Zabezpečení přístupu do Internetu z uzavřeného firemního intranetu

Bc. Jan Polášek

Diplomová práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan Polášek**
Osobní číslo:	**A15317**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Zabezpečení přístupu do Internetu z uzavřeného firemního intranetu**
Téma anglicky:	**Securing Access to the Internet from a Closed Corporate Intranet**

Zásady pro vypracování:

1. **Specifikujte důvody oddělení Internetové a Intranetové sítě.**
2. **Popište možnosti oddělení těchto segmentů pomocí HW a SW prvků.**
3. **Navrhněte řešení pro vzdálený zabezpečený přístup do Intranetu.**
4. **Navrhněte implementaci komplexního řešení pro oddělení Intranetu a Internetu.**
5. **Specifikujte IDS/IPS systém pro Vaše řešení.**
6. **Proveďte ověření řešení v testovacím provozu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **RUEST, Danielle a Nelson RUEST. Virtualizace: podrobný průvodce. Brno: Computer Press, 2010. ISBN 978-80-251-2676-9.**
2. **ŠIKA, Michal. 333 tipů a triků pro VMware. Brno: Computer Press, 2012. ISBN 978-80-251-3659-1.**
3. **LOWE, Scott. Mistrovství ve VMware vSphere 5: kompletní průvodce profesionální virtualizací. Brno: Computer Press, 2013. Mistrovství. ISBN 978-80-251-3774-1.**
4. **MATOUŠEK, Petr. Síťové aplikace a jejich architektura. Brno: VUTIUM, 2014. ISBN 978-80-214-3766-1.**
5. **KOSTOPOULOS, George K. Cyberspace and cybersecurity. Boca Raton, Fl.: CRC Press, c2013. ISBN 1466501332.**
6. **KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.**
7. **SOSINSKY, Barrie. Mistrovství počítačové sítě. 1. Praha: Computer Press, 2016. ISBN 9788025139165.**
8. **HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. února 2017**

Termín odevzdání diplomové práce: **24. května 2017**

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 11.5.2017

.....
podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá zjednodušením přístupu zaměstnanců Policie České republiky k Internetu v oddělené firemní síti intranetu. Práce je rozdělena na dvě části. V první části se zabýváme teoretickými možnostmi oddělení sítí Internetu a intranetu. V této části se také seznámíme se základy virtualizace. V praktické části diplomové práce vybereme nejvhodnější způsob zpřístupnění Internetu. Tento způsob poté implementujeme do stávající sítě intranet. V praktické části se budeme také věnovat zabezpečení celé architektury včetně systému prevence narušení. Na konci diplomové práce je provedena praktická zkouška systému.

Klíčová slova: virtualizace, virtualizace desktopu, firewall, IPS/IDS, SWOT analýza

ABSTRACT

This disseration thesis deals with simplifying of approach towards internet in field of company's intranet for employees of the Czech Republic police department. The thesis is divided into two parts. In first part, the focus is on theoretical possibilities in internet and Intranet fields. In this section, basics of virtualisation will be introduced. In practical part of this thesis will be chosed the most suitable approach for access to the Internet. This access will be implemented into current system of intranet. In practical part, focus will be on security of architecture including prevention of intrusion. At the end of the thesis, practical test of the system is being made.

Keywords: virtualization, desktop virtualization, firewall, IPS / IDS, SWOT analysis

Děkuji především vedoucímu práce Ing. Davidovi Malaníkovi, Ph.D. za věcné připomínky, rady a trpělivost při vedení mé diplomové práce. Také chci poděkovat rodině, která mě po celou dobu studiu podporovala.

OBSAH

ÚVOD

Výběr téma diplomové práce s názvem Zabezpečení přístupu do Internetu z uzavřeného firemního intranetu jsem si vybral z důvodu služebního zařazení na Odboru informačních a komunikačních technologií na Krajském ředitelství policie Jihomoravského kraje. Zde pracuji jako IT pracovník a má pracovní náplň je vzdálená správa a dohled nad hardwarem a administrace IT. Dalším důvodem proč jsem si vybral toto téma, jsou vysoké nároky na zabezpečení intranetu Ministerstva Vnitra České republiky. Policie má k dispozici velké množství informačních systémů, které jsou propojeny v intranetu. Tyto informační systémy obsahují citlivé nebo osobní data, které se musí chránit, což klade velké nároky na zajištění bezpečnosti. Přesto se policejní práce neobejde bez Internetu, kde jsou informace, které jinde nejdou nalézt. Páchání kybernetických trestných činů v síti Internet je další důvod, aby pracovníci Policie ČR měli zajištěný kvalitní přístup do Internetu. Původní stav zpřístupnění Internetu byl založen na zcela oddělené infrastruktuře, která byla nesystémová a chaotická. Tento systém zvyšoval nároky na administraci hardwaru a softwaru, což také vedlo ke zvyšování finančních nákladů. Další negativní vlastnost tohoto systému je nedostatečná kontrola a ochrana datového toku.

