virtualizovaného pracovního prostředí koncových stanic. Jedná se o pracovní prostředí, které bylo zvirtualizováno ze služebních notebooků a je používáno na neznámých zařízeních. Poměr zastoupení druhů zařízení přibližuje graf.



Obrázek 2-1-1-1: Počítače identifikované v síti TCZ. Zdroj: autor, z interních zdrojů TCZ.

Virtualizované firemní počítače jsou oblastí, pro kterou projekt BYOD pro notebooky vytvoří pravidla. Uživatelé těchto strojů budou mít vysokou motivaci vstoupit do BYOD programu.

Odhad rizika, plynoucího z neznámých zařízení je uveden v kapitole *2.4 Analýza bezpečnostních rizik*.

2.1.2 Přístup k veřejným cloudovým službám

Při monitorování aktivity na síti bylo zjištěno využívání veřejných webových služeb, které mohou sloužit jako úložiště souborů, sdílené různými zařízeními uživatele. Uživatel uloží data do cloudu ze služebního počítače a pak k nim přistupuje z tabletu nebo chytrého telefonu. Tato aktivita znamená zvýšené riziko pro důvěrnost informací. Přestože společnost TCZ uplatňuje bezpečnostní opatření, nelze se tomuto problému zcela vyhnout. Problém by pomohlo zmírnit zavedení BYOD pravidel nejen pro soukromé notebooky, ale i pro všechna soukromá zařízení.

2.1.3 Bezpečnostní incidenty neznámých zařízení

Ve společnosti byly zaznamenány bezpečnostní incidenty, které byly způsobeny z neznámých zařízení. Jejich detaily není možné kvůli ochraně interních informací podrobněji popsat. Přesto jejich existence a nezanedbatelný význam slouží jako další důvod pro zavedení cíleného programu pro BYOD zařízení.

2.2 Projekt BYOD pro notebooky

V době vzniku této práce byl v TCZ navržen koncept řešení pro projekt BYOD pro notebooky, který reaguje na vzrůstající zájem uživatelů používat soukromý notebook v práci a na rizika z neznámých zařízení ve vnitřní síti. BYOD je přirozený fenomén plynoucí z technologického vývoje na trhu mobilních zařízení a je třeba na něj reagovat. Cílem projektu je navrhnout jednoduché a bezpečné řešení, které nebude znamenat nutnost větších změn a zároveň poskytne zaměstnanci plnohodnotné pracovní prostředí i na jeho soukromém notebooku. Projekt zároveň musí znamenat provozní úsporu, aby sledoval strategii společnosti. Strategické cíle jsou přiblíženy v části *2.6 IT BSC pro projekt BYOD*.

Na projektu spolupracují zaměstnanci z oddělení informační bezpečnosti, sítí, IT provozu, lidských zdrojů a právního. Předkladatelem projektu je oddělení bezpečnosti, které přišlo s návrhem tohoto řešení.

Řešení je založeno na distribuované virtualizaci na platformě VMware Player/Fusion. Každý uživatel programu BYOD pro notebooky dostane BYOD VM s pracovním prostředím shodným, jako je na standardních služebních počítačích TCZ. Pro pracovní prostředí BYOD VM budou platit stejná pravidla, jako pro prostředí na počítačích TCZ.

Pro IT oddělení ani pro uživatele nepřináší řešení významné změny. IT oddělení bude spravovat stejné prostředí, jako spravuje doposud na služebních počítačích. Pouze s rozdílem, že prostředí bude provozováno virtuálně pod hypervizorem a ne přímo fyzicky na hardware. IT oddělení odpadá správa hardware, protože ten bude spravovat uživatel.

Z konzultace se zástupci IT oddělení vyplynulo, že životní cyklus VM bude shodný s životním cyklem pracovní stanice. Uživateli zůstanou díky shodnému prostředí stejné možnosti jako na služebním počítači. Hlavním rozdílem je to, že bude provozovat ve své režii hardware, hostitelský operační systém a hypervizor.

Díky oddělení soukromého a pracovního prostředí pomocí hypervizoru VMware je zachována vysoká úroveň bezpečnosti pro zaměstnance i firmu. Vyšší úrovně bezpečnosti je mimo jiné dosaženo bezpečnostními opatřeními popsanými v kapitole *4 Návrh VM* a organizačními opatřeními popsanými v kapitole *3 Návrh BYOD pro notebooky v TCZ*. Nutnou podmínkou je zabezpečení síťových prvků popsané v kapitole *2.3.1 L2 Security*, které zamezí přístupu z neznámého prostředí do vnitřní sítě a povolí do ní přístup pouze z pracovního prostředí.

Součástí projektu BYOD pro notebooky není zavedení celopodnikové strategie pro BYOD. Jedná se o projekt, který má rozvoj BYOD podporovat dílčím způsobem. Vzhledem k tomu, že zavedení BYOD pro notebooky nemůže sledovat globální BYOD strategii a IT strategii nebylo možné použít, je projekt navázán na obecné strategické programy přiblížené v kapitole *2.6 IT BSC pro projekt BYOD*.

Důvod výběru distribuované virtualizace

Místo ve světě častěji používané serverové virtualizace (VDI) byla pro doručení pracovního prostředí na BYOD notebooky vybrána virtualizace distribuovaná mimo jiné z důvodů:

- možné práce off-line,
- plnohodnotné náhrady služebního počítače,
- zachování současných pracovních postupů,
- odpadají investice do VDI a dalších serverů,
- nedojde k významnému nárůstu síťového provozu,
- virtualizaci už podporují i běžně dostupné notebooky.

Důvody výběru VMware Player/Fusion

Přestože má VMware řadu konkurentů, kteří nabízejí kvalitní alternativy (např. Parallels Desktop nebo Oracle VirtualBox), rozhodly o volbě VMware následující faktory:

- restricted mód VM[8],
- poskytovaná podpora,

[8] VM je chráněná proti zásahům uživatele. Podrobně je mód popsán v kap. *4 Návrh VM*.

- oddělení hostitelského a hostovaného systému,
- uživatelská přívětivost prostředí,
- kompatibilita s ostatními VMware platformami,
- spolupráce TCZ s VMware.

TCZ je partnerem VMware. Jeho produkty využívá na řadě svých serverů. Díky tomu je zajištěna podpora i možnost výhodnějších podmínek licencování.

2.3 Související projekty

V TCZ jsou dva další projekty, které úzce souvisí s projektem BYOD pro notebooky. Jedná se o L2 Security, který zamezuje přístupu neznámých zařízení do sítě a o projekt Mobile Device Management, který spravuje mobilní zařízení (chytré telefony a tablety) připojená k podnikovým IT službám.

Přestože všechny projekty svoji povahou spadají do BYOD programu, tak, jak byl nastíněn v kapitole *1.3 Trendy v BYOD*, nejsou zastřešeny jednotnou BYOD iniciativou a řídí se obecnými pravidly.

Tato podkapitola se podílí na naplnění cíle - *2. Charakterizovat prostředí ve společnosti ve vztahu k projektu* - tím, že identifikuje projekty, které s projektem BYOD bezprostředně souvisejí.

2.3.1 L2 Security

L2 Security je projekt, který s programem BYOD pro notebooky bezprostředně souvisí a je nutnou podmínkou k zavedení programu. Reaguje na rizika z připojování neznámých zařízení do vnitřní sítě a jeho cílem je zavedení povinné autentizace všech zařízení.

L2 Security pracuje s různými přístupovými kanály do vnitřní sítě (Wi-Fi, Ethernet, ...). Zavádí jasná pravidla pro povolování přístupu připojeného zařízení do vnitřní sítě pomocí protokolu 802.1x na síťových prvcích. Autentizace je možná buď pomocí zadání přístupových údajů nebo certifikátem.

V případě, že je do sítě připojen firemní počítač, který spravuje oddělení IT, síťové zařízení ho automaticky rozpozná a dovolí mu přistupovat do vnitřní sítě. V případě připojení zařízení, které nemá doménový účet, je pro přístup do sítě třeba zadat přístupové údaje ručně. V případě, že zařízení nebude identifikováno, je přístup do vnitřní sítě zablokován.

2.3.2 Mobile Device Management

Mobile Device Management (dále MDM) definuje (Keyes, 2013) jako soubor pravidel, činností a nástrojů, které jsou využity k bezpečnému a efektivnímu spravování mobilních zařízení firmy. MDM má za úkol formalizovat pravidla pro soukromá i firemní mobilní zařízení v pracovním prostředí a technologicky a procesně zajišťovat jejich správu. Obecně MDM zahrnuje podle (Keyes, 2013) činnosti jako jsou vzdálené ovládání a konfigurace, GPS lokalizace, instalace aplikací, nastavení politiky, logování, vzdálené uzamčení a vymazání obsahu a další.

S projektem BYOD pro notebooky nesouvisí tak úzce, jako projekt L2 Security. Průnik projektů BYOD pro notebooky a MDM je zejména v bezpečnostní politice. Větší část z obou projektů je však na sobě nezávislá.

2.4 Analýza bezpečnostních rizik

V průzkumech uvedených v kapitole *1.3 Trendy v BYOD* označili respondenti bezpečnost jako oblast, kterou jsou nejvíce znepokojeni. Vzhledem k tomu, že bezpečnostní aspekty jsou významnou oblastí, kterou je třeba se v souvislosti se zaváděním BYOD programu zabývat, byla provedena systematická analýza rizik.

Tato kapitola se významně podílí na naplnění cíle - *3. Vytvořit rámec pro projekt BYOD pro notebooky* - identifikací rizikových oblastí, na které je třeba se zaměřit. Dále na naplnění cíle - *4. Identifikovat a charakterizovat důvody k realizaci projektu* - kde kvalitativně porovnává úroveň rizik neznámých notebooků proti služebním a BYOD notebookům. Poznatky z této kapitoly jsou také využity při naplnění cíle - *5. vytvořit a otestovat model technického řešení BYOD pro notebooky* - návrhem bezpečnostních opatření.

Analýza rizik je inspirována metodikami CRAMM a ČSN ISO/IEC 27005:2009. Vychází z autorovy bakalářské práce (Pokorný, 2012) a má za cíl určit slabá místa použití BYOD notebooku, pro která je třeba navrhnout protiopatření. Dalším cílem analýzy rizik je ukázat, o kolik je potenciálně nebezpečnější neznámé zařízení používané zaměstnanci k práci, než použití BYOD notebooku, resp. řádně spravovaného služebního notebooku. Analýza rizik je provedena kvalitativně.

Na základě analýzy rizik jsou navržena protiopatření pro zmírnění nejvýznamnějších rizik BYOD notebooku na úrovni uživatele, hostitelského systému a konfigurace BYOD VM.

2.4.1 Identifikace aktiv

Jako první krok analýzy rizik byla provedena identifikace relevantních aktiv. Jako aktiva byla identifikována data a činnosti, které jsou provozovány na služebním notebooku, BYOD notebooku a na neznámém zařízení.

Uvažovanými aktivy jsou:

- lokálně uložená data (různého stupně klasifikace),
- lokální zpracování dat (texty, tabulky, databáze, ...),
- přístup k IT službám na síti, zejména:
    - využití komunikačních služeb (e-mail, kalendář, videokonference, ...),
    - přístup ke sdíleným datům (sdílené složky, databáze, intranet, ...),
    - přístup k informačním systémům (ERP, CRM, dohled a řízení sítě, ...).

Pro potřeby přípravy projektu BYOD je analýza rizik vypracována souhrnně pro všechny uvedené činnosti a data. Jsou seskupeny ve skupinách aktiv pro tři druhy notebooků. V případě potřeby je možné analýzu v budoucnu detailněji rozpracovat pro každou činnost na daném druhu notebooku.

Činnosti a data jsou jako aktiva uvažována ve všech třech případech ve stejné hodnotě. Stejně tak je hodnota hardware a software uvažována jako shodná u všech tří hodnocených variant. Z toho důvodu není hodnota aktiv v následující analýze rizik uvedena a je považována za konstantu.

Skupina aktiv: Služební notebook

Služební notebook je celý ve vlastnictví a správě podniku. Plní bezpečnostní požadavky dané interními předpisy. Uživatelé na něm mají omezená práva. Jeho obsah je šifrován a systém včetně aplikací je nastaven tak, aby byla zajištěna adekvátní úroveň bezpečnosti.

Skupina aktiv: BYOD notebook

Notebook je majetkem zaměstnance, který zajišťuje jeho správu a má k němu administrátorská práva. Za jeho zabezpečení a celkový soulad s interními předpisy zodpovídá zaměstnanec. Za zabezpečení a soulad s předpisy firemní BYOD VM provozované v notebooku zaměstnance zodpovídá IT oddělení. Aktuálně aplikovaná protiopatření jsou pro analýzu rizik uvažována pouze ta, která jsou implementovaná v pracovním prostředí BYOD VM spravovaném IT oddělením a jsou pevně daná.

Skupina aktiv: Neznámý notebook

Jedná se o neznámé zařízení, které je využíváno k práci bez vědomí zaměstnavatele. Nemusí odpovídat interním požadavkům ani nemusí být řádně zabezpečeno. Předpokládá se, že zařízení nemá implementovaná žádná bezpečnostní opatření.

2.4.2 Ohodnocení rizik

Hrozby jsou převzaty z číselníků CRAMM, který používá TCZ pro analýzu rizik. U hrozeb jsou popsány předpokládané dopady na jednotlivá aktiva. Detailní ohodnocení všech pravděpodobností a dopadů hrozeb je uvedeno v přílohách B.1, B.2 a B.3.

Pravděpodobnost (P) působení hrozby na aktivum je vyjádřena škálou 0 - 3, kde 0 znamená, že incident nemůže nastat, 1 je nízká pravděpodobnost, 2 střední a 3 je vysoká pravděpodobnost působení hrozby. Je určena odhadem autora a vychází z obecných zkušeností.

Dopad (D) je posuzován podle tzv. CIA modelu z pohledu narušení **dostupnosti**, **důvěrnosti** a **integrity**. Je ohodnocen na stupnici 0 - 3, kde 0 znamená, že hrozba nemá žádný dopad, 1 nízký dopad, 2 střední dopad a 3 vysoký dopad.

Riziko (R) vzniklé z působení hrozby na aktivum je vypočítáno podle následujícího vzorce:

$$R = P \times D$$

Obrázek 2-4-2-1: Obecný vzorec výpočtu rizika. Zdroj: (Pokorný, 2012).

Vzorec neuvádí hodnotu aktiva vzhledem k tomu, že aktiva jsou uvažována ve stejné hodnotě. Minimální hodnota rizika je 0, což znamená, že riziko je vyloučeno. Maximální hodnota, které může riziko nabývat je 9. Maximálními hodnoty značí velmi významná rizika, kterými je třeba se prioritně zabývat. Zmíněna jsou i významná rizika stupně 6. Kompletní výčet odhadovaných rizik je uveden v přílohách *B.1, B.2 a B.3 - Hodnocení rizik služebního, BYOD a neznámého notebooku*.

H1, H2, H3: Falšování uživatelské identity

Falšování uživatelské identity identifikovatelnou osobou, smluvními poskytovateli služeb nebo cizími osobami je pravděpodobnější u neznámého notebooku, který jako jediný nemá implementovaná opatření pro správu hesel. Nejvyšší potenciální dopady jsou na důvěrnost, kdy by útočník mohl získat přístup k lokálně uloženým datům. Méně významné dopady jsou z narušení integrity pro případ, že by útočník data neoprávněně pozměnil.

Riziko stupně 9 bylo odhadnuto v případě narušení důvěrnosti neznámého notebooku.

H4: Neoprávněné použití aplikace

Neoprávněné použití aplikace by mohlo mít střední dopad na důvěrnost, pokud by byly z aplikací vyčteny informace. Z hlediska dostupnosti neznamená hrozba významné riziko.

Neoprávněné použití aplikace nese srovnatelná rizika jak u služebního notebooku, tak u BYOD notebooku. Je pravděpodobnější u BYOD notebooku a neznámého notebooku, kde by mohl být použit nelegální software.

H5: Zavedení destruktivních a škodlivých programů

Zavedení malwaru je nejméně pravděpodobné u služebního notebooku, který má implementovaná ochranná opatření a většina uživatelů nemá administrátorská práva do OS. Vyšší pravděpodobnost je u BYOD notebooku, kde mají uživatelé hostitelský systém ve své správě. Nejvyšší pravděpodobnost zavedení škodlivých programů je u neznámého zařízení, které nemusí mít implementována žádná protiopatření a škodlivý kód se může volně šířit. Dopady na důvěrnost, dostupnost i integritu se mohou značně lišit. V analýze rizik jsou vzaty v úvahu nejvyšší možné dopady a tak mohou být dopady této hrozby vysoké.

Nejvyšší riziko ohodnocené stupněm 9 je u neznámého zařízení. Nižší riziko, přesto významné, na stupni 6 je u BYOD notebooku a zaslouží si pozornost.

H6: Zneužití systémových prostředků

Zneužití systémových prostředků má nejvyšší dopad na dostupnost, protože jejich zatížení může znamenat delší odezvu systému. V případě BYOD notebooku je zneužití systémových prostředků hrozbou, která stojí za povšimnutí, protože soukromé i pracovní prostředí se dělí o jedny systémové prostředky. Pokud by došlo k vyčtení obsahu paměti přidělené druhému prostředí, mohlo by dojít k narušení důvěrnosti či integrity.

Nejvyšší riziko 9 je vyhodnoceno u neznámého notebooku, kdy může být zneužitím systémových prostředků významně narušena dostupnost. Riziko stupně 6 u BYOD notebooku svědčí o tom, že je třeba se otázce sdílení systémových prostředků dále věnovat.

H7, H8, H9: Infiltrace, zachycení a manipulace komunikace

Infiltrace, zachycení a manipulace komunikace jsou hrozby, které dopadají na důvěrnost a případně i na integritu aktiv.

K infiltraci komunikace může dojít jak na síťovém rozhraní, tak mezi vstupními a výstupními zařízeními počítače. Příkladem možné infiltrace je v případě BYOD notebooku i odposlouchávání mezi hardwarovou vrstvou a hypervizorem - například instalací malware pro odchytávání vstupů (keyloggery apod.) - na hostitelský OS.

Významná rizika jsou vyhodnocena pro dostupnost BYOD notebooku z výše popsaného důvodu. U neznámého zařízení jsou rizika také významná. Služební notebook má proti hrozbě implementována technologická i procesní opatření, která riziko snižují.

H10: Odmítnutí odpovědnosti

Při odmítnutí odpovědnosti není původci možné dokázat, že učinil určitou akci. Uvažované dopady této hrozby jsou nízké a nepředstavuje významné riziko.

H11: Selhání komunikace

Selhání komunikace může způsobit nedostupnost IT služeb poskytovaných prostřednictvím sítě. Přesto řada činností a dat je přístupných i lokálně a proto není toto riziko ohodnoceno jako vysoké.

H12: Začlenění škodlivých programů

Začlenění škodlivých programů může mít vyšší dopady, než **H5: Zavedení škodlivých programů** a je hůře detekovatelné.

Rizika vyplývající z této hrozby jsou vysoká, u neidentifikovaných notebooků nejvyšší. U BYOD notebooku a služebního notebooku pak nižší z důvodu aplikovaných opatření ve firemním prostředí. Přesto je třeba u BYOD notebooku riziku věnovat pozornost, protože začlenění škodlivého kódu do hostitelského OS by mohlo znamenat vysoké dopady na bezpečnost aktiva.

H13: Chybné směrování

K chybnému směrování může například dojít odesláním dokumentu na jinou tiskárnu, nebo odesláním e-mailu na jinou adresu. Chybným směrováním je ovlivněna důvěrnost aktiva. Pravděpodobnost, že dojde k narušení důvěrnosti chybným směrováním je vyšší u neznámého notebooku, protože není možné určit pracovní postupy. Riziko plynoucí z chybného směrování není odhadnuto jako významné.

H14: Technická závada počítače

Z analýzy vyplývá, že technická závada nenaruší důvěrnost. Může ale narušit dostupnost a integritu. Nedostupnost vzniklá technickou závadou počítače je pravděpodobnější u neznámého notebooku než u služebního z důvodu, že neznámé zařízení nemá minimální požadavky na hardware a nevztahují se na něj pravidla pro správu zařízení.

H15: Technická závada paměťového zařízení

Technickou závadou paměťového zařízení mohou být ovlivněny zálohy uložené mimo notebook, případně aktuálně přenášená data. Ani jeden ze tří druhů notebooků není závislý na externích paměťových zařízeních, z toho důvodu je riziko z hrozby ohodnoceno jako méně významné.

H16: Technická závada tiskového zařízení

Technická závada tiskového zařízení neznamená pro činnosti a data uložená na noteboocích významná rizika.

H17, H18: Technická závada síťového distribučního prvku a síťové brány

Technická závada síťového distribučního prvku může způsobit nedostupnost některých IT služeb. Riziko, které z hrozby vyplývá, není hodnoceno jako významné.

H19: Technická závada počítače pro řízení/správu sítě

Pokud technická závada počítače pro správu sítě způsobí nedostupnost IT služeb poskytovaných po síti, jsou rizika stejná jako u hrozeb **H17** a **H18**.

H20: Technická závada síťového rozhraní

V případě technické závady síťového rozhraní budou nepřístupné síťové služby, tak jako při působení hrozeb **H17**, **H18**. Při závadě síťového rozhraní je možné použít jiný způsob připojení a tím zmírnit dopady (např. při poruše ethernetového rozhraní použít Wi-Fi nebo mobilní připojení s VPN). V případě poruchy na všech síťových rozhraních notebooku by pak dopady byly srovnatelné s dopady hrozeb **H17**, **H18**.

Rizika nejsou ohodnocena jako významná, tedy nižšími stupni než 6.

H21: Technická závada síťové služby

V případě technické závady síťové služby jsou odhadnuta rizika obdobně jako u hrozby **H17**, **H18**, protože budou nedostupná některá data a nebude možné provádět některé činnosti.

Rizika nejsou ohodnocena jako významná.

H22: Selhání napájení

Hrozba selhání napájení může mít dopady na dostupnost. Pravděpodobnost selhání napájení je snížena tím, že se ve všech třech posuzovaných případech jedná o notebook,

kde je zajištěn provoz na baterii. Větší pravděpodobnost dopadu na dostupnost je u delších výpadků napájení než 1 hodina. U všech hodnocených aktiv je riziko odhadnuto jako shodné.

Rizika plynoucí z této hrozby jsou nízká.

H23: Selhání klimatizace

V případě notebooku se jedná o selhání chlazení. Pravděpodobnost je při správném servisu nízká. Dopady hrozby mohou ovlivnit dostupnost, pokud by došlo k přehřátí a případně k fyzickému poškození.

Celkově z hrozby nevyplývá vysoké riziko.

H24: Selhání systémového nebo síťového programového vybavení

Selhání systémového nebo síťového programového vybavení je nejméně pravděpodobné v případě služebního notebooku, který prochází testováním. Vyšší pravděpodobnost selhání je v případě BYOD notebooku, kde dostupnost pracovního prostředí závisí na hostitelském i hostovaném operačním systému.

Nejvýznamnější dopady mohou být na dostupnost, případně na integritu. Nejvyšší riziko stupně 9 je ohodnoceno u neznámého notebooku, kde není dané, jaký systém je nainstalován. Významné riziko z hrozby vyplývá i pro BYOD notebook.

H25: Selhání aplikačního programového vybavení

Selhání aplikačního programového vybavení by mohlo mít vysoké dopady v případě selhání hypervizorové aplikace u BYOD notebooku. V takovém případě je celé firemní prostředí nedostupné. Selhání aplikací v pracovním prostředí BYOD VM i služebního notebooku mají stejná rizika. K selhání aplikací je potenciálně nejnáchylnější neznámé zařízení, které může mít nainstalované aplikace z neznámých zdrojů.

Riziko stupně 6 je odhadnuto u BYOD notebooku kvůli vysokým dopadům na dostupnost při selhání hypervizoru a riziko stupně 9 u neznámého notebooku.

H26: Provozní chyba

Provozní chyba je nejméně pravděpodobná u služebního notebooku, který má implementovanou řadu opatření. Z důvodu omezených uživatelských práv je menší pravděpodobnost i dopad případné provozní chyby. Vyšší pravděpodobnost a dopady jsou v případě BYOD notebooku, kdy má uživatel v hostitelském systému administrátorská práva a plný přístup k souborům BYOD VM. Stejně vysoká pravděpodobnost způsobení provozní chyby je i u neznámého notebooku.

Provozní chyba může být původcem rizika stupně 9 u BYOD notebooku i u neznámého zařízení z pohledu narušení dostupnosti, případně i integrity.

H27: Chyba údržby technického vybavení

Chyba údržby technického vybavení má potenciální vysoký dopad na dostupnost i důvěrnost. Nejnižší pravděpodobnost chyby údržby je v případě služebního notebooku, který je profesionálně spravován. Vyšší je pravděpodobnost chyby u BYOD notebooku, kde se o notebook starají sami uživatelé. Mohou například provádět některé opravy sami nebo je svěřovat neautorizovaným servisům.

Hrozba způsobuje nejvyšší riziko z narušení dostupnosti u BYOD notebooku a neznámého notebooku. V případě předání stroje nedůvěryhodnému servisu pak existuje i vysoké riziko z narušení důvěrnosti.

H28: Chyba úpravy programového vybavení

Nízké riziko z této hrozby plyne v případě služebního notebooku, kde nemá uživatel možnost zasahovat do programového vybavení. To je dodáváno IT oddělením a je důsledně testováno. Vyšší rizika jsou odhadnuta u BYOD notebooku, kde je možnost, že by uživatel mohl upravovat hostitelský OS a tím narušit zejména dostupnost případně i důvěrnost aktiv. V případě neidentifikovaného notebooku jsou rizika nejvyšší.

H29: Chyba uživatele

Chyba uživatele působí nejnižší rizika u služebního notebooku, kde jsou řízena uživatelská práva a zavedena opatření. Vyšší riziko plyne v případě BYOD notebooku, kde spravuje uživatel hostitelský OS a hypervizor. Zde může dojít k dopadům na dostupnost. Proti chybě uživatele je nejméně ochráněn neznámý notebook, kde není známa úroveň uživatelských oprávnění ani opatření. Z pohledu narušení dostupnosti je riziko BYOD notebooku i neznámého notebooku ohodnoceno jako významné.

H30: Požár

Pravděpodobnost i dopady požáru jsou u všech tří druhů notebooků srovnatelné. Výhodou je přenosnost notebooku, což snižuje pravděpodobnost jeho poškození požárem. V případě požáru mohou vzniknout vysoké dopady na dostupnost, přesto je riziko ohodnoceno jako méně významné kvůli nižší pravděpodobnosti.

H31: Poškození vodou

Poškození vodou může v případě notebooku nastat zejména v případě polití nebo neopatrné manipulace. U všech tří druhů notebooků je riziko srovnatelné a může znamenat dopady na dostupnost. Riziko je hodnoceno jako významné.

H32: Přírodní katastrofa

Riziko plynoucí z přírodní katastrofy je pro všechna aktiva srovnatelné. Celkově se pro definovaná aktiva nejedná o významné riziko.

H33: Nedostatek personálu

Nedostatkem personálu nebude významným způsobem bezpečnost aktiv narušena. Rizika nejsou hodnocena jako významná.

H34, H35: Krádež

Krádež provedená identifikovatelnými i neidentifikovatelnými osobami může mít významné dopady na důvěrnost lokálně uložených dat. V případě služebního notebooku jsou implementována opatření jako šifrování disku. V případě BYOD notebooku záleží na implementaci šifrování. Obsah virtuálního disku je chráněn pomocí stejných opatření, jako prostředí služebního notebooku. Nejvyšší riziko stupně 9 je u dostupnosti u neznámého zařízení, které nemusí mít implementováno šifrování dat. Pravděpodobnost krádeže notebooku je ohodnocena jako střední, případné dopady z narušení dostupnosti a důvěrnosti mohou být u neznámého a BYOD notebooku vysoké.

H36, H37: Úmyslné poškození osobami

Úmyslné poškození osobami je ve všech třech případech stejně ohodnocené. Může znamenat významnější riziko pro dostupnost aktiva.

H38: Terorismus

Hrozba terorismu proti koncovému zařízení je nepravděpodobná a neznamená významné riziko pro uvažovaná aktiva.

Závěr analýzy rizik

Analýza rizik ukázala, že ke služebnímu notebooku se v některých aspektech váží nižší rizika, než k BYOD notebooku. Je to z důvodu nižší zranitelnosti řešení (firemní prostředí běží přímo na hardware a ne v hostitelském OS, je kompletně spravován IT oddělením, ...).

Potenciál takto provedené analýzy rizik je ve vytipování kritických oblastí bezpečnosti používání BYOD notebooku a v porovnání rizik služebního notebooku, BYOD notebooku a neznámého zařízení systematickým způsobem.

Výstupem této analýzy nejsou finančně ohodnocené dopady. Možné je provést ohodnocení aktiv, výpočet nákladů na jejich obnovení do původního stavu, případně přidat možné sankce vyplývající ze zákona. Kvantitativně provedená analýza rizik by byla dalším prostředkem, jak obhájit realizaci projektu BYOD. Provedená kvalitativní analýza rizik je prvním krokem k vytvoření analýzy kvantitativní.

Rizika **služebního notebooku**, jako souboru aktiv (data, činnosti, hodnota hardware a software) se ukázala být z hodnocených druhů notebooků nejnižší. V analýze byla rizika ohodnocena z pohledu **důvěrnosti** na 56 bodů (riziko stupně 6 bylo odhadnuto pouze u hrozby začlenění škodlivých programů), z pohledu **dostupnosti** na 120 bodů (riziko stupně 6 bylo odhadnuto u hrozby krádeže a různých druhů poškození) a z pohledu zachování **integrity** na 69 bodů, kdy riziko stupně 6 bylo vypočítáno u hrozeb škodlivých programů, manipulace komunikace a u chyby uživatele.

Rizika **BYOD notebooku** byla ohodnocena na 70 bodů u narušení **důvěrnosti** (125 % rizik služebního notebooku), 142 bodů u narušení **dostupnosti** (118 % rizik služebního notebooku) a 78 bodů u narušení **integrity** (113 % rizik služebního notebooku). Rizika jsou vyšší než u služebního notebooku i z důvodu, že nebyla započítána bezpečnostní opatření jiná, než realizovaná v BYOD VM. Těmto rizikům se podrobněji věnuje následující kapitola.

Rizika **neznámého notebooku** byla zahrnuta do porovnání pro ilustraci toho, o kolik vyšší míra je stanovena oproti BYOD notebooku, případně oproti notebooku služebnímu. V oblasti narušení **důvěrnosti** byla rizika odhadnuta na 126 bodů (225 % rizik služebního notebooku), u narušení **dostupnosti** na 166 bodů (138 % rizik služebního notebooku) a u narušení **integrity** na 100 bodů (145 % rizik služebního notebooku).

Za povšimnutí stojí výše rizik z narušení důvěrnosti neznámého notebooku, která je 2,25 násobkem odhadnutých rizik služebního notebooku. V případě, že by na takovém zařízení byla uložena cenná nebo citlivá data, bylo by riziko ještě umocněno jejich hodnotou. To je jeden z důvodů pro potlačování používání neznámých zařízení a prosazování BYOD programu.

Je třeba dodat, že analýza rizik vychází z názoru autora a uvedené hodnoty slouží k porovnání odhadované výše rizik mezi služebním, BYOD a neznámým notebookem.

2.4.3 Významná rizika BYOD notebooku

K rizikům, která byla ohodnocena stupni 9 a 6 jsou navrženy kroky k jejich řízení. Obecné kroky, které je možné pro práci se zjištěnými riziky zvolit jsou:

- akceptace rizika,
- přenesení odpovědnosti,
- přijetí protiopatření ke zmírnění rizika,
- vyhnutí se riziku.

Pozornost je věnována možným protiopatřením ke zmírnění rizika.

Nejvýznamnější rizika

Hrozby **H5 a H12: Zavedení (začlenění) škodlivých programů** byly ohodnoceny, jako významné riziko, které může mít dopady na dostupnost, důvěrnost i integritu BYOD notebooku. V případě BYOD notebooku je třeba před škodlivým kódem chránit jak firemní, tak hostitelské prostředí spravované uživatelem.

Pro snížení rizik z této hrozby je vhodné zavést povinnost uživatelů BYOD používat v hostitelském prostředí bezpečnostní software, aktualizovat operační systém, dodržovat bezpečnostní zásady správy počítače a podobně. Dalším aplikovatelným opatřením je pravidelné školení a testování uživatelů BYOD na správu BYOD notebooku. Zabezpečení firemního prostředí v BYOD VM je na dostatečně vysoké úrovni.

Další velmi významné riziko způsobuje hrozba **H26: Provozní chyba**. BYOD notebook je k této hrozbě více zranitelný z důvodu správy hostitelského prostředí uživatelem. K provozní chybě může dojít jak na úrovni hostitelského systému, tak na úrovni správy hypervizoru, nebo při manipulaci se soubory BYOD VM. Provozní chyba může mít dopady na dostupnost systému.

Riziko z provozní chyby může být sníženo zavedením školení a testování uživatelů, nastavením základních pravidel pro konfiguraci hostitelského prostředí, nebo dalším zvyšováním kvalifikace uživatelů a poskytnutím znalostní báze k jejich dalšímu vzdělávání.

Další významná rizika

Riziko plynoucí z hrozeb **H7, H8: Infiltrace, zachycení a manipulace komunikace** je ohodnoceno jako významné z důvodu možných dopadů na důvěrnost a integritu. V případě BYOD notebooku existuje zvýšené riziko, že v případě infiltrace hostitelského systému

bude zachycena komunikace mezi systémovými prostředky počítače a hypervizorem. Může se jednat o přístup k paměti, zachytávání kláves nebo obrazu.

Aplikovatelná protiopatření jsou identická s opatřeními proti hrozbám H5 a H12 popsaná mezi nejvýznamnějšími riziky.

Riziko způsobené hrozbou **H27: Chyba údržby technického vybavení** může mít vliv na dostupnost i důvěryhodnost aktiv. Může být způsobeno neodbornými servisními zásahy nebo svěřením stroje do nedůvěryhodného servisu.

Opatřením je vzdělávání uživatelů BYOD a stanovení pravidel pro bezpečný servis BYOD notebooků (např. při předávání zařízení do servisu v něm nenechávat paměťová zařízení a pevné disky, pokud to není nutné a podobně).

Riziko způsobené hrozbami **H24, H25: Selhání systémového, síťového nebo aplikačního vybavení** je zvláště významné u BYOD notebooku, u kterého je funkčnost pracovního prostředí zcela závislá na hypervizorové aplikaci a hostitelském operačním systému. Nejvýznamnější riziko hrozí z nedostupnosti.

Možnými opatřeními je školení uživatelů, kontrola souladu hostitelského systému s pravidly, aktualizace systému a hypervizoru a testování.

Riziko, které způsobují hrozby **H34, H35: Krádež** může významně působit na důvěrnost. Oproti služebnímu notebooku je zde kromě fyzického odcizení celého stroje i možnost odcizení celého stroje pouhým vykopírováním souborů BYOD VM. To za sebou nemusí zanechat zřetelné stopy a tak o krádeži nemusí oběť ani vědět. Krádež může být provedena buď fyzickým přístupem ke stroji, nebo i na dálku.

Opatření, která je možné pro zmírnění dopadů hrozby aplikovat, jsou zejména školení uživatelů na bezpečnostní postupy při správě a používání BYOD VM, šifrování BYOD VM, uplatňování managementu hesel, chránit stroj před přístupem nedůvěryhodných osob, zabezpečení a aktualizace hostitelského OS.

BYOD notebook je srovnatelně náchylný k hrozbám **H31, H36, H37: Poškození**, jako služební notebook. Hrozba polití vodou má relativně vysokou pravděpodobnost i dopady a proto je zde uvedena. V případě úmyslného poškození může být riziko i vyšší, než u služebního, protože BYOD notebook je používán také k soukromým účelům a tak může být této hrozbě častěji vystavován.

2.5 Průzkum mezi zaměstnanci

Pro ověření zájmu o program BYOD pro notebooky a zjištění rámcových představ zaměstnanců je připraven průzkum, který bude proveden mezi uživateli firemních počítačů. Připravený dotazník je návrhem, který slouží jako podklad pro vytvoření celopodnikové ankety mezi uživateli. Pro přiblížení situace v TCZ a vyzkoušení návrhu dotazníku byl proveden předběžný průzkum na malém vzorku uživatelů.

Realizace předběžného průzkumu pomáhá naplňovat cíl práce - *2. Charakterizovat prostředí ve společnosti ve vztahu k projektu* - tím, že předkládá postoje skupiny potencionálních uživatelů a formuje podobu průzkumu pro celou organizaci.

2.5.1 Podoba dotazníku

Úvod

BYOD "Bring Your Own Device" je vzrůstajícím trendem, který znamená, že si zaměstnanci nosí svá soukromá zařízení (jako jsou notebooky, smartphony, tablety) do firemního prostředí a využívají je k práci.

Průzkum zjišťuje zájem uživatelů používat soukromý notebook pro soukromé i pracovní účely místo firemního notebooku nebo desktopu za měsíční příspěvek od zaměstnavatele.

Uživatelům BYOD bude nabídnuta možnost používat soukromé notebooky jako plnohodnotnou alternativu ke služebním počítačům. Bude k tomu využito řešení distribuce virtuálních strojů na koncová zařízení pomocí aplikace VMware Player (Fusion). Virtuální stroj obsahuje kompletní pracovní prostředí, shodné se služebními počítači (korporátní Windows 7, Office, korporátní aplikace dostupné ve služebních počítačích). Na soukromém notebooku se spouští virtuální stroj jako aplikace, která běží zcela odděleně od ostatních programů. Podporované operační systémy soukromých notebooků jsou Windows, OS X i Linux.

Za celkovou funkčnost (HW, aktuální operační systém včetně zabezpečení) soukromého notebooku budou zodpovídat sami uživatelé. Zajistí soulad notebooku s požadavky a servis pro případ poruchy. Funkčnost virtuálního stroje bude zajišťovat zaměstnavatel.

Pokládané otázky

1. Uvítali byste možnost pracovat na vlastním oblíbeném notebooku a používat ho pro soukromé i pracovní účely?
2. Souhlasíte s tvrzením, že byste si soukromý notebook stejně pořídili i bez programu BYOD?
3. Považujete se za uživatele, který zvládne svůj notebook spravovat sám? (např. zajistit aktualizovaný operační systém a antivir, zajistit servis notebooku nebo nainstalovat a nastavit aplikaci podle dodaných obrázkových návodů)
4. Je pro Vás zajímavé využít v případě poruchy soukromého notebooku možnost zapůjčení firemního notebooku zdarma s pozastaveným vyplácením příspěvku po dobu opravy?
5. Jak vysoký měsíční příspěvek by pro Vás byl dostatečnou finanční motivací pro vstup do programu? (uveďte částku v Kč)

Možnosti odpovědí

Otázky 1 - 4 mají odpovědi:

- Ano.
- Nevím/nedokáži se rozhodnout.
- Ne.

Otázka 5 má odpověď pomocí číselné hodnoty.

Distribuce dotazníku a sběr dat

Dotazník byl v rámci předběžného průzkumu distribuován pomocí e-mailu vybrané skupině 32 respondentů e-mailem ke zjištění prvotních ohlasů na projekt BYOD pro notebooky.

Všem potencionálním uživatelům BYOD (přes tisíc zaměstnanců) bude po úpravách dotazník zpřístupněn na intranetu. Zaměstnanci se o dotazníku dozví díky informačním e-mailům, které bude rozesílat oddělení lidských zdrojů. Při sbírání odpovědí bude zaznamenán otisk zařízení, aby bylo možné zjistit, zda respondent vyplnil dotazník z chytrého telefonu, tabletu nebo počítače, případně z jakého operačního systému a prohlížeče. To bude sloužit jako doplňující informace, kolik respondentů již využívá nějakou formu BYOD.

2.5.2 Vyhodnocení

Na předběžný průzkum odpovědělo 32 zaměstnanců společnosti TCZ. Byli vybráni z technologických i netechnologických oddělení. Přibližně polovinu tvořili stálí zaměstnanci a polovinu studenti a absolventi vysokých škol z programu Talentum.

Otázka 1: Využití soukromého notebooku pro práci

Z výsledků vyplývá, že 59 % respondentů má zájem využívat soukromý notebook pro pracovní účely. Z námětů, které zaměstnanci k odpovědím připojili, vyplynulo, že někteří již soukromý notebook pro práci používají a uvítali by oficiální zavedení BYOD programu. Dále se ukázalo, že veliký přínos by BYOD pro notebooky měl pro studenty Talentum programu, kteří podle současných pravidel mají nárok pouze na firemní desktop, přestože řada z nich pracuje i mimo kancelář. Ti by možnost oficiálně používat soukromý notebook k práci využili.

Oproti tomu 22 % respondentů by pro práci soukromý notebook využívat nechtělo.

Otázka 2: Pořízení soukromého notebooku i bez BYOD

Tato otázka nepřímo zjišťovala, zda již zaměstnanci soukromý notebook mají, případně zda plánují jeho zakoupení. Zde odpovědělo kladně celých 78 %.

Někteří respondenti u dotazníku uvedli, že by si v případě pořízení notebooku pro soukromé i pracovní účely pořídili výkonnější hardware, než kdyby si notebook pořizovali pouze pro soukromé použití.

O pořízení soukromého notebooku neuvažovalo pouze 15 % respondentů.

Otázka 3: Schopnost spravovat vlastní notebook

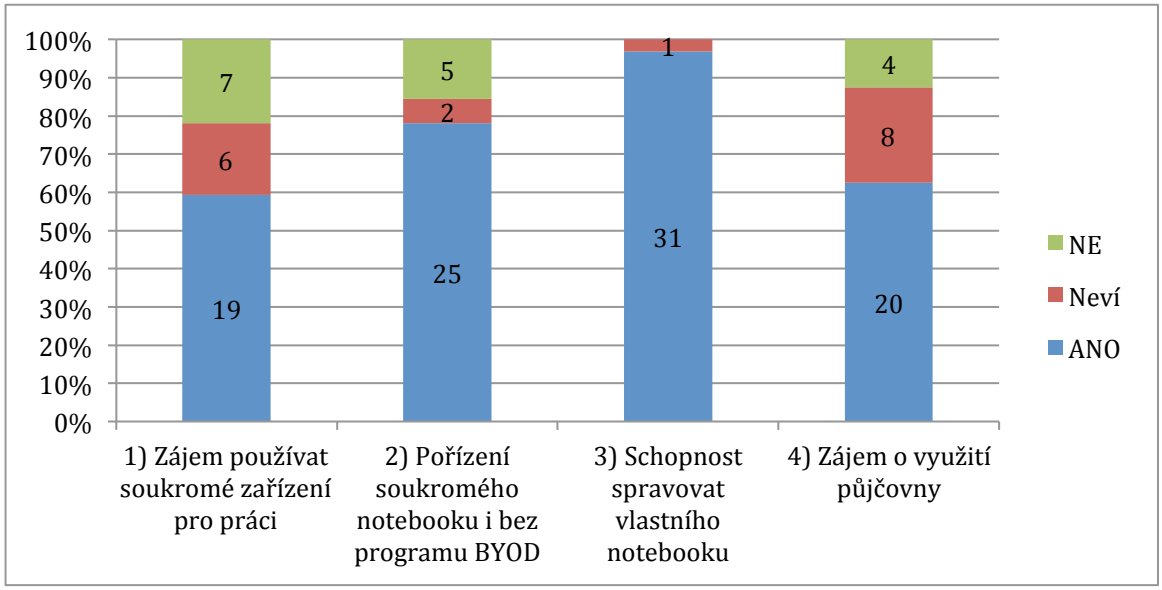
O své schopnosti spravovat vlastní notebook podle dodaných návodů a instrukcí jsou přesvědčeni téměř všichni respondenti, tj. 97 %. To dokládá vysoké přesvědčení uživatelů o vlastní počítačové gramotnosti. Schopnosti uživatelů spravovat vlastní zařízení jsou jedním z hlavních předpokladů pro zavedení programu BYOD. Pouze 3 % uživatelů neví, zda by bylo schopno svůj počítač spravovat, případně by potřebovalo více informací pro poskytnutí jasné odpovědi.

Otázka 4: Zájem o využití půjčovny notebooků

Na otázku odpovědělo 25 % respondentů, že nejsou schopni se v danou chvíli rozhodnout ani pro jednu možnost. To může mimo jiné ukazovat na chybné položení otázky, případně poskytnutí mála jasných informací respondentům ke zformování názoru.