Diplomovou práci rozdělíme na dvě základní části, a to na teoretickou a praktickou část. V teoretické části se budeme věnovat základními vlastnostmi síti Internet a intranet a důvodem jejich rozdělení. Dále se tato kapitola bude zabývat možnostmi oddělení těchto sítí. Prostor je zde také věnován teoretickým hrozbám v kybernetickém prostoru.

V praktické části popíšeme důvod výběru virtualizace desktopu, jako nejvhodnějšího způsobu oddělení sítí Internet a intranet. Z důvodu lepšího a přehlednějšího představení faktorů výběru této metody bude v praktické části diplomové práce provedena SWOT analýza. Po provedení této analýzy vybereme konkrétní řešení virtuální desktopové infrastruktury. Tato technologie zaručuje vysokou míru zabezpečení především oddělením sítí, ale přitom zachovává dostatečný komfort pracovníků Policie České republiky. Poté infrastrukturu systému implementujeme do sítě intranet a jednotlivé části systému nainstalujeme. V závěru kapitoly provedeme několik testů technologie.

I. TEORETICKÁ ČÁST

1 INTERNET, INTRANET, EXTRANET

1.1 Internet

Internet jsou spojené počítačové sítě, které navzájem propojují dílčí síťové uzly. Uzel tvoří počítač nebo specializované zařízení, například router. Síťové prvky připojené k internetu využívají protokoly TCP/IP. Protokoly TCP/IP definují dva základní typy přenosů, a to spolehlivé spojované služby TCP a nespolehlivé služby UDP. V internetu se používají různé typy adresování, které se liší podle vrstev. Pro rozpoznání síťového prvku se používají MAC adresy. Pro adresování uzlů slouží v Internetu IP adresy a na aplikační vrstvě (v originálním názvu application layer) se používají doménové adresy. Hlavní funkcí internetu je předání informací. Jednou z nejčastějších používanou technologií je World Wide Web (WWW), která pomocí protokolu HTTP popřípadě HTTPS slouží k přenosu, prohlížení, ukládání a odkazovaní dokumentů na internetu. [1]

1.2 Extranet

Extranet je druh webové aplikace sloužící ke sdílení citlivých dat s uživateli zvnějšku, nejčastěji se zákazníky, obchodními zástupci nebo spolupracujícími firmami. Velké společnosti také mívají několik webových aplikací. Ty se rozdělují například pro styk s veřejností, s jinými institucemi, s tiskem či medií. Extranet je chráněn autorizací oproti běžným webovým aplikacím. Autorizace může být řešena v několika úrovních, a tudíž se každému uživateli zobrazí jiné informace. Může se jednat například o informaci o plnění zakázky apod. Stejně jako intranet, tak i extranet může sloužit k mnoha účelům pro pracovníky firmy. Jedná se především o rychlé předání a dostupnost informací a dat, ke komunikaci nebo k plnění společných úkolů mezi pobočky firmy. [2]

1.3 Intranet

Intranet je část počítačové sítě, která se označuje jako privátní nebo soukromá, je oddělena od Internetu a používá stejné informační technologie jako například protokoly TCP/IP, http apod. Využívají jej uživatelé uvnitř firmy. Může se jednat o rozsáhlou informační a výpočetní počítačovou infrastrukturu nebo jen interní webové stránky. Slouží pro komunikaci a práci uvnitř firmy, pro přenos dat (FTP), emailů (SMTP) nebo webové služby (http/https). Intranet je v mnoha organizací chráněn pomocí firewallu, brány nebo je zcela oddělen.

Intranet využívá, podle standardů daných RFC 1918, vyčleněný rozsah IP adres pro soukromé účely:

- 10.0.0.0 – 10.255.255.255;

- 172.16.0.0 – 172.31.255.255;

- 192.168.0.0 – 192.168.255.255. [3]

1.3.1 Důvody oddělení intranetu od Internetu

Nejdůležitějším cílem intranetu bývá usnadnit sdílení informací mezi zaměstnanci firmy a zajištění bezpečnosti dat proti zneužití. Pravidelnými součástmi intranetu jsou různé analytické funkce, přehledy stavu projektů, nástroje pro správu dokumentů, využití lidských zdrojů, plánovače, adresáře, databáze zákonů, interních aktů a nařízení, rezervační systémy a jiné systémy pro zajištění každodenního chodu práce ve společnosti. [3]

Nejčastější výhody zavedení intranetu:

- Bezpečnost – bez přístupu z internetu jdou data v intranetu nedostupná pro možné napadení se sítě;
- Nenáročné sdílení informací – možnost šíření informací ve společnosti, zajištění spolupráce zaměstnanců a poboček, tvorba databáze informací;
- Vyšší produktivita – dostupnější a rychlejší dostupnost dat s využitím analytických dotazů vede ke zvýšení produktivity;
- Efektivnější komunikace a řízení – jednotné kalendáře, plánovače, nástěnky, adresáře vedou k efektivní komunikaci ve společnosti;
- Lepší využití lidských zdrojů a organizace práce – zavedením personálních a ekonomický nástrojů se zvyšuje kvalita využití lidských zdrojů;
- Odpovědnost vůči životnímu prostředí – intranet snižuje množství vytištěných dokumentů, což vede ke snížení dopadu na životní prostředí a také ke snížení nákladů společnosti. [3]

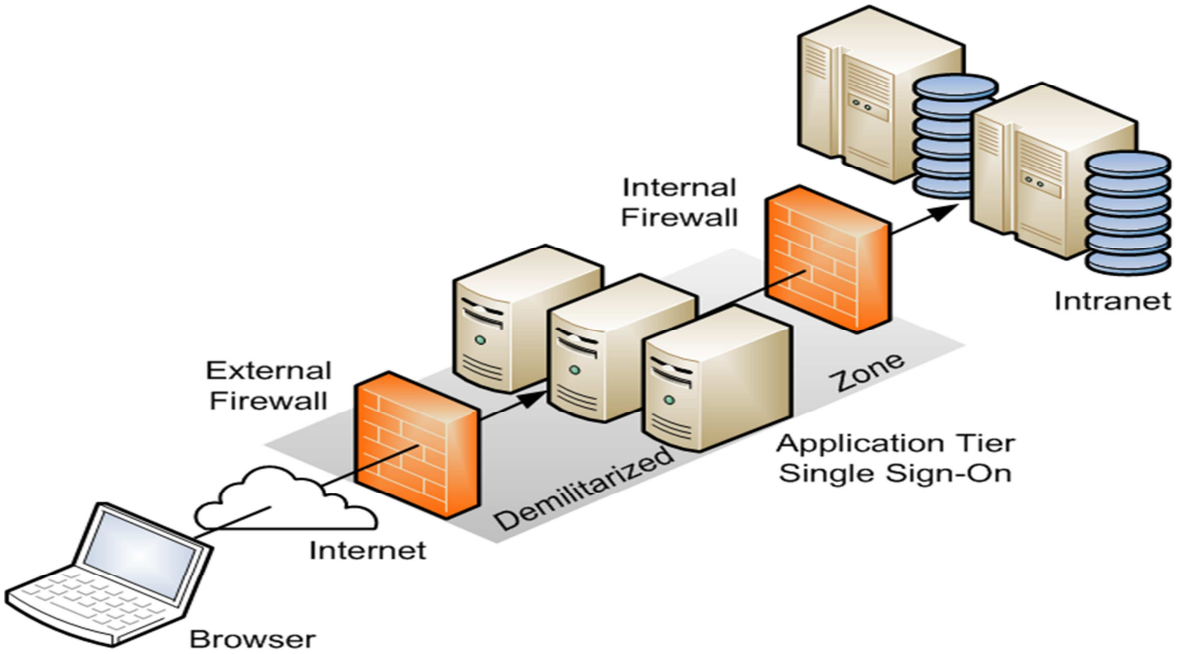
Tab. 1, Vlastnosti sítí [4]

	Internet	Intranet	Extranet
Typ přístupu	Otevřený	privátní	kontrolovaný
Uživatel	Veřejnost	vnitropodnikový	vybraní
Informace	všeobecné	lokální	konkrétní

1.3.2 Zajištění bezpečnosti intranetu

Při zajištění bezpečnosti provozu intranetu je kladen velký důraz na centralizaci všech klíčových komponent. Z technického hlediska lze řešení rozdělit do tří základních skupin:

- Uživatelské pracoviště, kde požadujeme především konektivitu se serverem a správnou verzi prohlížeče;
- Interní demilitarizovanou zónu, tj. bezpečnou vrstvu v síti LAN, která obsahuje služby intranetu, servery apod.;
- Zóna s vysokým zabezpečením - obsahuje aplikační logiku, interní a externí datové zdroje a podpůrné systémy. [5]



Obr. 1, Demilitarizovaná zóna [6]