Přes polovinu respondentů (63 %) uvedlo, že by pro ně bylo zajímavé využít v případě poruchy BYOD notebooku služby firemní půjčovny. Pro 12 % respondentů by pak využití půjčovny nemělo smysl. Například z důvodu, že mají náhradní soukromý notebook, který by mohli po přechodnou dobu používat. Dalším důvodem nezájmu může být samotný fakt, že o program BYOD neměli respondenti odpovídající negativně zájem.

Počet odpovědí na otázky 1 - 4 shrnuje následující graf.

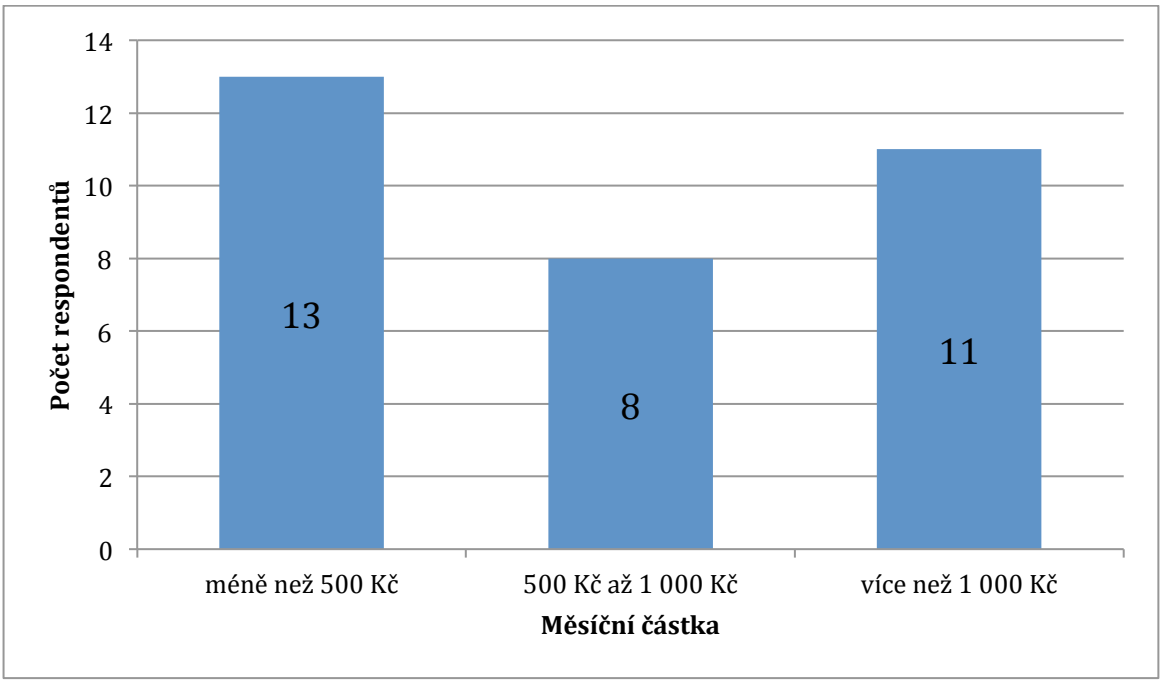


Obrázek 2-5-2-1: Výsledky předběžného průzkumu BYOD. Zdroj: autor.

Otázka 5: Představa výše měsíčního příspěvku

Odpovědi na otázku představy výše měsíčního příspěvku se mezi respondenty značně rozcházely. Bylo to z důvodu velké otevřenosti otázky. Uživatelé tak mohli napsat libovolnou částku, která se ani nemusela opírat o realitu.

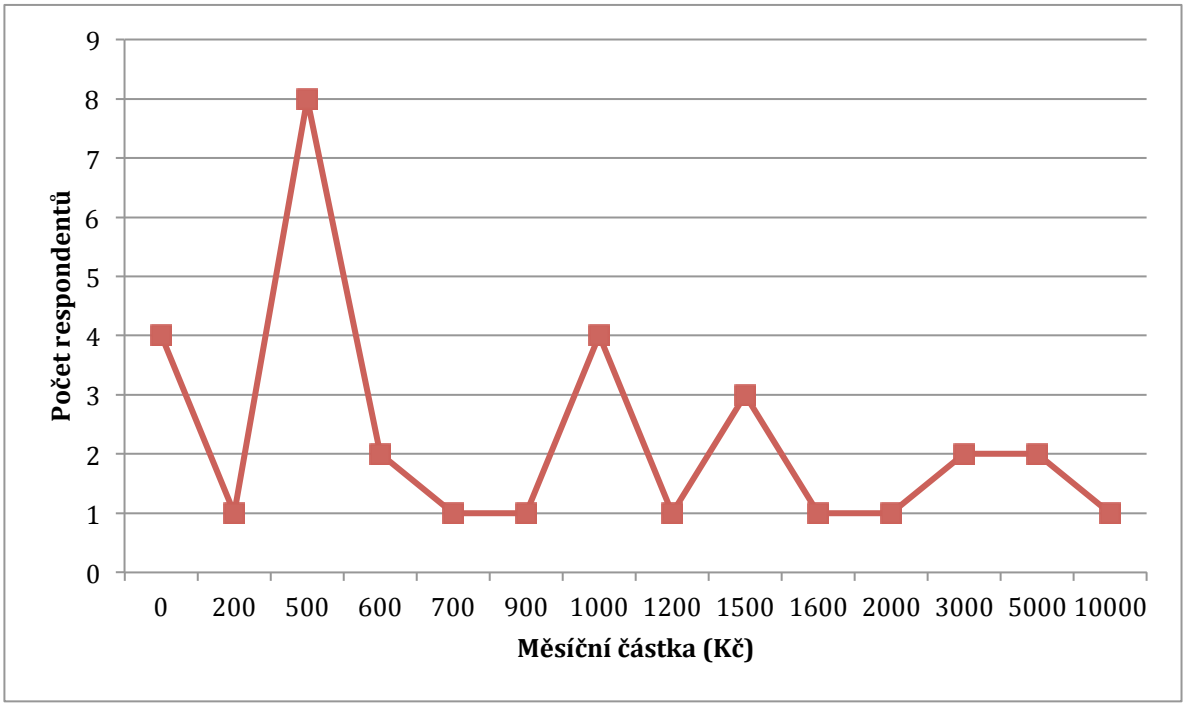
Celková částka vypočítaná aritmetickým průměrem by byla 1 447 Kč. To je z důvodu započítání i extrémně vysokých představ. Více vypovídající je mediánová částka, která činí 700 Kč měsíčně. Modus souboru představovaných částek je 500 Kč, který by jako motivace ke vstupu do BYOD programu pro notebooky postačoval 25 % respondentům.



Obrázek 2-5-2-2: Pásma představy měsíčního příspěvku. Zdroj: autor.

Pokud odpovědi rozdělíme na pásma do 500 Kč včetně, více než 500 Kč a do 1 000 Kč včetně a více než 1 000 Kč, pak v prvním pásmu do 500 Kč je nejvíce respondentů, a to 41 %. Ve druhém pásu mezi 500 Kč a 1 000 Kč je 25 % respondentů a ve třetím pásmu celých 34 % uživatelů. To ilustruje graf na začátku této stránky.

Četnost představovaných výší měsíčního příspěvku ukazuje následující graf.



Obrázek 2-5-2-3: Představa výše měsíčního příspěvku. Zdroj: autor.

Závěr z průzkumu

Z provedeného předběžného průzkumu vyplývá přesvědčení uživatelů o tom, že jsou schopni svůj soukromý notebook spravovat sami. Je to dáno jak vysokým počtem oslovených studentů a absolventů, kteří s výpočetní technikou vyrostli, tak i technologickou orientací společnosti TCZ. Lze usuzovat, že uživatelé budou schopni s vhodně vytvořenou znalostní bází BYOD svá zařízení spravovat. Pro další průzkum bude vhodné detailněji rozepsat požadované znalosti pro správu BYOD notebooků do více otázek.

Pro projekt BYOD pro notebooky je přínosné, že 78 % dotázaných má nebo plánuje pořídit soukromý notebook. Pokud by splňoval minimální požadavky, je tento faktor významnou motivací pro vstup zaměstnance do BYOD programu.

Ochotu využít soukromý notebook k práci projevilo 59 % respondentů. Bylo by vhodné, kdyby mělo zájem více, přesto je toto procento relativně vysoké a pokud by se udrželo i v hlavním projektovém průzkumu, znamenalo by to pro projekt vysoký potenciál. Zajímavá by byla informace, kolik respondentů již soukromý notebook k práci využívá. Dá se předpokládat, že mezi zaměstnanci, již využívajícími soukromé notebooky k práci by byla ke vstupu do programu BYOD největší vůle. Významnou roli zde hraje skutečnost, že by došlo k legalizaci zavedeného postupu.

Rozdílné představy o výši měsíčního příspěvku zaměstnavatele pro provoz soukromého notebooku nejsou v tuto chvíli směrodatné, protože se respondenti rozhodovali s minimem informací. Přesto modus 500 Kč a medián 700Kč by mohly být vhodným kompromisem jak pro firmu, tak pro zaměstnance.

2.6 IT BSC pro projekt BYOD

IT Balanced Scorecard je strategický rámec, který pomáhá naplňovat cíle organizace pomocí kaskádování strategických cílů na nižší útvary. IT BSC, kterou používá i (Keyes, 2013) je odvozena od BSC, kterou publikovali Robert S. Kaplan a David P. Norton v knize The Balanced Scorecard: Translating Strategy into Action roku 1996 (Kaplan, 2005).

IT BSC přebírá čtyři základní perspektivy BSC (Keyes, 2013) - Finance, Zákazník, Interní procesy a Učení se a růst. Každá perspektiva nahlíží na věc z úhlu dané zainteresované strany. V případě IT jsou ve finanční dimenzi zobrazeny finanční cíle, které slouží zejména ředitelům útvarů a finančnímu oddělení. Dále zákaznické cíle, přinášející přidanou hodnotu uživatelům služeb poskytovaných IT oddělením. Vnitřní procesy přináší přínosy IT oddělení ve formě zefektivnění a zdokonalení jeho vlastních procesů. Učení se a růst pak slouží jak zaměstnancům IT oddělení, tak může mít v případě programu BYOD i přesah mezi ostatní zaměstnance firmy.

IT BSC kaskádově navazuje na strategii nadřízených útvarů. Pomocí své vize a cílů rozvíjí strategii celé organizace a transformuje ji do IT oblasti. Princip IT BSC je možné díky vysoké flexibilitě rámce BSC využít při nastavování cílů a metrik projektu. BSC pomáhá zajistit, že projektové cíle jsou nastaveny tak, aby sledovaly strategické cíle IT oddělení i cíle globální. BSC je vhodné použít zejména v projektech většího rozsahu, které se projeví na fungování celé organizace. Takovým projektem je i zavádění BYOD programu.

Hlavními výhodami použití IT BSC při řízení projektu je:

- provázání cílů a přínosů pro zainteresované strany (stakeholdery),
- sledování jednotné vize a mise,
- komunikace cílů s okolím,
- podpora při řízení přínosů.

BSC je rámcem, který prochází fázemi vývoje a je nutné ho pravidelně vyvíjet a revidovat (Kaplan, 2005). To platí i při použití metody BSC v projektu. Model IT BSC, který vznikl pro sledování cílů projektu BYOD pro notebooky je platný pro výchozí stav při zahájení projektu. S postupujícím projektem ho bude třeba upravovat podle nových skutečností. Upravovány mohou být jak cíle, tak metriky, případně jejich cílové hodnoty či iniciativy. Prováděné úpravy je třeba zdůvodnit a zdokumentovat.

Použití IT BSC je pro projekt BYOD pro notebooky výhodné také z důvodu, že umožňuje sledovat i nefinanční přínosy. Těch BYOD pro zaměstnaneckou perspektivu a perspektivu učení se a růstu přináší veliké množství.

Tato kapitola významným způsobem naplňuje cíl - *4. Identifikovat a charakterizovat důvody k realizaci projektu* - zmapováním cílů projektu BYOD, které pomohou naplnit strategické cíle organizace. Popsané cíle a metriky pak slouží jako východisko při naplnění cíle - *3. Vytvořit rámec pro projekt projekt BYOD pro notebooky*.

2.6.1 Globální strategie TCZ

Skupina Telefónica formuje strategie, které přebírají její dceřiné společnosti, včetně TCZ. V současnosti má TCZ několik strategických programů, které jsou naplňovány dílčími projekty.

Programy se mimo jiné zabývají snižováním provozních nákladů, zvyšováním rychlosti interních procesů, spokojeností zákazníka, snižováním rizik či zvyšováním efektivity ve smyslu včasného, kvalitního a spolehlivého dodání služeb. Společnost podporuje inovace, kreativitu a každodenní využívání nejmodernějších technologií svými zaměstnanci.

Strategické cíle je možné shrnout do následujících bodů.

- Cíl S1: Zvýšení provozní efektivity.
- Cíl S2: Zrychlení interních procesů.
- Cíl S3: Zvýšení zákaznické spokojenosti.
- Cíl S4: Snížení provozních nákladů.
- Cíl S5: Zvýšení kvality zaměstnanců.

Cíl S3: Zvýšení zákaznické spokojenosti může znamenat buď spokojenost zákazníka společnosti TCZ nebo spokojenost interního zákazníka uvnitř TCZ. Pro účely této IT BSC se vždy jedná o spokojenost interního zákazníka (zaměstnance).

Mezi provozní náklady se řadí i náklady na podporu uživatelů, které může projekt BYOD snížit. Projekt BYOD má dále potenciál snižovat objem výkonů IT oddělení na správu hardware a je i trvale udržitelnou změnou, kterou je možné rozšiřovat napříč společností.

Cíle programu BYOD pro notebooky jsou navrženy tak, aby pomáhaly globální strategické cíle vhodným způsobem naplňovat.

2.6.2 Návrh IT BSC pro projekt BYOD

Vize a mise projektu

Projekt BYOD pro notebooky má vizi umožnit uživatelům pracovat na soukromých noteboocích stejně dobře nebo lépe, než na služebních počítačích. K tomu vytvoří

uživatelům takové podmínky, že volba soukromého notebooku místo služebního počítače bude pro uživatele odpovídající alternativou.

Návrh cílů a metrik

Cíle projektu BYOD sledují strategické cíle společnosti TCZ, uvedené v předchozí kapitole. Na strategické cíle S1 - S5 jsou u projektových cílů uvedeny odkazy.

Cíle a metriky částečně vycházejí z (Keyes, 2013), kde je v příloze Balanced Scorecard Metrics uvedena řada modelových metrik a cílů IT BSC použitelných pro program BYOD. Další cíle jsou inspirovány obecnými cíli BSC z (Kaplan, 2005) a některé cíle byly navrženy přímo autorem.

Finanční perspektiva

Finanční cíle jsou navrženy tak, aby znamenaly úspory pro IT oddělení, případně pro celou společnost. Příjemcem přínosů z těchto cílů jsou zejména osoby odpovědné za rozpočet IT oddělení. Všechny finanční přínosy vedou ke snížení nákladů.

Tabulka 2-6-2-1: IT BSC - cíl FIN 1. Zdroj: autor.

Zkratka cíle:	**FIN 1**
Název cíle:	**Snížení nákladů na dodání pracovního prostředí uživateli.**
Měřítka:	Výše nákladů na dodání pracovního prostředí.
Záměry:	Snížení o 5 % proti současnému stavu.
Iniciativy:	BYOD VM budou distribuovány automaticky a po síti.
Strateg. cíle:	Cíl S4

Tabulka 2-6-2-2: IT BSC - cíl FIN 2. Zdroj: autor.

Zkratka cíle:	**FIN 2**
Název cíle:	**Snížení nákladů na obnovu desktopů a notebooků.**
Měřítka:	Výše nákladů na obnovu desktopů a notebooků. Počet desktopů a notebooků.
Záměry:	Snížit náklady na obnovu nejméně o 10 %. Snížit stav o 500 zařízení v oběhu.
Iniciativy:	Uživatelé BYOD programu vymění služební počítač za BYOD VM.
Strateg. cíle:	Cíl S4

Tabulka 2-6-2-3: IT BSC - cíl FIN 3. Zdroj: autor.

Zkratka cíle:	**FIN 3**
Název cíle:	**Snížení celkových nákladů na správu a servis notebooků a desktopů.**
Měřítka:	Celkové náklady na správu a servis služebních notebooků a desktopů.
Záměry:	Snížení nákladů o 5 %.
Iniciativy:	Zavedení BYOD pro notebooky. IT nebude poskytovat podporu pro BYOD hardware. BYOD VM budou distribuovány po síti a ne fyzicky. BYOD VM budou spravovány pouze vzdáleným připojením po síti.
Strateg. cíle:	Cíl S4

Tabulka 2-6-2-4: IT BSC - cíl FIN 4. Zdroj: autor.

Zkratka cíle:	**FIN 4**
Název cíle:	**Zvýšení produktivity zaměstnanců.**
Měřítka:	Nárůst vykonané práce mimo běžnou pracovní dobu. Zvýšení kapacity personálních zdrojů při stejném počtu zaměstnanců.
Záměry:	Udržet práci mimo pracovní dobu mezi 3 - 7 hodinami týdně. Zvýšit objem práce vykonané jedním zaměstnancem o 10 %.
Iniciativy:	Zavedením BYOD pro notebooky zvýšit mobilitu a flexibilitu zaměstnanců.
Strateg. cíle:	Cíl S1

Tabulka 2-6-2-5: IT BSC - cíl FIN 5. Zdroj: autor.

Zkratka cíle:	**FIN 5**
Název cíle:	**Snížení finančních dopadů rizika z neznámých zařízení na síti**
Měřítka:	Finanční dopady analyzovaných rizik vyplývajících z připojení neznámých zařízení do vnitřní sítě.
Záměry:	Snížení finančních dopadů analyzovaných rizik o 80 %.
Iniciativy:	Propojení BYOD pro notebooky s projektem L2 Security. Zavedení BYOD pro notebooky. Vzdělávání BYOD uživatelů.
Strateg. cíle:	Cíl S1

Zákaznická perspektiva

Zákaznická perspektiva shrnuje cíle, které přinesou užitek BYOD uživateli.

Tabulka 2-6-2-6: IT BSC - cíl ZAK 1. Zdroj: autor.

Zkratka cíle:	**ZAK 1**
Název cíle:	**Nízký počet chyb při instalaci a používání VM**
Měřítka:	Poměr měsíčního počtu incidentů hlášených na helpdesk vztažený k celkovému počtu uživatelů BYOD.
Záměry:	Udržení poměru měsíčního počtu incidentů na počet uživatelů do 3 %.
Iniciativy:	Testování na různých platformách. Vytvoření návodů pro uživatele. Rozvoj znalostní báze BYOD.
Strateg. cíle:	Cíl S1, Cíl S2, Cíl S3

Tabulka 2-6-2-7: IT BSC - cíl ZAK 2. Zdroj: autor.

Zkratka cíle:	**ZAK 2**
Název cíle:	**Rychlé dodání nové VM**
Měřítka:	Rychlost dodání VM měřeno od okamžiku splnění podmínek uživatele pro vstup do BYOD, až po uložení VM do úložiště a informování uživatele o splnění požadavku.
Záměry:	Do 4 hodin.
Iniciativy:	Automatizace přípravy VM a jejich vystavení do úložiště VM.
Strateg. cíle:	Cíl S1, Cíl S2, Cíl S3

Tabulka 2-6-2-8: IT BSC - cíl ZAK 3. Zdroj: autor.

Zkratka cíle:	**ZAK 3**
Název cíle:	**Zajištění podpory uživatelům při problémech.**
Měřítka:	Počet uživatelů, kteří využili zápůjčku notebooku. Počet uživatelů, kteří úspěšně využili znalostní bázi BYOD.
Záměry:	Více než 20 % uživatelů, kteří při poruše HW využili zápůjčky notebooku. Více než 80 % uživatelů, kteří vyřešili problém díky znalostní bázi BYOD.
Iniciativy:	Krátkodobé zápůjčky služebního notebooku po dobu servisu od IT oddělení. Rozvoj znalostní báze BYOD.
Strateg. cíle:	Cíl S1, Cíl S3

Tabulka 2-6-2-9: IT BSC - cíl ZAK 4. Zdroj: autor.

Zkratka cíle:	**ZAK 4**
Název cíle:	**Nárůst mobility a flexibility zaměstnanců.**
Měřítka:	Počet hodin odpracovaných zaměstnanci mimo svoji kancelář.
Záměry:	Zvýšit počet odpracované doby mimo kancelář o 5 hodin týdně.
Iniciativy:	Zavedení BYOD pro notebooky, aby zaměstnanci, kteří mají dnes desktopy, mohli pracovat odkudkoliv.
Strateg. cíle:	Cíl S1, Cíl S3

Tabulka 2-6-2-10: IT BSC - cíl ZAK 5. Zdroj: autor.

Zkratka cíle:	**ZAK 5**
Název cíle:	Zajištění vysoké spokojenosti uživatelů BYOD programu.
Měřítka:	Procento spokojených uživatelů dle průzkumu, který bude zaměřen na rychlost odezvy na požadavky, adekvátnost a kvalitu vyřešení požadavků. Procento požadavků vyřízených ke spokojenosti uživatele.
Záměry:	Alespoň 80 % spokojených uživatelů. Alespoň 90 % kladně vyřízených požadavků.
Iniciativy:	Kvalitní poskytování BYOD. Zajištění kvalitní a rychlé uživatelské podpory. Dojednání slev u dodavatelů pro uživatele (notebooky, licence, pojištění, ...).
Strateg. cíle:	Cíl S3

Perspektiva interních procesů

Tato perspektiva zahrnuje cíle, které podporují efektivitu a kvalitu procesů projektu BYOD nebo přínosy, které vzniknou interním procesům díky zavedení programu BYOD.

Tabulka 2-6-2-11: IT BSC - cíl PROC 1. Zdroj: autor.

Zkratka cíle:	**PROC 1**
Název cíle:	**Nárůst počtu uživatelů**
Měřítka:	Počet uživatelů v BYOD programu. Počet uživatelů, kteří opustili BYOD program.
Záměry:	Získat 500 uživatelů do dvou let a alespoň 50 uživatelů každý další rok. Méně než 5 % odchodů z BYOD programu ročně.
Iniciativy:	Komunikace BYOD programu s uživateli. Finanční bonus uživatelům BYOD. Rozvoj znalostní báze pro BYOD uživatele. Nízká chybovost BYOD VM.
Strateg. cíle:	Cíl S1, Cíl S4

Tabulka 2-6-2-12: IT BSC - cíl PROC 2. Zdroj: autor.