Toto rozdělení do výše uvedených tří základních skupin je z pohledu bezpečnosti velmi prospěšné. Především odděluje citlivé informace od ostatních. Při dobrém zpracování tento koncept pak nutí administrátory dokumentovat jednotlivé informační toky. Výhodou tohoto konceptu je také zjednodušení ostatních backend procesů, především zálohy a archivace, protože data jsou centralizována a umístěna na jednom místě. [5]

1.3.3 Bezpečnostní technologie aplikované v intranetech

Existuje několik možností pro zajištění bezpečnosti intranetu. Jedna z nejznámějších bezpečnostních technologií je využití certifikátu pro server – pro jméno domény, kde je server provozován. Tento prvek se používá pro šifrování přenášených dat a pro ověření identity serveru. To zaručuje, že uživatel se dívá na konkrétní server a ne na napodobeninu od hackera. [5]

Ve spojení s intranetem se dále využívá technologie podepisování kódu. Některá intranetová řešení mohou využívat software, který je potřeba spouštět na straně uživatele. Toto je však potenciálně nebezpečné, protože lze vytvořit takový software, který kromě dané služby může obsahovat například vir. Tomu lze částečně zabránit použitím certifikační autority, čímž se zamezí modifikaci software na serveru. [5]

Výše uvedené techniky řešily problematiku autentizace intranetového serveru vůči uživateli, tak aby uživatel důvěřoval serveru, ale ne opačně. Abychom byli schopni zajistit důvěru počítače vůči serveru, musíme provést autentizaci počítačů. Toho dosáhneme tím, že vystavíme certifikáty všem oprávněným uživatelům intranetu. Abychom toho byli schopni, je třeba vystavit certifikáty všem oprávněným uživatelům intranetu. Poté, v případě, že uživatel má vystavený tento certifikát a žádá data z chráněné části intranetu, server vyžádá uživatele k zaslání podepsaného digitálního podpisu. Server ověří platnost certifikátu a platnost podpisu. Intranetový server pak podle práv uživatele rozhodne o tom, zda je klientovi zaslána požadovaná informace. Celý proces se provádí automaticky, což je uživatelsky přívětivé. [5]

Digitální podpis je také jedna z možností k zajištění autenticity uživatelských dat v intranetových aplikacích. Při odeslání dat je spuštěn software, který obsah formuláře shrnuje a opatří elektronickým podpisem vytvořeným pomocí klíče na kartě, kterým uživatel provádí autentizaci. Pokud je tato technologie využívána, je komunikace mezi serverem a uživate-

lem šifrována. Následně je na serveru provedena kontrola podpisu. Jestliže je podpis v pořádku, je prováděna služba podle požadavku uživatele. [5]