Zkratka cíle:	**PROC 2**
Název cíle:	**Rychlost vytvoření BYOD VM.**
Měřítka:	Doba vytvoření nové BYOD VM uživateli.
Záměry:	Méně než 30 minut.
Iniciativy:	Automatizace přípravy VM a jejich vystavení do úložiště VM.
Strateg. cíle:	Cíl S2

Tabulka 2-6-2-13: IT BSC - cíl PROC 3. Zdroj: autor.

Zkratka cíle:	**PROC 3**
Název cíle:	**Snížení bezpečnostních rizik**
Měřítka:	Míra rizika z neznámých zařízení připojených ve vnitřní síti. Počet bezpečnostních incidentů uživatelů BYOD. Počet bezpečnostních incidentů vzniklých při vytváření, dodávání nebo uchovávání BYOD VM.
Záměry:	Snížit rizika z neznámých zařízení ve vnitřní síti o 80 % oproti stavu před zavedením projektů programu BYOD. Udržet poměr bezpečnostních incidentů BYOD zařízení na jednoho uživatele na úrovni průměrného počtu bezpečnostních incidentů na uživatele služebních notebooků.
Iniciativy:	Propojení L2 Propojení BYOD pro notebooky s projektem L2 Security. Bezpečnostní testování BYOD VM. Školení a testování BYOD uživatelů.
Strateg. cíle:	Cíl S1

Tabulka 2-6-2-14: IT BSC - cíl PROC 4. Zdroj: autor.

Zkratka cíle:	**PROC 4**
Název cíle:	**Zajištění kvality a spolehlivosti provozu BYOD**
Měřítka:	Průměrná doba souvislého bezchybného provozu BYOD VM. Průměrný počet chyb a poruch BYOD VM. Doba na vyřízení požadavku (maximální a průměrná). Procento nevyřešených problémů BYOD.
Záměry:	Průměrná doba bezchybného provozu a průměrný počet poruch BYOD VM na úrovni služebního notebooku nebo lepší. Maximální doba vyřízení požadavku 4 hodiny, průměrná doba 30 minut.
Iniciativy:	Bezpečnostní testování VM. Rozvoj znalostní báze BYOD. Školení a testování uživatelů i administrátorů BYOD.
Strateg. cíle:	Cíl S1, Cíl S3

Perspektiva učení se a růstu

Perspektiva zahrnuje vzdělání a růst uživatelů BYOD i zaměstnanců IT oddělení.

Tabulka 2-6-2-15: IT BSC - cíl UCE 1. Zdroj: autor.

Zkratka cíle:	**UCE 1**
Název cíle:	**Vyšší atraktivita zaměstnání.**
Měřítka:	Počet kvalifikovaných zájemců o zaměstnání. Počet absolventů vysokých škol se zájmem o práci v TCZ.
Záměry:	Zvýšit počet kvalifikovaných uchazečů o 0 - 5 %.
Iniciativy:	Rozšíření možností, jak přistupovat k IT službám díky BYOD VM. Propagace BYOD programu při náboru zaměstnanců.
Strateg. cíle:	Cíl S5

Tabulka 2-6-2-16: IT BSC - cíl UCE 2. Zdroj: autor.

Zkratka cíle:	**UCE 2**
Název cíle:	**Vzdělanější uživatelé, kteří zvládnou spravovat vlastní zařízení.**
Měřítka:	Počet uživatelů, kteří vyřeší problém na zařízení bez nutnosti kontaktovat helpdesk. Počet vyřešených problémů ostatními uživateli ve znalostní bázi BYOD.
Záměry:	Snížit počet požadavků na helpdesk z důvodu podpory hardware o 8 %. Procento problémů, které pomohli vyřešit ostatní BYOD uživatelé větší než 50 %.
Iniciativy:	Rozšiřovat BYOD program. Poskytnout uživatelům znalostní bázi BYOD. Motivace uživatelů BYOD k sebevzdělávání a participaci ve znalostní bázi BYOD.
Strateg. cíle:	Cíl S5

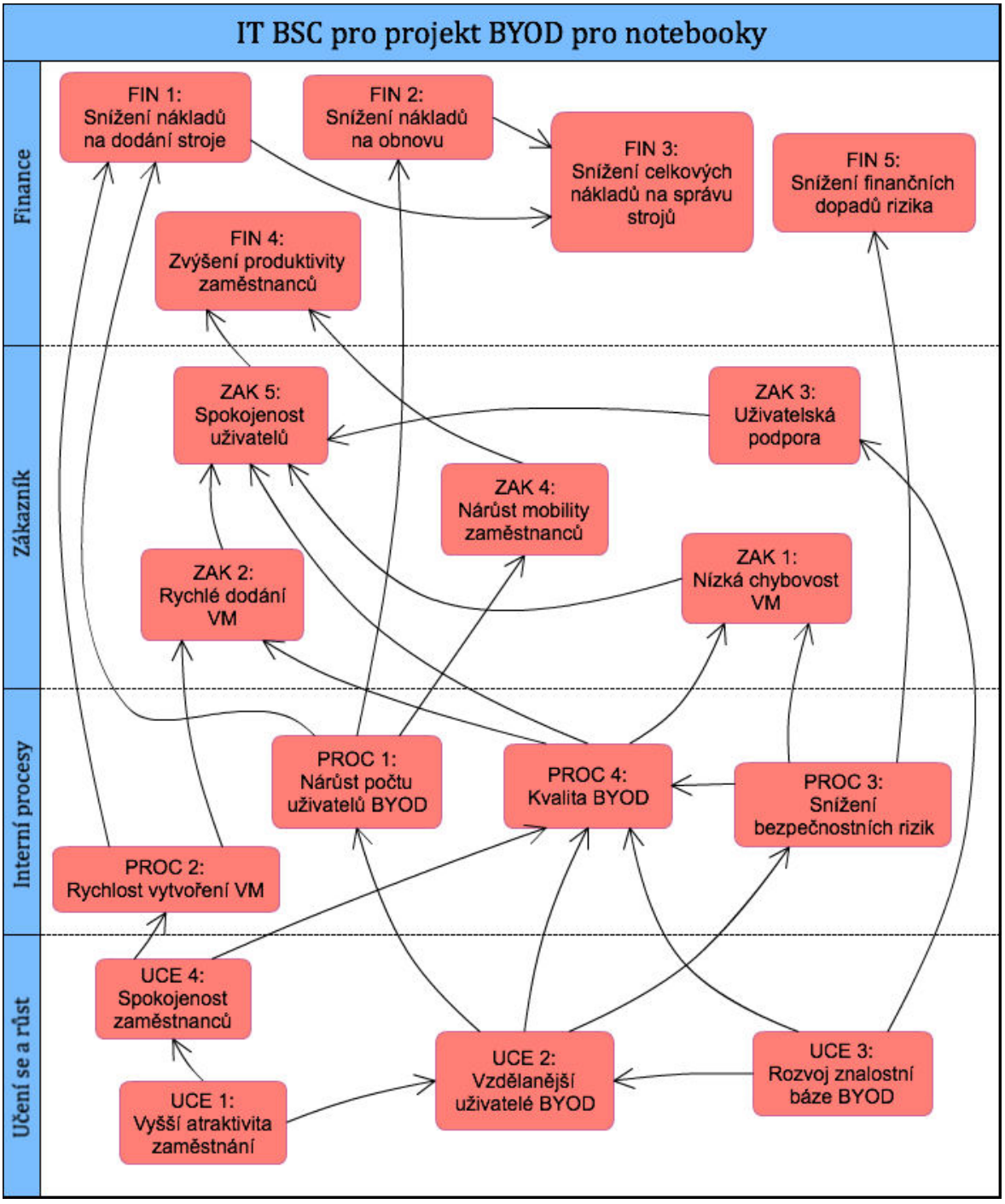
Tabulka 2-6-2-17: IT BSC - cíl UCE 3. Zdroj: autor.

Zkratka cíle:	**UCE 3**
Název cíle:	**Rozvoj znalostní báze pro uživatele BYOD**
Měřítka:	Počet uživatelů, kteří přistoupí do znalostní báze. Počet námětů ke zlepšení BYOD programu. Počet technických dotazů.
Záměry:	Počet unikátních denních přístupů vyšší než 30 % uživatelů BYOD. Počet kladně vyřízených námětů na zlepšení větší než 10 za měsíc. Počet technických dotazů, které alespoň 2 uživatelé označí za přínosné větší než 5 měsíčně.
Iniciativy:	Vytvořit na intranetu znalostní bázi pro BYOD. Odměňovat uživatele za přínosnou aktivitu ve znalostní bázi BYOD.
Strateg. cíle:	Cíl S1, Cíl S3, Cíl S5

Tabulka 2-6-2-18: IT BSC - cíl UCE 4. Zdroj: autor.

Zkratka cíle:	**UCE 4**
Název cíle:	**Nárůst spokojenosti zaměstnanců**
Měřítka:	Podíl zaměstnanců spokojených s pracovním prostředím. Podíl zaměstnanců spokojených s profesionalitou, kulturou a podporou ze strany zaměstnavatele.
Záměry:	Zvýšit podíl spokojených zaměstnanců díky zavedení BYOD pro notebooky o 0 - 5 %.
Iniciativy:	Zavedení a rozvoj BYOD pro notebooky. Zavedení a rozvoj znalostní báze BYOD.
Strateg. cíle:	Cíl S3

2.6.3 Strategická mapa projektu



Obrázek 2-6-2-1: Strategická mapa IT BSC projektu BYOD. Zdroj: autor.

Závěr

Vypracování IT BSC pomohlo identifikovat projektové cíle, kterých je třeba dosáhnout k úspěšnému nasazení projektu. Některé cíle a jejich metriky jsou převážně ovlivněny projektem BYOD. Některé však, jako *UCE 1: Vyšší atraktivita zaměstnavatele*, nebo *FIN 4: Zvýšení produktivity zaměstnanců*, jsou ovlivněny řadou dalších faktorů a projekt BYOD k jejich naplnění pouze z části přispívá.

Z IT BSC vyplynula potřeba vybudování znalostní báze pro BYOD program. Ta nebude nadměrně zvyšovat náklady na podporu uživatelů a zároveň bude sloužit jako samoobsluha pro pomoc uživatelům s problémy. Je kladen důraz na rychlost dodání BYOD VM, kvalitu BYOD programu, nárůst počtu uživatelů, snižování bezpečnostních rizik. Mezi hlavní nefinanční efekty patří nárůst mobility, vzdělanosti a spokojenosti zaměstnanců. Významným finančním přínosem je úspora nákladů na životní cyklus pracovní stanice a celkové snížení nákladů na správu desktopů a notebooků.

Je třeba dodat, že toto je úvodní návrh cílů založený na aktuálních informacích a odráží pouze pohled autora. Je pravděpodobné, že se cíle budou v průběhu času měnit tak, jak budou známy další informace. Navržený IT BSC by měl být revidován při dosažení projektových milníků.

2.7 Náklady

Tato kapitola významným způsobem naplňuje *cíl - 4. Identifikovat a charakterizovat důvody k realizaci projektu* - modelovým vyjádřením úspor, plynoucích ze zavedení BYOD pro notebooky a kalkulací odhadovaného bodu zvratu.

Při kalkulaci nákladů byl vzat v úvahu retrográdní kalkulační vzorec pro ABC[9] (Král, 2008):

- **Cena výkonu**
- − Variabilní náklady výrobku
  - přímý (jednicový) materiál
  - přímé (jednicové) mzdy
  - variabilní režie, ...
- **Marže I (Contribution Margin)**
  - − Variabilní náklady aktivit, vyvolaných druhem výkonu
- **Marže II (Activity Based Margin)**
  - − Fixní výrobkové náklady - vyhnutelné - s vlivem na CF
  - − utopené - bez vlivu na CF
- **Marže III**
  - − Fixní náklady střediskové
- **Marže IV**
  - − Fixní náklady podniku
- **Zisk nebo ztráta výkonu**

Tento vzorec je možným východiskem pro kalkulaci ceny IT služby a pro porovnání nákladů na životní cyklus BYOD notebooku a služebního počítače.

Zásadní jsou pro porovnání nákladů na BYOD notebook proti nákladům na služební počítač "variabilní náklady výrobku". Těmto se podrobněji věnují následující podkapitoly. Fixní náklady podniku ani střediska nemají při porovnání BYOD notebooku a služebního počítače významný vliv. Zavedení BYOD pro notebooky znamená jednorázové projektové investice a minimální dodatečné provozní náklady, protože většina provozu bude pokryta

[9] Znak "−" je mínus. Od ceny výkonu jsou postupně odečítány náklady.

z již alokovaných zdrojů. Navrhované řešení BYOD pro notebooky zachovává z finančního hlediska většinu procesů shodných, jako při správě služebního notebooku.

Kalkulované náklady a časy jsou odhadnuté průměrné hodnoty. Slouží k modelovému porovnání. Ceny hardware a software vycházejí z běžných maloobchodních cen. Kalkulovaná mzda technika je 500 Kč za hodinu.

Náklady na materiál jsou běžné maloobchodní ceny. V případě licencí je pro zjednodušení použita jednorázová maloobchodní cena. Nákup hromadných licencí a jejich správa nejsou v tomto modelu zohledněny.

Tabulka 2-7-0-1: Výchozí podmínky kalkulace nákladů životního cyklu. Zdroj: autor.

Cena notebooku/desktopu	20 000 Kč
Cena licence OS	5 000 Kč
Cena licence aplikací	5 000 Kč
Délka životního cyklu stroje	4 roky
Mzda technika	500 Kč / hod.

2.7.1 Vyčíslení nákladů

N-P: Příprava stroje

Příprava **služebního počítače** znamená zajištění stroje (notebooku nebo desktopu) buď ze skladu, nebo od dodavatele. V případě použití počítače ze skladu se jedná o činnosti:

- N-P-1: Zajištění počítače a transport na IT oddělení (objednání nového počítače nebo vyzvednutí použitého ze skladu)
    - materiál (notebook/desktop, dopravné): 20 000 Kč
    - mzda: 0,3 * 500 Kč = 150 Kč
- N-P-2: Instalace systému
    - materiál (licence OS): 5 000 Kč
    - mzda: 0,3 * 500 Kč = 150 Kč
- N-P-3: Spouštění skriptů pro přizpůsobení počítače a doinstalování základních aplikací,
    - materiál (licence aplikací): 5 000 Kč
    - mzda: 0,5 * 500 Kč = 250 Kč

- N-P-4: Otestování funkčnosti
    - materiál: 0 Kč
    - mzda: 0,3 * 500 Kč = 150 Kč
- N-P-5: Zařazení stroje do sítě (záznam do CMDB, přiřazení k uživateli,...)
    - materiál: 0 Kč
    - mzda: 0,3 * 500 Kč = 300 Kč

Při přípravě **BYOD notebooku** se přenáší činnosti spojené se zajištěním počítače a instalací systému na uživatele. IT oddělení připravuje **BYOD VM**. Ta je již připravená ve formě základní image. IT oddělení při přípravě VM provádí činnosti:

- N-P-6: Připravení nové VM z výchozí image
    - materiál (licence OS a aplikace): 10 000 Kč
    - mzda: 0,4 * 500 Kč = 200 Kč
- N-P-5: Zařazení stroje do sítě (záznam do CMDB[10], přiřazení k uživateli,...)
    - materiál: 0 Kč
    - mzda: 0,3 * 500 Kč = 150 Kč

N-D: Doručení stroje

Při doručení připraveného **služebního počítače** provádí IT oddělení fyzicky tyto činnosti:

- N-D-1: Transport počítače k uživateli
    - materiál (dopravné, ...): 100 Kč
    - mzda: 0,6 * 500 Kč = 300 Kč
- N-D-2: Zapojení a předání počítače
    - materiál: 0 Kč
    - mzda: 0,4 * 500 Kč = 200 Kč

V případě doručení **BYOD VM** není doručení realizováno fyzicky, ale přenosem souboru VM přes síťové úložiště VM. IT oddělení zajišťuje činnost:

- N-D-3: Doručení VM do úložiště VM a zpřístupnění uživateli
    - materiál: 0 Kč
    - mzda: 0,2 * 500 Kč = 100 Kč

[10] CMDB = Configuration Management Database, která slouží k zaznamenávání konfigurace IT zdrojů.

N-S: Servis stroje

Při servisu **služebního počítače** je v případě poruchy hardware nebo vážnější poruchy operačního systému nutný fyzický zásah technika. V případě méně vážné poruchy operačního systému, kdy je zachována možnost vzdáleného připojení, nebo v případě poruchy aplikace je služební počítač opravován vzdáleným přístupem.

- N-S-1: Oprava hardware
  - materiál (dopravné, nové komponenty, ...): 1 100 Kč (odhadnutý průměr v závislosti na druhu závady a záruce)
  - mzda: 1 * 500 Kč = 500 Kč
- N-S-2: Oprava operačního systému (s nutným fyzickým zásahem)
  - materiál (dopravné, ...): 100 Kč
  - mzda: 1 * 500 Kč = 500 Kč
- N-S-3: Oprava OS nebo aplikací (přes vzdálenou správu)
  - materiál: 0 Kč
  - mzda: 0,8 * 500 Kč = 400 Kč
- N-S-4: Zapůjčení náhradního notebooku při poruše hardware na 3 dny
  - materiál (přeinstalovaný služební notebook) = 1 031 Kč
    - instalace systému = 150 Kč
    - spouštění skriptů pro přizpůsobení počítače a doinstalování základních aplikací = 250 Kč
    - otestování funkčnosti = 150 Kč
    - zařazení stroje do sítě (záznam do CMDB, přiřazení k uživateli,...) = 300 Kč
    - vyřazení stroje ze sítě = 150 Kč
    - opotřebení hardware (20 000 Kč / 4 roky životnosti * 3 dny zápůjčky) = 31 Kč

BYOD notebook je spravován IT oddělením pouze pomocí vzdáleného přístupu. V případě poškození VM je distribuován uživateli virtuální stroj znovu. V případě poškození OS nebo aplikace, kdy je možný vzdálený přístup do hostovaného systému, je použit stejný postup, jako u vzdálené opravy služebního notebooku.

- N-S-3: Oprava OS nebo aplikací (přes vzdálenou správu)
  - materiál: 0 Kč
  - mzda: 0,8 * 500 Kč = 400 Kč

- N-S-5: Oprava operačního systému přeinstalováním VM (shodné s nákladem N-D-3)
    - materiál: 0 Kč
    - mzda: 0,2 * 500 Kč = 100 Kč
- N-S-4: Zapůjčení náhradního notebooku při chybě hardware
    - materiál (přeinstalovaný služební notebook): 1 031 Kč
    - mzda: 0 Kč

N-V: Vyřazení stroje

V případě vyřazení **služebního počítače** je nutné jeho fyzické vyzvednutí, kontrola a před uložením do skladu i vymazání. V případě úplného vyřazení je třeba zajistit ekologickou likvidaci.

- N-V-1: Kontrola stavu předávaného počítače
    - materiál: 0 Kč
    - mzda: 0,1 * 500 Kč = 50 Kč
- N-V-2: Transport počítače od uživatele do skladu
    - materiál (PHM, dopravné,...): 100 Kč
    - mzda: 0,6 * 500 Kč = 300 Kč
- N-V-3: Vyřazení stroje ze sítě
    - materiál: 0 Kč
    - mzda: 0,3 * 500 Kč = 150 Kč
- N-V-4: Likvidace hardware
    - cena služby: 100 Kč

Při vyřazení **BYOD notebooku** provádí IT oddělení pouze vyřazení stroje z domény.

- N-V-3: Vyřazení stroje ze sítě (záznam do CMDB, odebrat přiřazení k uživateli,...)
    - materiál: 0 Kč
    - mzda: 0,3 * 500 Kč = 150 Kč

N-N: Náklady spojené s HR

- N-N-1: Náhrady zaměstnancům za opotřebení hardware
    - minimální výše náhrady: 333 Kč / měsíčně
        - pořízení notebooku: 20 000 Kč
        - využití notebooku pro pracovní účely: 80 % času
        - životnost notebooku: 4 roky
        - výpočet: (20 000 Kč * 80 %) / 48 měsíců

Porovnání nákladů na životní cyklus stroje

Porovnáme-li náklady IT oddělení na provoz BYOD notebooku s náklady na provoz služebního notebooku, zjistíme, že IT oddělení přenesením některých činností na uživatele ušetří část nákladů. Podrobně úsporu zachycuje následující tabulka.

Náklady jsou vztaženy k celému čtyřletému životnímu cyklu stroje. Průměrné servisní zásahy za 4 roky jsou odhadnuty na:

- N-S-1: Oprava HW - 2x.
- N-S-2: Oprava OS fyzicky - 1x.
- N-S-5: Oprava pomocí nového nahrání VM - 1x.
- N-S-3: Oprava OS nebo aplikací (přes vzdálenou správu) - 4x.
- N-S-4: Zapůjčení náhradního notebooku - 1x.

Tabulka 2-7-1-1: Výpočet celkových nákladů na životní cyklus stanic. Zdroj: autor.

Náklad	**Služební notebook**	**BYOD notebook**
N-P: Příprava stroje	**31 000 Kč**	**10 500 Kč**
N-P-1: Zajištění počítače	20 150 Kč	0 Kč
N-P-2: Instalace systému	5 150 Kč	0 Kč
N-P-3: Konfigurace systému a instalace aplikací	5 250 Kč	0 Kč
N-P-4: Otestování funkčnosti	150 Kč	0 Kč
N-P-5: Zařazení stroje do sítě	300 Kč	300 Kč
N-P-6: Připravení nové VM	0 Kč	10 200 Kč

Náklad	Služební notebook	BYOD notebook
N-D: Doručení stroje	**600 Kč**	**100 Kč**
N-D-1: Transport počítače k uživateli	400 Kč	0 Kč
N-D-2: Zapojení a předání počítače	200 Kč	0 Kč
N-D-3: Doručení VM do úložiště VM	0 Kč	100 Kč
N-S: Servis stroje	**6 431 Kč**	**2 731 Kč**
N-S-1: Oprava hardware	3 200 Kč	0 Kč
N-S-2: Oprava operačního systému (fyzicky)	600 Kč	0 Kč
N-S-3: Oprava OS nebo aplikací (vzdáleně)	1 600 Kč	1 600 Kč
N-S-4: Zapůjčení náhradního notebooku	1 031 Kč	1 031 Kč
N-S-5: Přeinstalování VM	0 Kč	100 Kč
N-V: Vyřazení stroje	**700 Kč**	**150 Kč**
N-V-1: Kontrola stavu předávaného počítače	50 Kč	0 Kč
N-V-2: Transport počítače	400 Kč	0 Kč
N-V-3: Vyřazení stroje ze sítě	150 Kč	150 Kč
N-V-4: Likvidace hardware	100 Kč	0 Kč
Náklady IT oddělení celkem	**38 731 Kč**	**13 481 Kč**
N-N: Náklady spojené s HR	**0 Kč**	**16 000 Kč**
N-N-1: Náhrady zaměstnancům za opotřebení	0 Kč	16 000 Kč
Náklady životního cyklu celkem	**38 731 Kč**	**29 481 Kč**

Z výše uvedené tabulky lze usuzovat, že přechodem uživatele služebního notebooku do BYOD pro notebooky bude ušetřeno na nákladech IT oddělení 25 250 Kč během 4 letého životního cyklu jednoho stroje. To znamená pro IT průměrnou měsíční úsporu 526 Kč na uživatele.