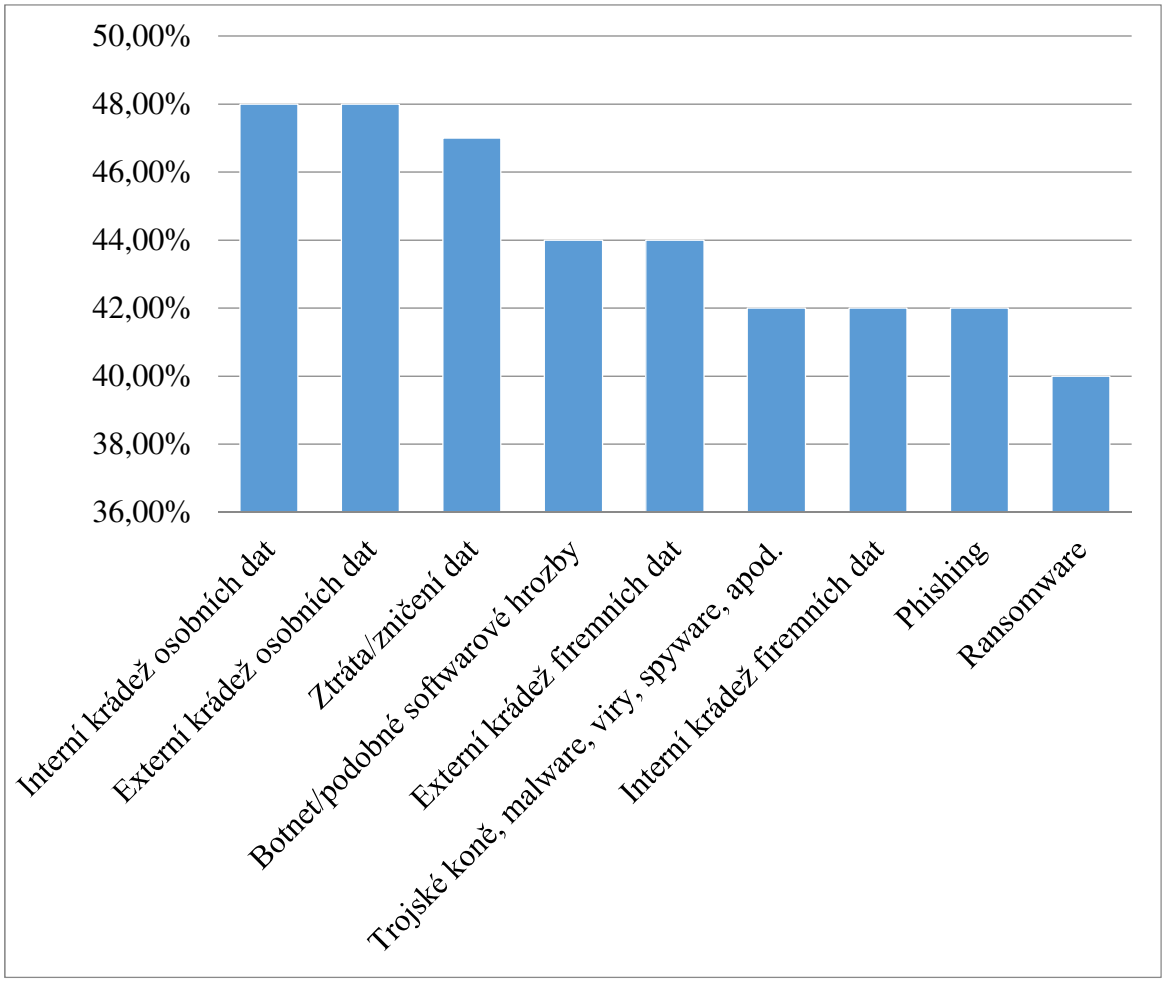
1.3.4 Intranet Policie ČR

Policie České republiky (PČR) je ozbrojený bezpečnostní sbor České republiky. Vznikl dne 15. července 1991 přeměnou české části československé Veřejné bezpečnosti Sboru národní bezpečnosti, a to dnem vyhlášení zákona ČNR č. 283/1991 Sb., o Policii České republiky. S účinností od 1. ledna 2009 je činnost Policie České republiky upravena novým zákonem č. 273/2008 Sb., o Policii České republiky. [7]

Z důvodu potřeby zajištění výkonu služby policejních složek bylo pro komunikaci v rámci Ministerstva vnitra, a tedy i Policie ČR, zřízena intranetová síť „HERMES“. Intranet umožňuje přenos dat, elektronické pošty, a také je zde k dispozici velké množství informačních systémů. Policejní informační systémy se člení na evidenční systémy, manažerské systémy, poznatkové fondy, specializované, laboratorní a expertní analytické systémy. [8]

1.4 Hrozby Internetu pro firmy

V roce 2016 provedla společnost Accenture HfS průzkum s názvem „Stav kybernetické bezpečnosti a digitální důvěry v roce 2016“. Tohoto průzkumu se zúčastnili 206 top manažerů napříč všemi obory. Předmětem průzkumu bylo zjištění současného a budoucího stavu kybernetické bezpečnosti v rámci podniku a navržení opatření pro zajištění lepší kybernetické bezpečnosti. Výsledky studie ukazují, viz graf č. 1, že respondenti mají obavy z interní krádeže firemních dat a infikace malwarem, přičemž s tímto tvrzení se ztotožnilo 42 % dotázaných. Respondenti ve 42 % případech uvádí, že na úroveň financování a zaměstnanosti a pro najímání a školení odborníků na zabezpečení potřebují větší rozpočet. Dále 54% dotázaných uvedlo, že jejich zaměstnanci nejsou na prevenci prolomení zabezpečení dostatečně proškoleni. [9]



Graf 1, Studie Stav kybernetického zabezpečení 2016, HfS Research a Accenture; Vzorek: 208 firemních odborníků na zabezpečení. [9]

Kybernetické hrozby lze rozdělit do základních čtyř skupin. První skupina tvoří úniky informací, což lze definovat jako vyzrazení chráněné informace neautorizovanému subjektu. Další kategorie je narušení integrity, které představuje poškození, změnu či vymazání dat. Třetí díl je potlačení služby, která znamená úmyslné bránění v přístupu k informacím, aplikacím či systému. Poslední skupinou je nelegitimní použití. Jedná se o užití informací neautorizovaným subjektem či neoprávněným způsobem. [10]