Podstatná je část **N-N: Ostatní náklady**, vyjadřující částku, která bude vyplácena uživatelům BOYD za opotřebení soukromého notebooku v souvislosti s plněním pracovních povinností. Částka bude pravděpodobně vyplácena oddělením lidských zdrojů. Nejedná se tedy o náklad IT oddělení. Po odečtení minimální kompenzace za opotřebení notebooku je úspora BYOD pro notebooky odhadována na 193 Kč za uživatele měsíčně, respektive 9 250 Kč za čtyřletý životní cyklus stroje.

2.7.2 Bod zvratu

Projektové investice

Projektové investice jsou očekávány v následujících oblastech a v uvedené výši. Jedná se o subjektivní odhad autora, který bude v průběhu projektu zpřesňován. Přesto má za cíl přiblížit pracnost jednotlivých činností na projektu a z celkové částky ukázat odhadovaný bod zvratu pro počet uživatelů BYOD notebooků. Činnosti jsou seřazeny chronologicky, některé na sebe navazují.

Výpočty vycházejí z předpokladu, že 1 MD[11] specialisty, pracujícího na projektových úkolech stojí v průměru 10 000 Kč. Uvedené pracnosti jsou odhady zaokrouhlené na 10 MD.

PI-1: Specifikace požadavků je první z projektových činností, které bude třeba provést. Týká se všech zainteresovaných oddělení a skládá se ze tří hlavních částí:

- požadavky na uživatele BYOD - jako jsou uživatelské kompetence, podmínky vstupu do BYOD programu, ...
- požadavky na zajištění BYOD - např. rozdělení kompetencí, povinnosti administrátorů VM, SLA pro zajištění služby, zajištění síťové infrastruktury, ...
- technologické požadavky - např. minimální požadavky na hardware operační systém a software, požadavky na síť, ...

Předpokládaná pracnost na těchto činnostech je 10 MD.

PI-2: Analýza licencí a příprava modelů licencování je podstatnou částí projektu. Zejména se jedná o licenční podmínky společností Microsoft a VMware pro zajištění licencování hostovaného systému Windows a hypervizoru VMware Player Plus / Fusion. Předpokládaná pracnost je 10 MD.

PI-3: Vytvoření etalonu BYOD VM se skládá ze dvou částí:

- vytvoření optimální konfigurace VM,
- příprava image hostovaného systému (Windows 7) optimalizované pro použití v BYOD noteboocích pod virtuálním prostředím.

Předpokládaná pracnost je 50 MD.

PI-4: Úprava software a infrastruktury je činnost odhadovaná v malém rozsahu, protože projekt předpokládá využití stávající infrastruktury. Přesto budou třeba úpravy, jako vytvoření úložiště BYOD VM nebo báze znalostí. Je odhadována pracnost 30 MD.

---

[11] MD = manday, člověkoden

PI-5: Technické řešení přípravy a doručení BYOD VM uživatelům je podstatnou částí projektu. Dle IT BSC analýzy v kapitole 2.6 je významným faktorem spokojenosti uživatelů a úspěšnosti projektu (z důvodu možných chyb a možné dlouhé doby dodání). Z toho důvodu je jí třeba věnovat zvláštní pozornost. Odhadovaná pracnost včetně testování je 30 MD.

PI-6: Úprava interních procesů je činnost, která předpokládá následující kroky:

- analýzu stávajících procesů,
- návrh a implementaci úprav pro procesy.

Procesně projekt BYOD zasáhne zejména oddělení IT, oddělení bezpečnosti a oddělení lidských zdrojů. Protože BYOD zasahuje do činností více oddělení, je předpokládaná pracnost 20 MD.

PI-7: Vytvoření návodů je významnou činností pro zajištění spokojenosti uživatelů a znalostí pro správce BYOD VM. Předpokládá:

- návody pro BYOD uživatele pro práci s VM a kroky, které provází uživatele BYOD VM v průběhu jejího životního cyklu,
- návody pro správce BYOD VM,
- vytvoření znalostní báze pro uživatele BYOD ve formě otevřené encyklopedie typu Wiki.

Odhadovaná pracnost je 10 MD.

PI-8: Vytvoření testů je jedním z posledních kroků, které navazují na činnost specifikace požadavků na kompetenci uživatelů. Do této části spadá:

- školení uživatelů BYOD,
- testy uživatelů BYOD,
- začlenění školení a testů do firemní univerzity a navázání na zisk oprávnění.

Předpokládaná pracnost je 10 MD.

PI-9: Testování funkčnosti BYOD programu v pilotním režimu na vybraných uživatelích je posledním krokem projektu. Znamená zvýšenou pozornost všem aspektům fungování BYOD programu, prvotní vyhodnocení a úpravu metrik definovaných v IT BSC (kapitola 2.6), případně dalších dodaných v průběhu projektu. Pracnost je odhadována na 20 MD.

PI-10: Propagace BYOD programu bude probíhat po vyhodnocení pilotního provozu. Zahrnuje propagaci na intranetu mezi zaměstnanci a články v interním časopise. Pracnost je předpokládána na 10 MD.

Tabulka 2-7-2-1: Odhad celkové výše projektových nákladů. Zdroj: autor.

Činnost	**Pracnost**	**Cena**
PI-1: Specifikace požadavků	10 MD	100 000 Kč
PI-2: Analýza licencí	10 MD	100 000 Kč
PI-3: Vytvoření etalonu BYOD VM	50 MD	500 000 Kč
PI-4: Úprava software a infrastruktury	30 MD	300 000 Kč
PI-5: Technické řešení přípravy a doručení BYOD VM	30 MD	300 000 Kč
PI-6: Úprava interních procesů	20 MD	200 000 Kč
PI-7: Vytvoření návodů	10 MD	100 000 Kč
PI-8: Vytvoření testů	10 MD	100 000 Kč
PI-9: Testování funkčnosti BYOD programu	20 MD	200 000 Kč
PI-10: Propagace BYOD programu	10 MD	100 000 Kč
PI celkem	**200 MD**	**2 000 000 Kč**

Z výše uvededeného vyplývají odhadované náklady na projekt ve výši celkem 2 miliony korun.

Výnosy z projektu

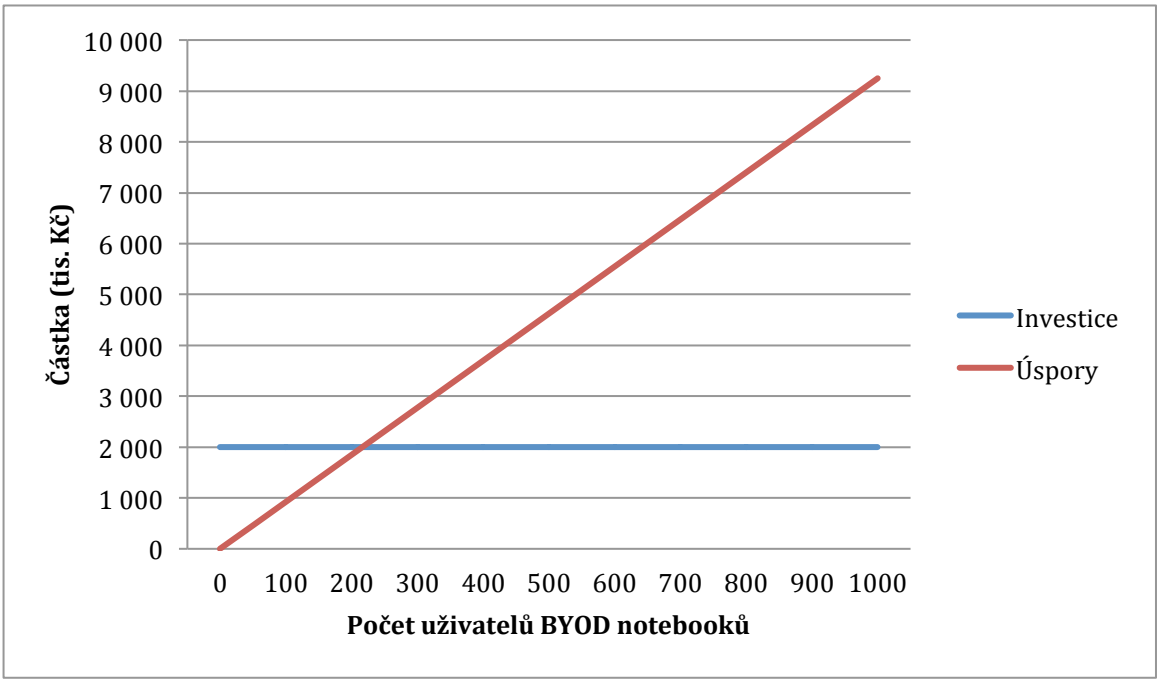
Z předchozí podkapitoly vyplývá celková úspora na čtyřletý životní cyklus uživatele 9 250 Kč oproti služebnímu notebooku.

Předpokládá se, že jedinými náklady na projekt budou jednorázové pořizovací náklady. Náklady na provoz BYOD řešení budou pokryty ze stávajících zdrojů IT a ostatních oddělení a nebudou významně vysoké.

Výpočet bodu zvratu

Bod zvratu byl vypočítán vydělením předpokládaných projektových nákladů úsporou na životní cyklus stroje pro jednoho uživatele.

Výpočet je tedy 2 000 000 / 9 250 Kč = 216,22. Vývoj úspor a investic dokumentuje následující graf.



Obrázek 2-7-2-1: Bod zvratu projektu BYOD. Zdroj: autor.

Bodu zvratu bude při stanovených podmínkách dosaženo při 217 uživatelích BYOD. Každý další uživatel znamená pro společnost úsporu nákladů.

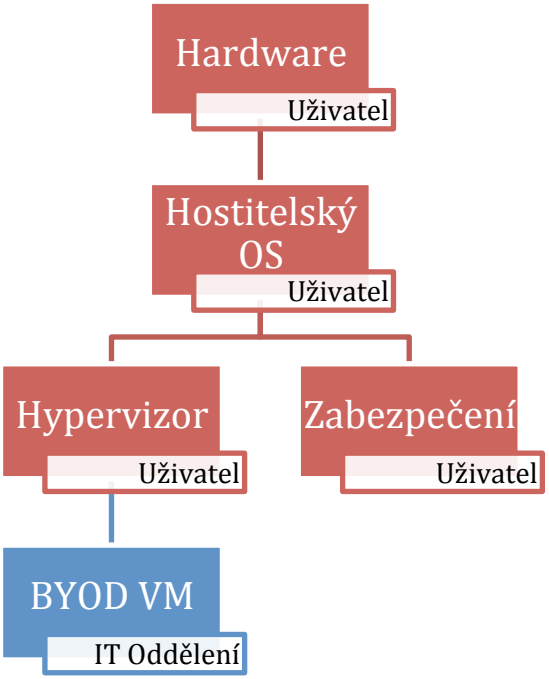
3 Návrh BYOD pro notebooky v TCZ

Cílem této kapitoly je rámcově navrhnout pravidla pro program BYOD pro notebooky v TCZ tak, aby mohla sloužit jako podklad pro vytvoření interní směrnice. Významným způsobem naplňuje cíl práce - *3. Vytvořit rámec pro projekt BYOD pro notebooky*.

3.1 Pravidla programu

Z průzkumu v kapitole *1.3 Trendy v BYOD* vyplývá, že firmy implementující BYOD formulují pravidla napříč odděleními. BYOD program má přesah z IT do oblasti bezpečnostní, personální i právní. Z toho důvodu se na formování pravidel podílí nejen oddělení IT, ale i oddělení bezpečnosti, lidských zdrojů a právní oddělení, případně daňové a finanční ke schválení finančních modelů a způsobu kompenzací za opotřebení soukromého hardware.

Následující schéma zachycuje rozdělení odpovědnosti mezi uživatelem BYOD (červeně) a IT oddělením (modře). Ukazuje, že uživatel je zodpovědný za pořízení a správu hardware (notebooku), hostitelského OS, hypervizorové aplikace VMware Player/Fusion a zabezpečení (antivir, zálohování, ...). IT oddělení dodává a spravuje BYOD VM.



Obrázek 3-1-0-1: Rozdělení odpovědnosti mezi uživatelem a IT oddělením. Zdroj: autor.

Dále jsou uvedeny úlohy uživatelů a jednotlivých útvarů v BYOD programu.

3.1.1 IT oddělení

IT oddělení zajišťuje kompletní servis BYOD VM v celém jejím životním cyklu. Je odpovědné za vytvoření vzorové VM (etalonu), přípravu nové VM uživateli BYOD, její distribuci, podporu VM během používání a její vyřazení.

Interní procesy spojené se správou životního cyklu VM jsou plně v kompetenci IT oddělení. Vzhledem k velmi malým odlišnostem od prostředí standardního firemního počítače je vliv na interní procesy IT minimální. Možné dopady jsou přiblíženy v kapitole *1.4.1 Dopady na IT procesy* podle dopadů v ITIL v3. Pro IT oddělení to znamená zejména zavedení nového procesu vytvoření a dodání VM, úpravu katalogu služeb apod. Z pohledu uživatelů bude IT dodávat novou službu, poskytování firemní VM pro uživatele BYOD notebooků.

Příprava VM uživateli

IT oddělení provádí přípravu BYOD VM uživateli. Uživatelská VM vychází z připravené výchozí VM - etalonu, jehož klonováním a úpravami vznikají uživatelské VM. Etalon dodá IT oddělení na základě zadání dodavatel.

Při přípravě VM dojde ke změně názvu VM a dalších parametrů na úrovni konfigurace virtuálního hardware.

Dále je nakonfigurován hostovaný OS. Je provedena změna názvu stanice a zařazení firemního prostředí v BYOD VM do domény. Tyto postupy jsou shodné se standardními postupy pro přípravu operačního systému a software služebního počítače.

Výstupem přípravy je balíček VM <user_id>.zip, který obsahuje soubory VM (konfiguraci virtuálního HW a hostovaný OS) přizpůsobené konkrétnímu uživateli k provozu na VMware Player/Fusion.

Podrobný postup přípravy VM vytvoří IT oddělení ve spolupráci s dodavatelem etalonu. Je žádoucí, aby byl postup přípravy BYOD VM co nejvíce zautomatizován pro zkrácení doby dodání, snížení pracnosti a pravděpodobnosti vzniku chyb, což bude podporovat cíle z kapitoly *2.6 IT BSC pro projekt BYOD*. Maximální čas pro přípravu je odhadován na 20 min, záleží však na konkrétním způsobu řešení.

BYOD VM musí být připravena v souladu s platnými bezpečnostními požadavky TCZ. Jedním z ochranných mechanizmů bude omezení kopírování VM. Další způsoby technologického zabezpečení na úrovni hypervizoru a nastavení virtuálního hardware jsou popsány v kapitole *4.1 Konfigurace VM*. Bezpečnostní opatření hostovaného OS s firemním prostředím budou využity stávající, která jsou již využívána pro služební notebooky.

Vytvořená BYOD VM a hostitelský systém musí být oddělen, aby nebylo možné z firemního prostředí přistupovat do soukromého a zároveň i zajistit co největší míru oddělení pro neoprávněný přístup ze soukromého prostředí do firemního ve VM.

Distribuce VM

Vytvořená BYOD VM ve formě balíčku <user_id>.zip je umístěna do úložiště VM, odkud je zpřístupněna uživateli BYOD. V úložišti je uživateli vytvořen profil, pod kterým mu jsou soubory zpřístupněny.

Přihlášení do úložiště VM je přístupné z interní sítě všem připojeným zařízením. Po úspěšném ověření získá uživatel přístup ke svému profilu.

Technické řešení vystavení VM do úložiště vypracuje IT oddělení ve spolupráci s dodavatelem řešení.

Správa VM

Správa firemního prostředí v BYOD VM probíhá stejně, jako správa firemního prostředí ve služebním notebooku. Z pohledu zavedených technologií správy koncových zařízení vystupuje BYOD VM jako standardní firemní počítač. Zásadní odlišnost je v tom, že IT oddělení spravuje BYOD VM pouze vzdáleně.

IT oddělení má právo změnit minimální parametry pro používání VM, nejčastěji však jednou za životní cyklus stroje, tedy 4 roky.

Vyřazení VM

Při vyřazení BYOD VM vyřazuje IT oddělení hostovaný OS z domény a provádí standardní úpravy v konfigurační databázi. K vyřazení může dojít buď z důvodu konce životního cyklu VM, nebo mimořádného důvodu, jako je poškození, ztráta nebo krádež VM (respektive celého BYOD notebooku). Za bezpečné smazání souborů BYOD VM je při vyřazení zodpovědný uživatel.

Podpora uživatelů BYOD - znalostní báze

Uživatelé BYOD budou mít ze strany IT oddělení omezenou podporu pro své notebooky. Podpora bude poskytována zajištěním znalostní báze. Znalostní báze bude obsahovat návody na instalaci a nastavení VMware Player/Fusion a řešení nejčastějších problémů.

Znalostní báze bude otevřená všem uživatelům, kteří budou moci pomocí diskuzních fór řešit své problémy. Problém pomohou vyřešit buď ostatní BYOD uživatelé nebo v případě nevyřešení uživateli přímo administrátor BYOD znalostní báze.

Vytvoření a správa BYOD webu

Pro podporu BYOD uživatelů by bylo vhodné vytvořit BYOD web. Ten by kompletně pokrýval služby pro uživatele BYOD programu.

BYOD web by zastřešoval jak znalostní bázi BYOD, tak úložiště VM. Uživatel tak na jednom místě nalezne jak návody, pravidla a postupy, tak i instalační soubory VMware Player/Fusion i svoji BYOD VM.

Půjčovna notebooků

IT oddělení je povinno zajistit možnost půjčování služebních notebooků pro případ poruchy BYOD notebooku uživatele.

Půjčovány jsou notebooky shodné jako služební. Pracovní prostředí je na nich nainstalováno přímo a ne přes BYOD VM. IT oddělení poskytne nově nainstalovaný služební notebook.

Pro omezení nákladů jsou notebooky půjčovány v místě působení IT oddělení a je nutné osobní vyzvednutí zaměstnancem.

3.1.2 Oddělení bezpečnosti

Oddělení bezpečnosti má zejména funkci poradní a kontrolní. Je významným způsobem zapojeno do BYOD programu.

Bezpečnostní směrnice a dokumentace

Oddělení bezpečnosti vytváří požadavky na uživatele a zařízení BYOD, které pomohou zajistit bezpečný a bezchybný běh BYOD notebooků. Požadavky jsou navrženy tak, aby byla zajištěna akceptovatelná úroveň bezpečnosti.

Pravidla pro zabezpečení BYOD VM a pravidla pro bezpečné používání BYOD VM uživatelem jsou zpracovány do závazných interních směrnic.

Oddělení zajišťuje schvalování, revize a aktualizace bezpečnostních směrnic i BYOD politiky.

Z bezpečnostního hlediska posuzuje a připomínkuje procesy BYOD programu.

Penetrační testování nových verzí etalonu VM

Pro nové verze etalonů provádí oddělení bezpečnosti penetrační testování. Zaměřuje se jak na posuzování dokumentace, tak na samotnou realizaci penetračních testů. Cílem penetračních testů je odhalit chyby ještě před nasazením nových verzí.

Návrh možných oblastí pro penetrační testování je uveden v kapitole *4.5 Bezpečnostní testování VM*.

Zajištění školení a zkoušek

Oddělení bezpečnosti zajišťuje školení uživatelů BYOD, ve kterém jsou uživatelé seznámeni s jejich právy a povinnostmi v rámci programu. Jsou jim navrženy možnosti, jak svůj systém adekvátně zabezpečit a spravovat. Součástí školení by mělo být i upozornění na sankce, které mohou vyplynout z porušení stanovených pravidel.

Se školením je spojené i roční přezkoušení uživatelů, které ukáže, že splňují požadavky pro správu BYOD notebooku a mají dostatečné znalosti.

3.1.3 Uživatel BYOD

Požadavky na BYOD uživatele

Uživatel má volbu, zda vstoupí do programu BYOD pro notebooky nebo zda bude využívat služební počítač. BYOD notebook je náhradou za počítač poskytovaný zaměstnavatelem.

Uživatel musí splnit požadavky jak technické, tak i znalostní. K tomu slouží přezkušování uživatelů BYOD.

Zajištění odpovídajícího hardware

Uživatel je povinen zajistit pro provoz firemního prostředí zařízení v minimální konfiguraci:

- HDD: 50GB pro VM
- CPU: Intel i5 nebo ekvivalentní
- RAM: 4GB (2GB pro VM)
- Operační systém: kompatibilní s VMware Player/Fusion 6

Zajištění aktuálního a aktualizovaného OS

Uživatel je povinen zajistit hostitelský operační systém, který odpovídá požadavkům VMware Player/Fusion. Jiné systémy, než vyjmenované, nejsou povoleny. Pro vybraný systém musí uživatel zajistit nasazení všech dostupných bezpečnostních aktualizací. A nemůže použít systémy s ukončenou podporou (jako Windows XP a starší).

Zajištění VMware Player/Fusion

Uživatel je povinen zajistit na svém zařízení hypervizorovou aplikaci VMware Player/ Fusion pro provoz BYOD VM. Tuto aplikaci získá za výhodných podmínek od zaměstnavatele. Dále uživatel zajistí instalaci aktualizací aplikace.