1.4.1 Červy přenesené elektronickou poštou

Nebezpečí pro intranet a samotnou firmu spočívá v infiltraci koncového zařízení pomocí červa v elektronické poště. Jedná se především o infikaci typu červ, který se do počítače dostane elektronickou poštou. Zpravidla se v počítači objevuje jako jeden soubor, který neobsahuje nic jiného než červa. Infikovaný e-mail obsahuje mimo textu také přílohu se souborem. Text nabádá k otevření souboru, a tím se červ aktivuje. Poté se tento červ uloží

do konkrétního souboru. Ve vhodné chvíli tento červ odešle infikovaný email na další emailové adresy, a to především uložené v adresáři uživatele. [11]

Další možností, jak přenést červa do počítače, je využití HTML formátu. Podmínkou je, aby poštovní klient umožňoval technologii HTML, poté není potřeba žádné přílohy. S příchodem HTML formátu se vizuálně zlepšily zprávy, ale také se otevřely dveře červům. Červ se do počítače dostane jen otevřením zprávy. [11]

Červ kromě svého vlastního šíření má také sekundární činnost, která je červem nesená jako náklad. Tomuto kódu se říká payload. Sekundární činnosti červa může být například zamezení činnosti počítače, odstranění nějakého souboru, zašifrování souborů či vytvoření zadních vrátek. [11]

1.4.2 Červi v operačních systémech

Červi se také nacházejí v souborech samostatně a nepotřebují žádné hostitele. Většina červů si zajistí samočinné spuštění, a to nejčastěji pomocí modifikace registrů, modifikace souboru WIN.INI nebo SYSTEM.INI v adresáři s instalací Windows. [12]

1.4.3 Spam

Nevyžádaná zpráva doručená elektronickou poštou se nazývá spam, převážně s obchodním reklamním obsahem. Spamming je vlastní aktivita rozesílání spamových zpráv. Spamming iniciuje jedna strana, a to odesílatel, který se snaží ovlivnit jiné osoby, příjemce, což je základní problém spamu. Další riziko spamu spočívá v eskalaci do takové míry, že uživatelé nebudou chtít používat běžnou poštu, nebo v záplavě nevyžádané pošty se firemní pošta ztratí.

Ochrana proti spammingu pomocí technických opatření, přísluší především filtrování a následné eliminace spamu. Tyto opatření neodstraňují příčiny, ale snižují dopad. [13]

1.4.4 Hacking

Hacking znamená vniknutí do počítačového systému jinou než běžnou cestou. Jedná se především o obejití bezpečnostních opatření a prolomení ochrany počítačového systému. Motivace hackera, který provádí hacking, je především zjištění informací o počítačovém systému nebo uživateli. Jeho motivace můžou být prestiž, uznání od ostatních hackerů, finanční stimul nebo se může jednat o průmyslovou či jinou špionáž. [14]

1.4.5 Typy hackerských útoků

V současné době se vyskytuje velký počet síťových útoků. Útoky zneužívají slabých míst operačních systémů, firmwarů či jiných softwarů nainstalovaných v počítači. K zajištění bezpečnosti intranetu je potřeba druhy síťových útoků znát. Lze jej rozdělit do několika skupin. [14]

Prohledávání portů je typ hrozby, která obvykle předchází útoku na počítač, a proto není sám o osobě útokem. Prohledávání portu je jedním ze základních činností pro sběr informací o počítači. Jsou analyzovány porty UDP a TCP používané síťovými nástroji na počítači, na který se útočník zaměřil a je zjištěno, v jakém stavu se nacházejí, například zda jsou otevřené nebo zavřené. [14]

Útok typu DoS nebo také útoky odmítnutí služby jsou útoky, které způsobují destabilizaci nebo nečinnost systému. Tento typ útoku může způsobit nedostupnost systému nebo blokování přístupu do Internetu. [14]

Útok typu „narušení“ se zakládá ve snaze ovládnout napadený počítač. Je to jeden z nejnebezpečnějších typů útoků. V situaci, kdy se útok povede, získá útočník úplný přístup k předmětnému počítači. Útočníci tento typ útoku využívají v případě získání důvěrných informací. Může se jednat o osobní údaje nebo o čísla kreditních karet. Útočník také může proniknout do systému a použít jeho výpočetní prostředky ke škodlivým účelům. Tato skupina obsahuje největší počet zaznamenaných útoků. Rozdělit se dají podle různých kritérií. Například útoky na systém Microsoft Windows, útoky na systémy typu Unix a útoky na síťové služby používané v různých systémech. [14]

1.4.6 Falšování webové stránky

Falšování webu je jedním z útoku hackera, který vytvoří přesvědčivou, avšak falešnou kopii celého webu. Tento falešný web musí vypadat co nejvíce jako originální. Celý web však řídí útočník, a to včetně komunikace, čímž může útočník získat data, která může modifikovat nebo dále zneužít. Komunikaci může útočník ovlivňovat oboustranně, od uživatele k serveru nebo opačně. Agresor může sledování provést dokonce i v případě, že se oběť zdánlivě připojila k bezpečnému spojení. Údajně bezpečné spojení pomocí SSL nebo S-http může útočník zfalšovat. Falšování webové stránky je součástí techniky zvané phishing, nebo taky rhybaření, což je snaha oběť nalákat, chytnout a následně získat citlivá data. [15]

1.4.7 Viry

Virus je typ záludného programu, složeného z kódu binární soustavy, který se sám množí a tím infikuje další programy kolem sebe. Červ, oproti viru, žije svůj život a může se sám šířit mimo nakažené prostředí. Vir infikuje dané prostředí a vykonává akce nezávisle a bez vědomí uživatele. Vir není schopen samostatné existence a musí mít nositele. V současné době existuje několik základních druhů virů. Základní typy virů jsou:

- Souborový vir, který napadá převážně spustitelné soubory;
- Boot viry, které napadají boot sektory na disku;
- Rezidentní viry sídlí v operační paměti a kontrolují diskové operace;
- Makroviry napadající dokumenty MS Office;
- Stealth viry se maskují před antivirovým programem;
- Polymorfní viry mění svůj kód v závislosti na potřebě;
- Červi, které jsou popsány výše. [16]

Projevů nakažení systému počítačovým virem je velké množství. Jeden z projevů je například blokování místa, tj. zabírání místa na uložišti. Další příznak je zpomalení systému, protože vir pro svou činnost alokuje část HW prostředků. Nestabilita, vypsání textu nebo zvukové projevy jsou další možné symptomy nakaženého systému počítačovým virem. Jiná možnost projevu počítačového viru je krádež, poškození nebo pozměnění dat. [17]

2 ZÁKLADNÍ PŘIPOJENÍ DO INTERNETU Z INTRANETU

Základní připojení Intranetu do Internetu z hlediska bezpečnosti jsou:

- Žádné připojení, které se používá a obecně doporučuje v případě bezpečnostních složek nebo státní správy, a to z důvodu ochrany strategických, kritických a osobních dat. Uživatel musí mít k dispozici jiný PC, který je připojený do Internetu, ale není propojen s Intranetem;
- Plné připojení, což je opak předchozí možnosti. Jedná se o připojení bez jakéhokoliv bezpečnostního omezení;
- Propojení intranetu s Internetem tím způsobem, že je použit prvek bezpečnosti, který snižuje riziko. Pro oddělení používáme proxy, wrapper nebo firewall. Předpokladem je vybudovaný intranet, který nesmí být přímo připojený s Intranetem;
- Úplné připojení do Internetu, s použitím technologií, které snižují bezpečnostní rizika Internetu, například SSH, HTTPS, FTPS apod. [18]

2.1 Oddělení intranetu od Internetu

Intranet můžeme izolovat především pomocí:

- Skrytých sítí;
- Filtrace;
- Proxy a gateway;
- Wrapperu;
- Firewallu;
- Využití síťového tunelování;
- Virtualizace. [18]

2.1.1 Privátní (skryté sítě)

Jak již bylo uvedeno výše, není nutné, aby intranet využíval IP adresy známé v Internetu, má tedy vyhrazené intervaly IP adres. Podmínkou je, aby mezi intranetem a Internetem byl síťový prvek proxy nebo gateway. Počítače ležící v intranetu jsou tedy chráněny před navázání spojení z Internetu. V případě, že mezi intranetem a Internetem není proxy nebo

gateway, je možné použít Network Address Translator. Ten může být řešen softwarově nebo je součástí routerů. [18]

2.1.2 Filtrace

Na přístupovém routeru, kterým je oddělená síť připojená k internetu, je nastaven filtr. Filtrace je vlastností routeru. Může se jednat o klasický router nebo PC se dvěma síťovými kartami. Filtrovat lze pomocí MAC adres, IP adres, domény apod. Filtrací lze dále dosáhnout toho, že uživatelé Intranetu mají přístup do internetu, ale uživatelé Internetu nikoli. V tomto případě je potřeba provádět filtraci nejenom IP, ale současně i filtraci protokolu TCP.