Bezpečnost

Zabezpečení hostitelského systému je jedním z klíčových faktorů bezpečnosti celého BYOD řešení. Povinností uživatele je zejména chránit notebook před ztrátou, zničením či poškozením. Zároveň musí zaměstnanec zamezit přístupu třetích osob k BYOD VM - jak k souborům VM, tak k datům a aplikacím hostovaného OS s firemním prostředím.

Zaměstnanec musí pro vstup do BYOD programu potvrdit souhlas s BYOD politikou a směrnicemi, čímž se zaváže dodržovat bezpečnostní pravidla a chránit data zaměstnavatele.

V rámci zachování bezpečnosti je zaměstnanec povinen umožnit pověřené osobě kontrolu soukromého prostředí, zda je v souladu s požadavky programu.

Zajištění servisu

V případě poruchy BYOD notebooku je třeba umožnit zaměstnanci pracovat, aby mu nevznikla překážka v práci. Po dobu servisu má uživatel možnost využít zápůjčky služebního notebooku od IT oddělení. Tato služba bude poskytnuta zdarma. Po dobu používání náhradního notebooku bude zaměstnanci pozastaveno vyplácení měsíčního příspěvku. Maximální doba zápůjčky je 10 dní ročně. Po překročení desetidenní doby může zaměstnanec zápůjčku využít, ale bude zpoplatněna.

Zároveň je uživatel povinen si zajistit nadstandardní servis s vyřešením do 5 pracovních dnů. Možnost bezplatné zápůjčky by tak uživateli měla pokrýt ročně dva servisy soukromého notebooku.

Pravidla pro servis notebooků vypracuje oddělení bezpečnosti s ohledem na možná bezpečnostní rizika, popsaná v kapitole *2.4 Analýza bezpečnostních rizik*.

Použití BYOD VM

Uživatel má právo používat BYOD VM pouze na jednom vybraném soukromém notebooku.

Pro použití BYOD VM platí stejná pravidla, jako pro používání služebního notebooku.

Uživatel má právo pouze na vzdálenou podporu při problémech souvisejících s BYOD VM. Podporu pro provoz VMware Player/Fusion a svého systému získá uživatel ve znalostní bázi BYOD.

Po dobu používání BYOD notebooku čerpá uživatel náhradu za opotřebení soukromého hardware.

Vystoupení z programu BYOD pro notebooky

Uživatel má právo vystoupit z programu BYOD pro notebooky a vyměnit BYOD notebook za služební. Výpovědní lhůta z programu je 2 měsíce. Dnem ukončení členství uživatele v programu dojde k vyřazení BYOD VM a uživateli přestanou být vypláceny náhrady.

3.1.4 Další oddělení

Poskytnutí náhrady

Podle zákoníku práce (zákon č. 262/2006 Sb., zákoník práce) vyplácí zaměstnavatel zaměstnanci dohodnutou náhradu za opotřebení vlastního zařízení potřebného pro výkon práce.

Výpočet výše náhrady byl navržen v kapitole *2.7 Náklady*. Vzhledem k tomu, že výše náhrady je významná motivace ke vstupu do BYOD programu, bylo by vhodné poskytovat náhradu na vyšší úrovni, například 500 - 700 Kč měsíčně, což by odpovídalo představám největšího počtu respondentů z předběžného průzkumu v kapitole *2.5 Průzkum mezi zaměstnanci*.

Zajištění výhod u dodavatelů

Zaměstnavatel zajistí výhodnější podmínky u dodavatelů díky své vyjednávací pozici na:

- licence VMware Player/Fusion,
- operační systém,
- notebooky,
- servis notebooků,
- pojištění notebooků.

Tyto výhody budou moci čerpat všichni uživatelé BYOD.

3.2 Návrh základních procesů

Návrh procesů slouží jak pro přiblížení možné implementace programu BYOD ve společnosti TCZ, tak jako východisko k modelování procesů v rámci projektu. Sleduje tak cíl - *3. Vytvořit rámec pro projekt BYOD pro notebooky*.

3.2.1 Přihlášení do programu

Přihlášení do programu BYOD bude zpřístupněno stávajícím zaměstnancům v systému IAM (Identity and Access Management), který je v TCZ používán k centrální správě přístupů.

V případě, že se do BYOD programu rozhodne vstoupit nový zaměstnanec a bude splňovat podmínky, zadá za něho žádost příslušný nadřízený pracovník.

Vstup zaměstnance do programu BYOD schvaluje jeho nadřízený a garant programu. Může se stát, že vstup zaměstnance do programu nebude žádoucí. Příkladem jsou zaměstnanci, pracující s citlivými údaji. Tito zaměstnanci pracují na desktopu z důvodu zvýšení bezpečnosti a zvýšení mobility jejich počítače by znamenalo zvýšení rizika. V takovém případě zamítne garant nebo zaměstnancův nadřízený požadavek.

Po schválení požadavku nadřízeným a garantem musí zaměstnanec potvrdit svůj souhlas s pravidly programu BYOD. Pravidlům se podrobněji věnuje předchozí kapitola 3.1.

Následně zaměstnanec absolvuje školení ve virtuální univerzitě, která je dostupná na intranetu TCZ a je centrálním systémem pro absolvování online kurzů. V závěru školení BYOD složí zaměstnanec závěrečnou zkoušku, čímž prokáže svou způsobilost a znalost podmínek programu BYOD.

Přihlášení lze shrnout do následujících kroků:

1. Zaměstnanec zažádá o vstup do programu.
2. Požadavek schválí zaměstnancův nadřízený a garant programu.
3. Zaměstnanec potvrdí souhlas s pravidly programu.
4. Zaměstnanec absolvuje školení a zkoušku.
5. Zaměstnanec splnil podmínky a stává se uživatelem BYOD.

3.2.2 Distribuce VM

Po splnění kroků předchozího procesu je vytvořen požadavek na IT oddělení. To vytvoří uživateli BYOD nový virtuální stroj. Ten je následně pracovníkem IT nahrán do úložiště VM.

Po nahrání jsou uživateli doručeny potřebné přístupové údaje, včetně těch k přihlášení do úložiště VM.

Uživatel se připojí z BYOD notebooku do vnitřní sítě, kde má zpřístupněné úložiště VM. Po autentizaci uživatel stáhne svou BYOD VM do počítače a dle dostupného návodu provede instalaci VMware Player a následně BYOD VM.

Distribuci lze shrnout do kroků:

1. IT oddělení dostane požadavek na vytvoření nové BYOD VM.
2. IT oddělení vytvoří novou BYOD VM a umístí do úložiště BYOD VM.
3. Zaměstnanec je informován a dostane pokyny s přihlašovacími údaji.
4. Zaměstnanec si z úložiště VM stáhne svou BYOD VM.
5. Zaměstnanec si nainstaluje VMware Player/Fusion a svou BYOD VM.

3.2.3 Provoz VM

Proces správy a provozu pracovního prostředí je shodný jak v BYOD VM, tak na služebním notebooku. Je tedy možné využít zavedené postupy.

Provoz prostředí pro běh BYOD VM (operačního systému a hypervizoru) zajišťuje uživatel dodržováním pravidel BYOD programu.

V případě poruchy BYOD notebooku začne uživatel problém řešit. Pokud se jedná o závažnější poruchu (na hardware nebo operačním systému), kterou nelze vyřešit rychle, využije zápůjčky náhradního notebooku od IT oddělení, na kterém bude po dobu trvání poruchy pracovat, a zajistí servis BYOD notebooku. V případě, že bude nutné znovu nainstalovat BYOD VM, zažádá zaměstnanec IT oddělení buď o vytvoření nové VM, nebo v případě, že se nezmění hardwarová konfigurace, využije původní BYOD VM z úložiště VM.

3.2.4 Vyřazení VM

Důvody vyřazení VM

K vyřazení VM může dojít ze třech důvodů. Prvním je přirozené ukončení životního cyklu image, který je plánován na 4 roky. Po 4 letech VM expiruje a není možné ji spustit. Je buď vydána nová VM standardním postupem, nebo prodloužena platnost stávající. Druhým důvodem je uživatelovo opuštění BYOD programu buď kvůli přechodu na služební notebook, nebo kvůli odchodu uživatele ze společnosti. Třetím možným důvodem vyřazení VM je její poškození, případně kompletní zničení, například z důvodu krádeže notebooku, zničení disku nebo hostitelského stroje.

Průběh vyřazení VM

Pokud nastane jeden z důvodů pro vyřazení VM je zaměstnanec povinen bezpečně smazat soubory BYOD VM z disku a případně dalších umístění (neplatí v případě zcizení nebo kompletního zničení).

IT oddělení vyřadí pracovní prostředí v BYOD VM z domény a provede záznam do konfigurační databáze stejně, jako u standardních firemních notebooků.

4 Návrh VM

S ohledem na identifikovaná rizika, požadavky a další body analýzy z kapitoly *2.4 Analýza bezpečnostních rizik* je navržena modelová VM, která má za cíl identifikovat optimální konfiguraci pro BYOD VM a prověřit funkčnost návrhu.

Touto kapitolou je naplněn cíl práce - *5. Vytvořit a otestovat model technického řešení BYOD pro notebooky*.

4.1 Konfigurace VM

Požadavky pro konfiguraci VM vyplývají z předchozích kapitol a nejvýznamnějšími z nich jsou:

- plynulý běh hostovaného OS Windows 7,
- úplné oddělení hostovaného a hostitelského prostředí,
- zabezpečení VM před neoprávněným zásahem a krádeží.

4.1.1 Systémová nastavení

Při zvažování vhodné konfigurace byly vzaty v úvahu minimální konfigurace OS Windows 7 a software, instalovaného ve VM (zejména Microsoft Office). Konfigurace vychází i z doporučení v manuálu, který je součástí aplikace Workstation.

Následující nastavení bylo navrženo podle VMware Workstation 10.

Obecné

Hostovaný operační systém - tato možnost ovládá profil kompatibility s hostovaným operačním systémem. Je zvolen Windows 7.

Automatické nabootování VM při spuštění VMware Player/Fusion - pro uživatele s jedinou VM je vhodné použít a proto je možnost povolena.

Sdílení složek

Sdílení složek je z popsaných bezpečnostních důvodů zakázáno.

Výchozí aplikace

Tato volba umožňuje spouštět aplikace mezi hostovaným a hostitelským systémem. V konfiguraci VM jsou všechny možnosti volby zakázány.

Menu aplikací

Menu aplikací umožňuje přímo spouštět konkrétní aplikace hostovaného systému z hostitelského. Ve VM je tato volba zakázána z důvodu oddělení obou systémů.

Klávesnice a myš

Tato konfigurační položka umožňuje přizpůsobit mapování klávesnice v závislosti na druhu hostitelského a hostovaného systému. Jsou nastaveny výchozí hodnoty.

Procesor a paměť

Pro plynulý běh hostovaného systému jsou VM nastavena 2 jádra procesoru. BYOD notebook splňující minimálními požadavky (procesor Intel i5) disponuje čtyřmi jádry, tudíž budou 2 jádra vyhrazena pro hostovaný OS a 2 pro hostitelský.

Velikost paměti VM je zvolena 2 048 MB.

Volba pokročilých virtualizačních funkcí - možnosti provozování hypervizorových aplikací ve VM a profilování aplikačního kódu podle využití procesoru jsou zakázány.

Zobrazení

Akcelerace 3D grafiky je povolena kvůli plynulejšímu běhu hostovaného OS. V případě Mac zařízení je povoleno použití plného rozlišení Retina displeje a automatické přizpůsobení uživatelského rozhraní Windows je také povoleno, kvůli zlepšení tzv. user experience.

4.1.2 Periferie a zařízení

Síť

Použita je konfigurace bridge. Síťové rozhraní hostitele je sdíleno pro hostitelský OS i pro VM. Zařízení vystupuje v síti pod jedním fyzickým síťovým rozhraním, na kterém je provoz filtrován pro hostitelský i pro hostovaný OS. Hostovaný OS získá v síti IP adresu a vystupuje jako samostatné zařízení. Virtuální síťový adaptér je nastavený tak, aby replikoval stav síťového adaptéru v hostitelském OS.

Disk

Velikost disku VM (vmdk souboru) je nastavena na 50 GB, které pokryjí požadavky OS a firemních aplikací včetně prostoru pro uživatelská data. Typ sběrnice je SCSI LSI Logic SAS.

Vyhrazení celého prostoru na disku předem je zakázáno a disk tak bude přirůstat postupně až do maximální velikosti 50 GB. Rozdělení virtuálního disku do více vmdk souborů je povoleno z důvodu snížení fragmentace disku.

Optická mechanika

Optická mechanika je ve VM povolena přes virtuální SATA rozhraní. Je detekována automaticky.

Zvuková karta

Přístup ke zvukové kartě je VM povolen.

USB a Bluetooth

Připojování USB zařízení do VM je povoleno. Kompatibilita je nastavena až do verze USB 3.0. Výchozí akce po zapojení USB zařízení je jeho připojení do běžící VM.

Sdílení Bluetooth zařízení s hostovanými Windows 7 je vypnuto.

Sdílení tiskáren

Sdílení tiskáren hostitele s hostem je zakázáno a možnost sdílení tiskáren je z konfigurace zcela odebrána.

4.1.3 Zabezpečení

Šifrování VM

Šifrování je zapnuté. Heslo pro šifrování je známé uživateli. Šifrování nemůže uživatel vypnout, pokud je VM chráněna restricted módem.

Restricted mode

Restricted mód je zapnutý a chráněný heslem administrátora VM z IT oddělení. Toto heslo je unikátní a nesmí být uživateli sděleno.

Ve zprávě uživateli je nastaven text s informací, že tato VM je majetkem společnosti TCZ a nesmí být dále šířena. Je doplněna o kontakt na IT helpdesk pro případné řešení problémů.

Vyžadování změny hesla k šifrované oblasti disku je zapnuto.

Připojení USB zařízení je povoleno.

Expirace VM je nastavena na 4 roky, jako je životní cyklus stanice.

Po povolení Restricted módu je většina konfiguračních položek uživateli nepřístupná. Přístupné jsou pouze:

- automatický start VM při startu aplikace VMware Player/Fusion,
- možnosti zobrazení aplikačního menu VM v hostitelském OS,
- nastavení profilů klávesnice a myši,
- nastavení USB (USB je povoleno),
- odemknutí VM z Restricted módu.

Obsah souboru .vmx s touto konfigurací je uveden na DVD přiloženém k práci. Konfigurace je vypsána bez zapnutého šifrování. V případě aktivního šifrování jsou soubor .vmx a další konfigurační soubory zašifrovány.

BIOS

Virtuální stanice má svůj BIOS, který se při každém spuštění znovu vytváří (Shackleford, 2013). Jeho konfigurace se odvíjí od konfigurace VM a není nutné ho zabezpečovat administrátorským heslem tak, jako na fyzických počítačích.

Kroky k dalšímu zabezpečení BIOS jsou uvedeny v kapitole 4.1.5 Konfigurace souboru VMX a provádějí se přímou editací konfiguračního souboru pomocí vkládání parametrů isolation.bios.* .

4.1.4 Ostatní

Nastavení kompatibility VMware

Je nastavena nejnovější verze virtuálního hardware - 10. Je kompatibilní s produkty Player/Workstation 10 a Fusion (Pro) 6. Automatický upgrade virtuálního hardware je zakázán. V případě dostupné nové verze tak nedojde k automatickému přechodu na vyšší. Zakázáním této možnosti klesá riziko chyb z neotestované konfigurace.

Izolace VM

Pro VM je zakázána funkce Drag and Drop[12] a sdílení schránky pro funkci kopírovat/vložit mezi hostitelským OS a hostitelem.

Pokročilé

Synchronizace času je zakázána. Čas synchronizuje hostovaný OS s firemním časovým serverem.

Přenos informace o napájení do VM je povoleno. Díky tomu má například ve full screen módu uživatel možnost sledovat zbývající čas baterie.

Preferovaná technologie virtualizace je nastavena na automatickou. Hypervizor rozhodne při spouštění VM o tom, zda využije technologii překladu binárního kódu nebo virtualizační funkce implementované v procesoru (např. Intel VT-x nebo AMD-V).

Možnost ladění je zakázána. Hypervizor neprotokoluje chyby a problémy a tím je běh VM rychlejší.

Přednačítání dat disku je zvoleno automatické. V případě, že má hostitelský stroj vhodný OS a dostatek operační paměti, je přednačítání automaticky zapnuto a tím dojde ke zvýšení výkonu VM.

Přenášení vzdáleného obrazu přes protokol VNC je zakázáno z důvodu bezpečnosti.

4.1.5 Konfigurace souboru VMX

Některé parametry VM není možné nastavit pomocí GUI ve Workstation a proto je nutné je nastavovat manuálně editací nezašifrovaného .vmx souboru. Pro zvýšení bezpečnosti, spojené mimo jiné s funkcemi VMware Tools, doporučuje VMware v manuálu pro VMware Tools (VMware, 2012) nastavit textově některé další parametry.

VMware dává administrátorům VM možnost zvolit, jak se bude VM chovat při zkopírování na jiný stroj, případně do jiného umístění. VMware Player počítá identifikátor virtuálního hardwaru UUID z hardwarového ID procesoru (CPUID) a názvu souboru včetně jeho umístění. Aby se VM chovala podobně, jako fyzický systém (který si vytváří UUID z hardwarové konfigurace), je nastavena automatická změna UUID - což odpovídá volbě "copy", pokud by byla změna UUID řešena uživatelskou interakcí v dialogovém okně VMware Player. Pro administrátory VM tak bude překopírovaný stroj vypadat jako další nové zařízení v síti.

---

[12] Drag and Drop = funkce pro "přetahování" objektů mezi hostitelským a hostovaným OS

Parametr k nastavení automatické změny UUID:

```
uuid.action = "create"
```

VMware doporučuje zakázat funkci pro zmenšování velikosti souborů virtuálních disků z důvodu jejího trvání a hrozbě DoS - odmítnutí služby z důvodu zaneprázdnění disku. Nastavuje se parametry:

```
isolation.tools.diskWiper.disable = "TRUE"
isolation.tools.diskShrink.disable = "TRUE"
```

Dále VMware doporučuje explicitně zakázat sdílení schránky hosta a hostitele:

```
isolation.tools.copy.disable = "TRUE"
isolation.tools.paste.disable = "TRUE"
```

VMware doporučuje zakázat připojování a úpravu zařízení. V případě BYOD VM je připojování zařízení povoleno z důvodu zachování podpory přenosných paměťových zařízení, externích disků, mobilních telefonů nebo třeba tiskáren.

Dalším aplikovaným nastavením je zákázání protokolu pro komunikaci mezi VM běžící v jednom hypervizoru:

```
vmci0.unrestricted = "FALSE"
```

Hypervizor může poskytovat informace o výkonu hostovanému systému. Ty využívá například komponenta Windows PerfMon pro monitorování výkonu hardware. Funkce může znamenat bezpečnostní slabinu a VMware ji doporučuje zakázat:

```
tools.guestlib.enableHostInfo = "FALSE"
```

Doporučeno je nastavení následujících parametrů, které zakazují některé integrační funkce a pomáhají izolovat hostovaný a hostitelský systém:

```
isolation.tools.unity.push.update.disable = "TRUE"
isolation.tools.ghi.launchmenu.change = "TRUE"
isolation.tools.ghi.autologon.disable = "TRUE"
isolation.tools.hgfsServerSet.disable = "TRUE"
isolation.tools.memSchedFakeSampleStats.disable = "TRUE"
isolation.tools.getCreds.disable = "TRUE"
```

(Shackleford, 2013) doporučují kromě popsaných parametrů dále nastavení tzv. VM Self-Awarness, tedy možnost rozpoznání virtuálního prostředí v hostovaném systému. Tímto nastavením zvýšíme úroveň izolace hostovaného a hostitelského systému:

```
isolation.monitor.control.disable = "TRUE"
```

Dále doporučuje zakázání VIX API a VMsafe API:

```
isolation.tools.vixMessage.disable = "TRUE"
vmsafe.enable = "FALSE"
```

Na základě doporučení (Shackleford, 2013) byla navíc aplikována následující souhrnná bezpečnostní opatření nastavením parametrů:

```
isolation.bios.bbs.disable = "TRUE"
isolation.tools.ghi.protocolhandler.info.disable = "TRUE"
isolation.ghi.host.shellAction.disable = "TRUE"
isolation.tools.dispTopoRequest.disable = "TRUE"
isolation.tools.trashFolderState.disable = "TRUE"
isolation.tools.ghi.trayicon.disable = "TRUE"
isolation.tools.unity.disable = "TRUE"
isolation.tools.unityInterlockOperation.disable = "TRUE"
isolation.tools.unity.taskbar.disable = "TRUE"
isolation.tools.unityActive.disable = "TRUE"
isolation.tools.unity.windowContents.disable = "TRUE"
isolation.tools.vmxDnDVersionGet.disable = "TRUE"
isolation.tools.guestDnDVersionSet.disable = "TRUE"
```

Jedná se o zakázání hosta přistupovat do virtuálního BIOS, zjišťovat topologii hostitelských disků, zakázání Unity módu pro integraci oken hosta v prostředí hostitele a celkové zvýšení izolace hosta od hostitele.

Výše popsaná opatření jsou aplikovatelná jak pro produkty pro desktopovou virtualizaci - Workstation, Player nebo Fusion, tak pro produkty pro serverovou virtualizaci ESX a ESXi. Vzhledem k přenositelnosti VM mezi těmito platformami doporučuje (Shackleford, 2013) tato opatření aplikovat vždy pro všechny platformy.

VMware nezveřejnil kompletní seznam konfiguračních parametrů pro VM. Výše popsané parametry byly uveřejněné ve VMware knowledge base jako rady administrátorům ke zvýšení bezpečnosti.

4.1.6 Konfigurace VMware Tools

VMware Tools budou do BYOD VM distribuovány automaticky pomocí systému pro distribuci aplikací na koncové stanice, který spravuje IT oddělení ve firemním prostředí. Instalace VMware Tools uživateli přímo z hypervizoru je zakázána. Před instalací nové verze Tools je nutné otestování kompatibility.

VMware Tools jsou v modelové VM nainstalovány s následujícími komponentami:

- Paravirtual SCSI (ovladač virtuálního disku),
- Memory Control Driver (rozšířená správa paměti),

- USB Mouse Driver (USB ovladač myši),
- SVGA Driver (ovladač grafického rozhraní),
- Audio Driver (ovladač zvukového rozhraní),
- VMXNet3 NIC Driver (ovladač síťového rozhraní),
- Volume Shadow Copy Services Support (podpora stínových kopií svazků Windows).

Ostatní komponenty nejsou nainstalovány dle bezpečnostního pravidla povolovat pouze funkce nutné pro zajištění funkčnosti. Nepotřebné komponenty nebudou tedy nainstalovány.

4.2 Úprava VM pro nového uživatele

Zásadní úpravy bude provádět IT oddělení na straně hostovaného pracovního prostředí. Tyto úpravy jsou shodné, jako u pracovního prostředí ve služebním počítači.

Základní postupy byly vyzkoušeny u testovací VM na úrovni virtuálního stroje.

Přejmenování VM

Při přizpůsobování etalonu uživateli je třeba přejmenovat VM. Jak je popsáno v pravidlech, název VM by měl obsahovat identifikátor zaměstnance.

Nastavení hesel

Při přípravě VM jsou nastavena dvě hesla do VM a jedno do hostovaného OS (Windows 7). Ve VM je nastaveno heslo pro šifrování a heslo pro restricted mód. Heslo pro restricted mód je známo pouze správci. Hesla k šifrování VM a do pracovního prostředí jsou známy uživateli.

Je třeba dodat, že při přípravě modelové VM nebyl nalezen způsob, jak vynucovat politiku hesel (pravidelnou změnu, minimální požadavky na sílu hesla apod.)

Příprava k první aktivaci

V případě testovací VM nebyla příprava k první aktivaci provedena. Pro provoz BYOD pro notebooky je tento krok podstatný a podrobnou specifikaci kroků provede dodavatel řešení při vytváření etalonu. Jedná se zejména o detailní konfiguraci systémových zařízení nebo o nastavení identifikátoru VM UUID.

4.3 Distribuce VM

V kapitole *1.5.3 VMware Workstation 10* byly obecně popsány druhy distribuce VMware virtuálních strojů. Vzhledem k využití VMware Player (Fusion) jako jediného podporovaného hypervizoru pro BYOD VM je výhodné zvolit postup distribuce pomocí zip souborů.

Tato podkapitola se věnuje modelovému technickému návrhu distribuce VM.

Jeho výhodami jsou:

- zachování všech nastavených parametrů,
- distribuce VM v jediném souboru,
- odpadá možnost chyb při konverzi,
- jednoduchá instalace.

Postup při přípravě modelové VM

Složka virtuálního počítače, obsahující soubory <user_id>.vmx, <user_id>.vmdk, <user_id>-s001.vmdk a další (podrobněji popsané v kapitole 1.5.3) je zabalena do souboru zip <user_id>.zip, kde "user_id" je jedinečný identifikátor zaměsntnance.

Soubor <user_id>.zip je pak nahrán do úložiště VM, kterým je webový server pro sdílení souborů umístěný na intranetu. Na tomto serveru je uživateli vytvořen profil s názvem jeho "user_id", vygenerovaným heslem s adresou:

https://<název_serveru_úložiště_VM>/<user_id>.

Postup při získávání modelové VM a instalaci

Uživatel získá přihlašovací údaje k připravené BYOD VM. Součástí přihlašovacích údajů je i licenční klíč pro VMware Player (nebo Fusion) a adresa pro stažení aktuální verze aplikace. Uživatel připojí notebook určený pro BYOD do interní sítě (vzhledem k velikosti VM - cca 25GB použije Ethernetové připojení). Stáhne VMware Player/Fusion pro svůj operační systém a s doručeným licenčním klíčem ho nainstaluje. Následně zadá do prohlížeče adresu svého profilu na úložišti VM a použije doručené přihlašovací údaje.

Po úspěšném přihlášení do úložiště VM získá uživatel přístup k souboru <user_id>.zip, který stáhne do počítače. Po stažení rozbalí uživatel soubor do lokálního úložiště VM, které bylo vytvořeno při instalaci VMware Player/Fusion. Toto umístění už nebude moci později změnit. Po rozbalení souborů a prvním spuštění je BYOD VM nainstalován a připraven k používání.

4.4 Uživatelské testování VM

Postup a konfigurace navržené v předchozích kapitolách byly vyzkoušeny v modelovém testovacím prostředí.

Cílem uživatelského testování je prokázat funkčnost návrhu modelové VM a její distribuce. Naplňuje cíl práce - *5. Vytvořit a otestovat model technického řešení BYOD pro notebooky*.

4.4.1 Příprava testovací VM

Podle modelového postupu tvorby VM z předcházejících kapitol byla vytvořena testovací VM.

VM byla vytvořena v prostředí s konfigurací, která odpovídá minimální konfiguraci BYOD notebooku:

- Procesor: Intel i5,
- Operační paměť: 4 GB,
- Operační systém: Windows 7 Enterprise 64-bit.

Testovací VM (s názvem xpokd00) byla vytvořena ve VMware Workstation 10 podle konfigurace popsané v kapitole 4.1.

Do testovací VM byl nainstalován OS Windows 7 Professional 32-bit ve výchozí konfiguraci.

Na hostovaný operační systém v testovací VM byly nainstalovány VMware Tools s konfigurací ovladačů, navržené v předchozí kapitole.

Vytvořená testovací VM, včetně nainstalovaného hostovaného systému, má velikost 5,08 GB, po zabalení do ZIP archivu pro distribuci pak 5,07 GB.

ZIP archiv odpovídá modelu navrženému v předchozí kapitole a je připraven k distribuci na další zařízení.

4.4.2 Instalace

Instalace proběhla na stroji Apple MacBook Pro 15" 2011 v konfiguraci:

- Procesor: Intel i7,
- Operační paměť: 8 GB,
- Operační systém: OS X 10.9.2 Mavericks.

Před instalací testovací VM byl na cílový notebook nainstalován hypervizor VMware Fusion 6 ve výchozí konfiguraci.

ZIP soubor testovací VM, byl přenesen na cílový notebook překopírováním přes paměťové zařízení. Nebyl testován navržený způsob distribuce přes síťové úložiště VM, ale vzhledem k tomu, že se jedná běžnou operaci, není v tomto kroku předpokládán žádný významnější problém.

ZIP soubor testovací VM byl rozbalen do výchozího umístění virtuálních strojů VMware Fusion - /Users/<uživatel>/Documents/Virtual Machines.localized/xpokd00. Následně byla rozbalená složka VM přejmenována na xpokd00.vmwarevm, aby ji bral operační systém OS X jako balík virtuálního stroje.

Poklikáním na balík xpokd00.vmwarevm byla testovací VM poprvé spuštěna.

4.4.3 Provoz

Ke spuštění VM bylo třeba zadat heslo, kterým je VM zašifrována. Po zadání hesla byla VM spuštěna.

Testovací VM byla orientačně otestována i za běhu. Na testovacím notebooku byl běh systému plynulý, zcela srovnatelný se systémem provozovaným přímo na hardware. Díky nainstalovaným VMware Tools bylo rozlišení obrazovky VM automaticky přizpůsobováno velikosti okna a displeje. Nedocházelo k zasekávání ani tuhnutí.

V oblasti síťové konektivity vystupoval VM jako další zařízení v síti s vlastní IP adresou (díky zvolenému síťovému módu bridge). Zařízení tak bylo na síti přístupné a mohlo poskytovat síťové služby. Ostatní zařízení na lokální síti byla z testovací VM bez problémů dostupná. Přístup z lokální sítě do internetu fungoval také bez problémů.

Po připojení USB paměťového zařízení bylo toto zařízení hostovaným systémem rozpoznáno a automaticky k němu připojeno (dle navržené konfigurace VM). Přenos souborů probíhal standardní rychlostí.

Při pokusu o drag and drop nebo o kopírování do schránky mezi hostitelským a hostovaným OS nebyla tato možnost funkční, v souladu s návrhem. Sdílení souborů také nebylo přístupné a při pokusu o změnu konfigurace spuštěné testovací VM vyzval VMware Fusion k zadání hesla pro odemknutí restricted módu.

Uvedený test modelové VM prokázal funkčnost modelového návrhu i jeho přenositelnost mezi platformami Microsoft Windows 7 a Apple OS X.

4.5 Bezpečnostní testování VM

Bezpečnostní testování je významná činnost, kterou se v TCZ zabývá oddělení bezpečnosti. Před nasazením dodavatelem vytvořené BYOD VM je třeba provést penetrační testy a určit, zda VM odpovídá bezpečnostním požadavkům společnosti.

Cílem této podkapitoly je přiblížit čtenáři dva základní scénáře pro penetrační testy, které budou po rozpracování provedeny na BYOD VM. Je zde uveden i jeden modelový penetrační test.

4.5.1 Modelový penetrační test

Modelový penetrační test má za cíl ověřit zranitelnosti testovací VM vůči hrozbám *H7 a H8 Infiltrace a zachycení komunikace* a hrozbě *H12 Začlenění škodlivých programů*, které, jak bylo uvedeno v kapitole *2.4 Analýza bezpečnostních rizik*, znamenají významná rizika pro BYOD notebook. Využitím takové zranitelnosti by mohl útočník zaznamenávat komunikaci mezi firemním prostředím a vstupními a výstupními zařízeními. Těmi mohou být obrazovka nebo klávesnice. Nejpravděpodobnější forma takového útoku by byla vedena začleněním škodlivého programu do vrstvy hostitelského systému, a proto bude v testu útok takto proveden.

Výchozí podmínky testu

Test je prováděn na stejném systému, jako uživatelské testy, tedy na notebooku Apple MacBook s operačním systémem OS X 10.9.2. Byla použita i stejná testovací VM.

Krok 1: Instalace škodlivého programu

Pro infiltraci hostitelského systému byl zvolen Elite Keylogger 1.2.027[13], který je oficiálně dostupným programem s možností jak skrytého (verzi Pro), tak viditelného sledování uživatele (verze Free). K testu byla použita verze Free. Program byl nainstalován do hostitelského systému OS X standardním způsobem, jako běžná aplikace. Po instalaci bylo změněno nastavení snímkování obrazovky na 5 minut (nejkratší doba pro verzi Free) a povoleno zaznamenávání systémových kláves. Po změně nastavení bylo spuštěno monitorování.

Krok 2: Monitorování

Pro vyzkoušení funkčnosti aplikace bylo monitorování nejprve provedeno v hostitelském systému. Bylo provedeno modelové přihlášení v internetovém prohlížeči do webové

[13] Homepage Elite Keylogger: http://www.widestep.com/elite-keylogger-mac

aplikace. Při následné analýze logů byly nalezeny všechny stisknuté klávesy, tedy i jméno a heslo do webové aplikace. V průběhu přihlašování byl pořízen také snímek obrazovky s celým jejím obsahem. Tím byla ověřena funkčnost aplikace v hostitelském systému.

Dalším krokem bylo vyzkoušení škodlivé aplikace při práci v prostředí testovací VM. Ta byla spuštěna v režimu celé obrazovky a bylo v ní provedeno stejné přihlášení k webové aplikaci, jako z hostitelského systému. Při analýze logů byl nalezen záznam o spuštění aplikace VMware Fusion. Avšak klávesy, které byly stisknuty při práci v prostředí VM zaznamenány nebyly. V logu aplikace byl nalezen snímek obrazovky virtuálního počítače.

Závěr

Penetrační test potvrdil zranitelnost v oblasti zachycení obrazovky virtuálního počítače. Zranitelnost pro zaznamenávání kláves z hostitelského systému potvrzena nebyla. Přesto je možné, že jiný keylogger by klávesy zaznamenat mohl. Záleží na tom, v jaké vrstvě keylogger komunikaci odposlouchává. Úspěšnost keyloggeru by mohl ovlivnit i hostitelský OS. Proto je třeba se tomuto riziku věnovat podrobněji při penetračních testech.

4.5.2 Návrh oblastí bezpečnostních testů

Objektem testování je etalon BYOD VM dodaný IT oddělením, které pro IT vytvoří externí dodavatel.

Testování se bude odehrávat podle dvou základních scénářů. Prvním je offline testování, které se bude věnovat zranitelnostem vypnuté VM. Druhým je online testování, které bude zaměřeno na zranitelnosti, které se váží k běhu VM.

Otestovat zranitelnosti hostitelského prostředí by bylo vzhledem k mnoha jeho typům velmi náročné. Proto budou penetrační testy zaměřeny primárně na hypervizor a VM.

Scénář 1: Offline VM

Výchozí situace je taková, že útočník získá přístup k vypnuté VM, která není natažena v operační paměti a existuje pouze jako soubory na disku hostitelského systému. Může dojít ke krádeži souborů VM, k vyčtení dat nebo k neoprávněnému spuštění VM.

BYOD VM je chráněna šifrováním. Zašifrován je virtuální disk i konfigurace virtuálního hardware, takže by nemělo být možné VM vůbec spustit. Pokud by došlo k prolomení šifrování BYOD VM, jsou ve firemním prostředí implementována další opatření proti krádeži dat. Ta jsou již standardní součástí testů služebních notebooků a není je potřeba testovat zvlášť pro VM.

Scénář 2: Online VM

Při scénáři online testování je BYOD VM spuštěna a pracovní prostředí běží. VM se tak nachází jak ve formě souborů na disku, tak v operační paměti. Na běžící systém pak mohou působit jiné hrozby, než při testu offline VM. Příkladem je hrozba malware zavedeném v hostitelském systému nebo hrozba zachycení komunikace. Součástí online testování je i modelový penetrační test z předchozí kapitoly.

Zranitelnosti testované v rámci tohoto scénáře jsou spojeny s odposloucháváním vstupů a výstupů, pokusy o vykopírování dat, přístup do paměti VM apod.

V rámci penetračního testování je třeba zjistit, jakým způsobem přistupuje VMware Player/Fusion k systémovým zdrojům a jakým způsobem by bylo možné tento přístup narušit. Jedním z takových způsobů narušení by mohl být útok typu man in the middle, tedy získání přístupu ke komunikačnímu kanálu mezi VM a hypervizorem nebo hypervizorem a systémovým prostředkům.

5 Závěr

Předložená diplomová práce si ve svém úvodu kladla několik cílů. Hlavním cílem bylo navrhnout řešení pro zavedení programu BYOD pro notebooky do společnosti Telefónica Czech Republic. Tento cíl byl naplněn pomocí pěti dílčích cílů.

První cíl - **Zpracovat teoretická východiska práce na základě dostupných zdrojů** - byl naplněn rozborem materiálů dostupných v době zpracování předložené práce. Zdrojů k dané problematice se dosud vyskytuje poměrně malé množství a většinu informací lze čerpat především z průzkumů poradenských firem a článků v oborových časopisech. Vzhledem k tomu, že oblast BYOD je aktuální a poptávaná, nezveřejňují poradenské firmy své know-how. Problematika propojení BYOD s distribuovanou virtualizací není k dispozici prakticky vůbec. Lze očekávat, že s rostoucím zájmem o toto téma bude počet spolehlivých zdrojů narůstat a objeví se i nová odborná literatura.

Druhý cíl - **Charakterizovat prostředí ve společnosti ve vztahu k projektu** - byl zpracován v kapitolách *2.1 Aktuální stav používání soukromých zařízení*, *2.2 Projekt BYOD pro notebooky*, *2.3 Související projekty* a *2.5 Průzkum mezi zaměstnanci*. Tento cíl byl naplněn v souladu s očekáváním a bylo zjištěno, že:

1. Využití programu BYOD v praxi společnosti TCZ je žádoucí mimo jiné z toho důvodu, že je již soukromý hardware využíván. Oficiálním zavedením programu by byla snížena bezpečnostní rizika.
2. Daný program by zaměstnanci ať již z ekonomických nebo jiných důvodů uvítali.
3. Využití programu se jeví nástrojem možného snížení nákladů.
4. První kroky, které byly v programu realizovány v rámci společnosti, napovídají, že program bude pro společnost všeobecně přínosný.

Třetí cíl - **Vytvořit rámec pro projekt BYOD pro notebooky** - vycházel ve svých základech jak z teoretické části, tak z kapitoly *2 Analýza pro program BYOD v TCZ*. Klíčová byla pro naplnění tohoto cíle kapitola třetí *Návrh BYOD pro notebooky v TCZ* s podkapitolami *3.1 Pravidla programu*, kde jsem zpracoval podklady pro vytvoření interní směrnice programu BYOD pro notebooky a *3.2 Návrh základních procesů*. Ten byl jako námět k vytvoření procesů velmi kladně přijat odpovědnými zaměstnanci TCZ. Klíčovými body naplnění cíle jsou:

1. Shrnutí informací z obecných zdrojů i z prostředí TCZ k BYOD pro notebooky.
2. Byl vytvořen základ pro interní směrnici k BYOD.
3. Vytvořené základy procesů jsou kvalitním vstupem pro další vývoj procesů.

Naplnění čtvrtého cíle - **Identifikovat a charakterizovat důvody k realizaci projektu (především finanční, bezpečnostní a zaměstnanecké)** - vycházelo z teoretických

poznatků, zejména z uvedených průzkumů. Prakticky byl naplněn ve druhé kapitole *Analýza pro program BYOD v TCZ*. Klíčovým zjištěním bylo:

1. Ve stávajícím prostředí existují bezpečnostní rizika způsobená neznámými zařízeními, která by byla snížena zavedením BYOD programu.
2. Provedením kvalitativní analýzy rizik bylo zjištěno, že rizika plynoucí z neznámého zařízení jsou prokazatelně vyšší, než u BYOD notebooku.
3. Systematická analýza rizik identifikuje významné hrozby, které působí na BYOD notebook a navrhuje opatření.

V IT BSC navrhuji systém cílů a metrik, který podporuje úspěšné zavedení a provoz BYOD programu a při realizaci projektu bude využit. Vhodným způsobem navazuje na strategické cíle společnosti a podporuje jejich naplnění. Mezi projektovými cíli ukazuje kauzální vazby ve strategické mapě.

Na základě modelu nákladů životního cyklu BYOD notebooku a odhadu projektových nákladů byla zjištěna návratnost investice již při 217 uživatelích.

Na základě daných skutečností se projekt jeví jako proveditelný a prospěšný jak společnosti, tak zaměstnancům.

Pátý cíl - **Vytvořit a otestovat model technického řešení BYOD pro notebooky** - je realizován v kapitole *4 Návrh VM*. V rámci naplnění tohoto cíle jsem navrhl konfiguraci VM, podle které jsem modelovou VM následně vytvořil. Tuto VM jsem podle popsaných postupů otestoval. Výsledek testování modelové VM prokázal možnost využití konceptu distribuované virtualizace, ze kterého tato práce vychází. Pokusně jsem provedl penetrační test na zranitelnost modelové VM vůči hrozbám zavedení škodlivého kódu a infiltrace komunikace. V souvislosti s tím jsem ukázal směr pro penetrační testování BYOD VM.

Práce je přínosem jak pro rozvoj projektu BYOD ve společnosti Telefónica Czech Republic, tak i příspěvkem k řešení obdobných problémů v jiných společnostech.

5.1 Posudek garanta z TCZ

Zájem o využití a další pokračování této práce dokládám kladným posudkem garanta z TCZ Jana Černého:

"Posudek garanta diplomové práce Zavedení BYOD pro notebooky v Telefónica Czech Republic

Projekt Bring Your Own Device (BYOD) ve společnosti Telefonica Czech Republic, a.s. byl inicializován v oddělení Bezpečnosti, za účelem vytvořit pravidla pro nefiremní zařízení přistupující do interní sítě společnosti. Na technickém a procesním řešení, která vycházela z vize oddělení Bezpečnost, se nemalou mírou podílel autor diplomové práce David Pokorný. Významně přispěl k přípravě nezbytných podkladů pro rychlou a efektivní implementaci řešení do společnosti.

Pan Pokorný zmapoval problematiku BYOD ve světě, což přispělo k formování BYOD řešení ve společnosti. Aktivně se účastnil všech přípravných projektových schůzek, při nichž prezentoval vlastní nápady, které byly následně do projektového řešení zaneseny (znalostní báze, návody, fóra k problematice do prostředí intranetu společnosti).

Velkým přínosem autora diplomové byla práce provedena analýza přínosů, nákladů a rizik. Tato analýza byla důležitým startovním elementem pro argumenty nasazení BYOD řešení do společnosti a posloužila pro obhajobu potřebných nákladů pro implementaci projektu.

Z technického a procesního pohledu byly užitečné návrhy procesů a možností VMware Playeru, které byly systematicky shrnuty do pravidel BYOD na základě projektových schůzek a informací kolegů.

Diplomová práce ve společnosti bude využita jako projektová příprava k odstartování projektu. Popisuje poměrně širokou problematiku a tím pádem není možné rozepsat úplně jemné detaily, které v rámci projektu bude potřeba detailněji rozpracovat a objasnit.

Jako nejhlavnějším přínosem diplomové práce vidím ucelený dokument, který bude využit jako podkladový materiál pro implementaci BYOD projektu a zároveň představuje neocenitelný zdroj informaci, které do budoucna nebude potřeba složitě vyhledávat v různých zdrojích na internetu, odborné literatuře nebo v produktových materiálech dodavatelů."

Terminologický slovník

Termín	Zkratka	Význam (zdroj)
Bring Your Own Device	BYOD	BYOD je jakékoliv vlastní zařízení přinesené zaměstnancem do prostředí firmy. (Keyes, 2013)
Virtual Machine	VM	Virtuální stroj, anglicky Virtual Machine (VM), je libovolný systém provozovaný nad virtualizovaným hardwarem. Je složen z konfiguračních dat, které od hypervizoru vyžaduje pro svůj běh, a z virtuálního disku, na kterém jsou uložena data hostovaného operačního systému. (Shackleford, 2013)
Virtual Appliance	VA	Virtual Appliance je předkonfigurovaná VM, která může být distribuována v jediném souboru. Obsahuje vždy konfiguraci stroje a může obsahovat i virtuální disky. (Oracle, 2013)
Hypervizor	VMM	Hypervizor (Virtual Machine Monitor) je software, který zpřístupňuje hardwarové zdroje hostitelského systému vituálním strojům. (Shackleford, 2013)
Host OS / Hostitelský OS		Hostitelský operační systémem je operační systém, ve kterém je spuštěna aplikace zajišťující funkci hypervizoru. (Shackleford, 2013)
Guest OS / Hostovaný OS		Hostovaný operační systém je operační systém běžící ve virtuálním prostředí zajištěném hypervizorem. (Shackleford, 2013)
Virtual Desktop Infrastructure	VDI	VDI je množina technických prostředků sloužící ke zpřístupnění virtuálního pracovního prostředí uživateli. Zahrnuje jak virtualizační servery, tak síťovou infrastrukturu. (autor)
MDM	Mobile Device Management	MDM je soubor procesů a technologií, který zabezpečuje, monitoruje, řídí a spravuje mobilní zařízení různých značek a vlastníků. (Keyes, 2013)

Seznam literatury

ASHFORD, W. Nearly half of firms supporting BYOD report data breaches. computerweekly.com [online] [aktualizováno: 2012-08-09] [cit. 2014-04-03] Dostupný z: <http://www.computerweekly.com/news/2240161202/Nearly-half-of-firms-supporting-BYOD-report-data-breaches>

CITRIX, Inc. Citrix Mobility Report: A Look Ahead. slideshare.net [online] [aktualizováno: 2013-12] [cit. 2014-04-03] Dostupný z: <http://www.slideshare.net/citrix/citrix-mobility-report-a-look-ahead>

CITRIX, Inc. IT Organizations Embrace Bring-Your-Own Devices. Global BYO Index. citrix.com [online] [aktualizováno: 2011-10-02] [cit. 2014-04-02] Dostupný z: <http://www.citrix.com/go/lp/pgm/byoindex2011>

DIGNAN, L. Researcher: Critical vulnerability found in VMware's desktop apps. zdnet.com [online] [aktualizováno: 2008] [cit. 2014-03-22], Dostupný z: <http://www.zdnet.com/blog/security/researcher-critical-vulnerability-found-in-vmwares-desktop-apps/902>

DOHERTY, S. BYOD is not for everybody, and especially not for executives. techrepublic.com [online] [aktualizováno: 2013-03-26] [cit. 2014-04-02] Dostupný z: <http://www.techrepublic.com/blog/tech-decision-maker/byod-is-not-for-everybody-and-especially-not-for-executives/8220/>.

FORRESTER CONSULTING. Key Strategies To Capture And Measure The Value Of Consumerization Of IT. trendmicro.com [online] [aktualizováno: 2012-05] [cit. 2014-03-01] Dostupný z: <http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf>

GARTNER. Employee Attitudes Toward Bring Your Own Device. gartner.com [online] [aktualizováno: 2013-12-06] [cit. 2014-04-29] Dostupný z: <http://www.gartner.com/it-glossary/bring-your-own-device-byod>

KAPLAN, R., NORTON, D. *Balanced Scorecard: Strategický systém měření výkonnosti podniku.* 4. vyd. Praha: Management Press, 2005, 267 s. ISBN 80-726-1124-0.

KEYES, J. *Bring your own devices (BYOD) survival guide.* 1. vyd. Boca Raton: CRC Press, 2013, 443 s. ISBN 978-1-4665-6504-3. (eBook PDF)

KRÁL, Bohumil. *Manažerské účetnictví: strategický systém měření výkonnosti podniku*. 2., rozš. vyd. Praha: Management Press, 2006, 622 s. ISBN 80-726-1141-0.

MARYŠKA, M. *Referenční model řízení podnikové informatiky, disertační práce,* VŠE-FIS, Praha, 2010.

NORSA, G. BYOD and ITSM: What you need to know. cio.com.au [online] [aktualizováno: 2013-04-30][cit. 2014-03-31] Dostupný z: <http://www.cio.com.au/article/460465/byod_itsm_what_need_know/>

ORACLE, Corp. Oracle VM VirtualBox User Manual. virtualbox.org [online] [verze: 4.3.6] [cit. 2014-04-15] Dostupný z: <download.virtualbox.org/virtualbox/UserManual.pdf>

POKORNÝ, D. *Analýza rizik bezpečnosti informačních systémů – volba metodiky, bakalářská práce, VŠE-FIS,* Praha, 2012.

PROACTIVE. The impact of BYOD trends on ITSM. proactiveservices.com.au [online] [aktualizováno: 2013] [Získáno 2014-04-05] Dostupný z: <http://www.proactiveservices.com.au/download.asp?file=/uploads/Guidance%20-%20BYOD%20and%20ITSM.pdf>

ROBINSON, S. In Enterprise Mobility, BYOD is Just the Beginning. comptia.org [online] [aktualizováno: 2013-04-09] [cit. 2014-04-06] Dostupný z: <http://www.comptia.org/news/blog/view/13-04-09/In_Enterprise_Mobility_BYOD_is_Just_the_Beginning.aspx>

RUEST, D., RUEST N. *Virtualizace: podrobný průvodce*. Vyd. 1. Brno: Computer Press, 2010, 408 s. ISBN 978-80-251-2676-9.

SHACKLEFORD, D., RUEST, N. *Virtualization security: Protecting Virtualized Environments*. Vyd. 1. Hoboken, N.J.: Wiley, 2013, 360 s. ISBN 978-1-118-33375-4. (eBook)

SHAH, A. Intel CIO says BYOD programme produced massive productivity gains. cio.uk [online] [aktualizováno: 2013-03-06] [cit. 2014-04-06] Dostupný z: <http://www.cio.co.uk/news/strategy/intel-cio-says-byod-programme-produced-massive-productivity-gains/>

VMWARE, Inc. Desktop and Application Virtualization. vmware.com: [online] [aktualizováno: 2014] [cit. 2014-04-30] Dostupný z: <http://www.vmware.com/products/desktop-virtualization.html>

VMWARE, Inc. Installing and Configuring VMware Tools. vmware.com [online] [aktualizováno: 2012-09] [cit. 2014-04-14] Dostupný z: <http://www.vmware.com/pdf/vmware-tools-installation-configuration.pdf>

VMWARE, Inc. Service Provider Program Guide. vmware.com: [online] [aktualizováno: 2013-04] [cit. 2014-03-24] Dostupný z: <http://www.vmware.com/files/pdf/partners/vspp/VSPP-Program-Guide.pdf>

VMWARE, Inc. VMware Fusion 6. store.vmware.com: [online] [aktualizováno: 2014-03-24] [cit. 2014-03-24] Dostupný z: <http://store.vmware.com/store/vmwde/en_IE/DisplayProductDetailsPage/ThemeID.29219600/productID.285633400>

VMWARE, Inc. VMware Player Plus. store.vmware.com [online] [aktualizováno: 2014-03-24] [cit. 2014-03-24] Dostupný z: <http://store.vmware.com/store/vmwde/en_IE/DisplayProductDetailsPage/ThemeID.29219600/productID.285606200>

VMWARE, Inc. VMware Success Stories. vmware.com: [online] [aktualizováno: 2014-03-24] [cit. 2014-03-24] Dostupný z: <https://upgrade.vmware.com/a/customers/search/account/mysupport/undefined?sort=d&next=981>

VMWARE, Inc. *VMware Workstation - Porovnání*. vmware.com: [online] [aktualizováno: 2014] [cit. 2014-04-25] Dostupný z: <http://www.vmware.com/cz/products/workstation/compare.html>

VMWARE, Inc. *VMware Workstation 10*. Načteno z VMware Store: [online] [aktualizováno: 2014] [cit. 2014-03-24] Dostupný z: <http://store.vmware.com/store/vmwde/en_IE/DisplayProductDetailsPage/ThemeID.29219600/productID.285614000>

Seznam obrázků a tabulek

Základní text

Seznam obrázků

Seznam tabulek

Přílohy

Seznam tabulek

Příloha A: Statistiky BYOD

A.1 Úplné výsledky průzkumu Forrester 2012

Tabulka A-1-1: Výsledky průzkumu Forrester 2012. Zdroj: (Forrester, 2012; Kaplan, 2005).

Název metriky	**% firem, které metriku používá**	**% firem, které naměřilo zvýšení**	**% firem, které naměřilo snížení**
náklady na softwarové licence	60 %	51 %	41 %
náklady na správu a údržbu	59 %	38 %	43 %
náklady na telekomunikační infrastrukturu	58 %	50 %	29 %
náhrady zaměstnancům za hrazené náklady - příspěvky na zařízení	53 %	59 %	26 %
náhrady zaměstnancům za hrazené náklady - příspěvky na platby za hovory	58 %	39 %	39 %
náhrady zaměstnancům za hrazené náklady - příspěvky na platby za data	52 %	34 %	41 %
náklady na výměnu zařízení	51 %	30 %	59 %
náklady na přenos hlasu	50 %	neuvedeno	neuvedeno
náklady na zabezpečení aplikací	49 %	66 %	25 %
náklady na VDI	49 %	45 %	25 %
náklady na zabezpečení zařízení	48 %	63 %	38 %
náklady na integraci back-endu	48 %	64 %	28 %
náklady na servery	47 %	47 %	46 %
poplatky za služby profesionálů	45 %	neuvedeno	neuvedeno
náklady vzniklé k dodržení regulatorních požadavků	48 %	64 %	28 %
náklady na skladování zařízení	44 %	neuvedeno	neuvedeno
náklady na vzdělání a tréninik	43 %	18 %	45 %

Název metriky	**% firem, které metriku používá**	**% firem, které naměřilo zvýšení**	**% firem, které naměřilo snížení**
náklady vázané k přenosu dat	41 %	50 %	35 %
náklady na MDM - Mobile Device Management	40 %	60 %	24 %
náklady na vývoj aplikací	39 %	49 %	42 %
právní poplatky	38 %	neuvedeno	neuvedeno
celkové příjmy	59 %	69 %	11 %
vnímání značky	47 %	neuvedeno	neuvedeno
telekomunikační náklady na zaměstnance	50 %	neuvedeno	neuvedeno
náklady na helpdesk na jednoho zaměstnance	40 %	neuvedeno	neuvedeno
počet hovorů na helpdesk (L1 / L2)	45 %	60 % / 50 %	25 % / 25 %
flexibilní pracovní prostředí	40 %	neuvedeno	neuvedeno
produktivita zaměstnanců	43 %	82 %	11 %
náklady IT sítě na zaměstnance	32 %	neuvedeno	neuvedeno
tržní výhoda	28 %	neuvedeno	neuvedeno

Příloha B: Hodnocení rizik

B.1 Hodnocení rizik služebního notebooku

Tabulka B-1-1: Hodnocení rizik služebního notebooku. Zdroj:autor.

Hrozba	**Důvěrnost**			**Dostupnost**			**Integrita**		
	P	**D**	**R**	**P**	**D**	**R**	**P**	**D**	**R**
H1: Falšování uživatelské identity identifikovatelnými osobami	1	3	**3**	1	1	**1**	1	2	**2**
H2: Falšování uživatelské identity smluvními poskytovateli služeb	1	3	**3**	1	1	**1**	1	2	**2**
H3: Falšování uživatelské identity cizími osobami	1	3	**3**	1	1	**1**	1	2	**2**
H4: Neoprávněné použití aplikace	2	2	**4**	0	0	**0**	1	1	**1**
H5: Zavedení destruktivních a škodlivých programů	1	3	**3**	1	3	**3**	2	3	**6**
H6: Zneužití systémových prostředků	1	3	**3**	2	1	**2**	1	1	**1**
H7: Infiltrace komunikace	2	2	**4**	1	2	**2**	2	2	**4**
H8: Zachycení komunikace	2	2	**4**	1	1	**1**	1	1	**1**
H9: Manipulace komunikace	1	1	**1**	1	2	**2**	2	3	**6**
H10: Odmítnutí odpovědnosti	1	1	**1**	1	1	**1**	1	1	**1**
H11: Selhání komunikace	1	1	**1**	2	2	**4**	2	2	**4**
H12: Začlenění škodlivých programů	2	3	**6**	2	3	**6**	2	3	**6**
H13: Chybné směrování	2	2	**4**	0	0	**0**	0	0	**0**
H14: Technická závada počítače	0	0	**0**	2	3	**6**	2	2	**4**
H15: Technická závada paměťového zařízení	0	0	**0**	2	2	**4**	2	2	**4**
H16: Technická závada tiskového zařízení	0	0	**0**	1	2	**2**	0	0	**0**
H17: Technická závada síťového distribučního prvku	0	0	**0**	2	2	**4**	1	1	**1**
H18: Technická závada síťové brány	0	0	**0**	2	2	**4**	1	1	**1**

Hrozba	**Důvěrnost**			**Dostupnost**			**Integrita**		
	P	**D**	**R**	**P**	**D**	**R**	**P**	**D**	**R**
H19: Technická závada počítače pro řízení / správu sítě	0	0	**0**	2	2	**4**	0	0	**0**
H20: Technická závada síťového rozhraní	0	0	**0**	2	2	**4**	1	1	**1**
H21: Technická závada síťové služby	0	0	**0**	2	2	**4**	1	1	**1**
H22: Selhání napájení	0	0	**0**	2	3	**6**	2	2	**4**
H23: Selhání klimatizace	0	0	**0**	2	2	**4**	1	1	**1**
H24: Selhání systémového nebo síťového programového vybavení	1	1	**1**	1	3	**3**	1	3	**3**
H25: Selhání aplikačního programového vybavení	1	1	**1**	1	2	**2**	1	2	**2**
H26: Provozní chyba	1	2	**2**	2	2	**4**	1	2	**2**
H27: Chyba údržby technického vybavení	1	2	**2**	1	3	**3**	1	1	**1**
H28: Chyba úpravy programového vybavení	1	2	**2**	1	2	**2**	1	2	**2**
H29: Chyba uživatele	1	2	**2**	1	2	**2**	2	3	**6**
H30: Požár	0	0	**0**	2	2	**4**	0	0	**0**
H31: Poškození vodou	0	0	**0**	2	3	**6**	0	0	**0**
H32: Přírodní katastrofa	0	0	**0**	1	2	**2**	0	0	**0**
H33: Nedostatek personálu	0	0	**0**	1	2	**2**	0	0	**0**
H34: Krádež provedená identifikovatelnými osobami	1	3	**3**	2	3	**6**	0	0	**0**
H35: Krádež provedená cizími osobami	1	3	**3**	2	3	**6**	0	0	**0**
H36: Úmyslné poškození identifikovatelnými osobami	0	0	**0**	2	3	**6**	0	0	**0**
H37: Úmyslné poškození cizími osobami	0	0	**0**	2	3	**6**	0	0	**0**
H38: Terorismus	0	0	**0**	0	0	**0**	0	0	**0**
Suma rizik			**56**			**120**			**69**

B.2 Hodnocení rizik BYOD notebooku

Tabulka B-2-1: Hodnocení rizik BYOD notebooku. Zdroj:autor.

Hrozba	**Důvěrnost**			**Dostupnost**			**Integrita**		
	P	**D**	**R**	**P**	**D**	**R**	**P**	**D**	**R**
H1: Falšování uživatelské identity identifikovatelnými osobami	1	3	**3**	1	1	**1**	1	2	**2**
H2: Falšování uživatelské identity smluvními poskytovateli služeb	1	3	**3**	1	1	**1**	1	2	**2**
H3: Falšování uživatelské identity cizími osobami	1	3	**3**	1	1	**1**	1	2	**2**
H4: Neoprávněné použití aplikace	2	2	**4**	0	0	**0**	1	1	**1**
H5: Zavedení destruktivních a škodlivých programů	2	3	**6**	2	3	**6**	2	3	**6**
H6: Zneužití systémových prostředků	2	3	**6**	2	1	**2**	2	1	**2**
H7: Infiltrace komunikace	2	3	**6**	1	2	**2**	2	2	**4**
H8: Zachycení komunikace	2	3	**6**	1	1	**1**	1	1	**1**
H9: Manipulace komunikace	1	1	**1**	1	2	**2**	2	3	**6**
H10: Odmítnutí odpovědnosti	1	1	**1**	1	1	**1**	1	1	**1**
H11: Selhání komunikace	1	1	**1**	2	2	**4**	2	2	**4**
H12: Začlenění škodlivých programů	2	3	**6**	3	3	**9**	3	3	**9**
H13: Chybné směrování	2	2	**4**	0	0	**0**	0	0	**0**
H14: Technická závada počítače	0	0	**0**	2	3	**6**	2	2	**4**
H15: Technická závada paměťového zařízení	0	0	**0**	2	2	**4**	2	2	**4**
H16: Technická závada tiskového zařízení	0	0	**0**	1	2	**2**	0	0	**0**
H17: Technická závada síťového distribučního prvku	0	0	**0**	2	2	**4**	1	1	**1**
H18: Technická závada síťové brány	0	0	**0**	2	2	**4**	1	1	**1**
H19: Technická závada počítače pro řízení / správu sítě	0	0	**0**	2	2	**4**	0	0	**0**

Hrozba	**Důvěrnost**			**Dostupnost**			**Integrita**		
	P	**D**	**R**	**P**	**D**	**R**	**P**	**D**	**R**
H20: Technická závada síťového rozhraní	0	0	**0**	2	2	**4**	1	1	**1**
H21: Technická závada síťové služby	0	0	**0**	2	2	**4**	1	1	**1**
H22: Selhání napájení	0	0	**0**	2	3	**6**	2	2	**4**
H23: Selhání klimatizace	0	0	**0**	2	2	**4**	1	1	**1**
H24: Selhání systémového nebo síťového programového vybavení	1	1	**1**	2	3	**6**	2	3	**6**
H25: Selhání aplikačního programového vybavení	1	1	**1**	2	3	**6**	1	2	**2**
H26: Provozní chyba	1	2	**2**	3	3	**9**	2	2	**4**
H27: Chyba údržby technického vybavení	2	3	**6**	1	3	**3**	1	1	**1**
H28: Chyba úpravy programového vybavení	1	2	**2**	1	2	**2**	1	2	**2**
H29: Chyba uživatele	1	2	**2**	2	3	**6**	2	3	**6**
H30: Požár	0	0	**0**	2	2	**4**	0	0	**0**
H31: Poškození vodou	0	0	**0**	2	3	**6**	0	0	**0**
H32: Přírodní katastrofa	0	0	**0**	1	2	**2**	0	0	**0**
H33: Nedostatek personálu	0	0	**0**	1	2	**2**	0	0	**0**
H34: Krádež provedená identifikovatelnými osobami	2	3	**6**	2	3	**6**	0	0	**0**
H35: Krádež provedená cizími osobami	2	3	**6**	2	3	**6**	0	0	**0**
H36: Úmyslné poškození identifikovatelnými osobami	0	0	**0**	2	3	**6**	0	0	**0**
H37: Úmyslné poškození cizími osobami	0	0	**0**	2	3	**6**	0	0	**0**
H38: Terorismus	0	0	**0**	0	0	**0**	0	0	**0**
Suma rizik			**76**			**142**			**78**

B.3 Hodnocení rizik neznámého notebooku

Tabulka B-3-1: Hodnocení rizik neznámého notebooku. Zdroj:autor.

Hrozba	**Důvěrnost**			**Dostupnost**			**Integrita**		
	P	**D**	**R**	**P**	**D**	**R**	**P**	**D**	**R**
H1: Falšování uživatelské identity identifikovatelnými osobami	2	3	**6**	1	1	**1**	1	2	**2**
H2: Falšování uživatelské identity smluvními poskytovateli služeb	2	3	**6**	1	1	**1**	1	2	**2**
H3: Falšování uživatelské identity cizími osobami	3	3	**9**	1	1	**1**	1	2	**2**
H4: Neoprávněné použití aplikace	3	2	**6**	0	0	**0**	1	1	**1**
H5: Zavedení destruktivních a škodlivých programů	3	3	**9**	3	3	**9**	3	3	**9**
H6: Zneužití systémových prostředků	3	3	**9**	3	1	**3**	2	1	**2**
H7: Infiltrace komunikace	3	3	**9**	1	2	**2**	2	2	**4**
H8: Zachycení komunikace	3	3	**9**	1	1	**1**	1	1	**1**
H9: Manipulace komunikace	1	1	**1**	1	2	**2**	2	3	**6**
H10: Odmítnutí odpovědnosti	1	1	**1**	1	1	**1**	1	1	**1**
H11: Selhání komunikace	1	1	**1**	2	2	**4**	3	2	**6**
H12: Začlenění škodlivých programů	3	3	**9**	3	3	**9**	3	3	**9**
H13: Chybné směrování	3	2	**6**	0	0	**0**	0	0	**0**
H14: Technická závada počítače	0	0	**0**	3	3	**9**	2	2	**4**
H15: Technická závada paměťového zařízení	0	0	**0**	2	2	**4**	2	2	**4**
H16: Technická závada tiskového zařízení	0	0	**0**	1	2	**2**	0	0	**0**
H17: Technická závada síťového distribučního prvku	0	0	**0**	2	2	**4**	1	1	**1**
H18: Technická závada síťové brány	0	0	**0**	2	2	**4**	1	1	**1**
H19: Technická závada počítače pro řízení / správu sítě	0	0	**0**	2	2	**4**	0	0	**0**

Hrozba	**Důvěrnost**			**Dostupnost**			**Integrita**		
	P	**D**	**R**	**P**	**D**	**R**	**P**	**D**	**R**
H20: Technická závada síťového rozhraní	0	0	**0**	3	2	**6**	1	1	**1**
H21: Technická závada síťové služby	0	0	**0**	2	2	**4**	1	1	**1**
H22: Selhání napájení	0	0	**0**	2	3	**6**	2	2	**4**
H23: Selhání klimatizace	0	0	**0**	2	2	**4**	1	1	**1**
H24: Selhání systémového nebo síťového programového vybavení	1	1	**1**	3	3	**9**	3	3	**9**
H25: Selhání aplikačního programového vybavení	1	1	**1**	2	2	**4**	2	2	**4**
H26: Provozní chyba	2	2	**4**	3	3	**9**	3	3	**9**
H27: Chyba údržby technického vybavení	3	3	**9**	2	3	**6**	1	1	**1**
H28: Chyba úpravy programového vybavení	2	3	**6**	2	3	**6**	2	3	**6**
H29: Chyba uživatele	2	3	**6**	3	3	**9**	3	3	**9**
H30: Požár	0	0	**0**	2	2	**4**	0	0	**0**
H31: Poškození vodou	0	0	**0**	2	3	**6**	0	0	**0**
H32: Přírodní katastrofa	0	0	**0**	1	2	**2**	0	0	**0**
H33: Nedostatek personálu	0	0	**0**	0	0	**0**	0	0	**0**
H34: Krádež provedená identifikovatelnými osobami	3	3	**9**	3	3	**9**	0	0	**0**
H35: Krádež provedená cizími osobami	3	3	**9**	3	3	**9**	0	0	**0**
H36: Úmyslné poškození identifikovatelnými osobami	0	0	**0**	2	3	**6**	0	0	**0**
H37: Úmyslné poškození cizími osobami	0	0	**0**	2	3	**6**	0	0	**0**
H38: Terorismus	0	0	**0**	0	0	**0**	0	0	**0**
Suma rizik			**126**			**166**			**100**