Filtr se rozhoduje na základě údaje uložených v záhlaví datagramu a záhlaví paketu. Pro protokoly HTTP/S, TELNET, POP apod., není problém docílit toho, aby uživatelé intranetu měli přístup do Intranetu a naopak nikoli. Problém nastává v provozu FTP a SMTP a všech aplikačních protokolů, které využívají UDP. Filtr, který filtruje podle údajů v datagramu, se nazývá Packet Filter a filtr, který filtruje pomocí údaje v záhlaví TCP resp. UDP, se nazývá Circuit Filter. [18]

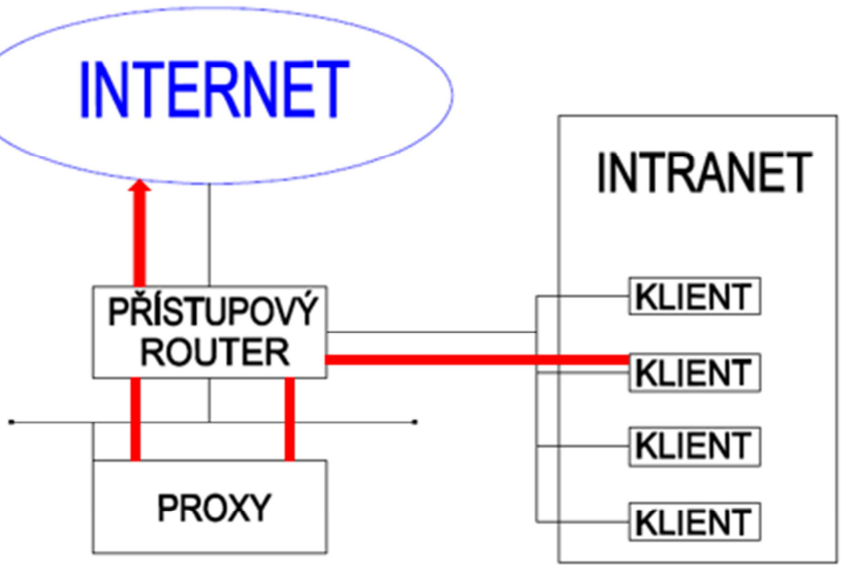
Výhody a nevýhody filtrace pro zajištění bezpečnosti firemní privátní sítě

Pravděpodobně nejdůležitější a zásadní výhodou paketových filtrů je jejich účinnost v případě provozu na síťové a transportní vrstvě protokolu ISO/OSI. V případě, že intranet je k Internetu připojen pouze jedním směrovačem a je zde dobře nastavená filtrace, dokáže ochránit celou privátní síť a nezáleží na její velikosti. Jak je uvedeno výše, paketové filtry ve většině případů pracují na síťové a transportní vrstvě protokolu ISO/OSI či TCP/IP, což pro zajištění bezpečnosti firemního intranetu nemusí stačit. Firemní bezpečnostní politika může stanovovat zákaz různých aplikací, které pracují na aplikační vrstvě protokolu ISO/OSI. Tudíž paketový filtr je neúčinný a musí se využít jiné zajištění bezpečnosti provozu sítě. Další nevýhodou, v případě že je paketový filtr součástí nějakého směrovače, je další zátěž zařízení. Zde záleží na konkrétním zařízení, infrastruktuře intranetu, celkovém datovém toku a složitosti filtrace. [18]

2.1.3 Proxy server a gateway

Proxy server slouží jako prostředník mezi klientem a cílovým počítačem nebo serverem. Jeho základní úkol je překládání klientských požadavků. Vůči cílovému počítači vystupuje

jako klient. Proxy lze instalovat několika způsoby. Klasické zapojení je proxy se dvěma síťovými rozhraními, a to jedno do intranetu a jedno do Internetu. Proxy zprostředkovává spojení mezi oběma sítěmi automatizovaně. Z hlediska klienta se proxy chová jako server. Proxy pracuje na aplikační vrstvě modelu ISO/OSI, což znamená, že vidí do aplikačního protokolu. Filtrace je možné provádět při předávání mezi serverovou a klientskou částí. [18]



Obr. 2, Schéma oddělení sítí pomocí proxy

V současné době rozlišujeme tyto typy proxy:

- Klasické proxy – klient se zpočátku přihlásí k proxy. Následně klient sdělí jméno cílového serveru a proxy jej propojí s cílovým serverem. Používá se pro protokoly FTP, HTTP/S a TELNET;
- Generické proxy – klient nesděluje jméno cílového serveru, proto je proxy přesměrována na jeden konkrétní server. Využívá se pro protokoly POP, firemní aplikace apod.;
- Transparentní proxy – klient adresuje cílový server. Proxy toto akceptuje a přečte si IP datagram, kde se dozví adresu cílového serveru, poté klient naváže komunikaci. Proxy se z pohledu klienta jeví jako router. Transparentní proxy se používají pro protokoly TELNET a FTP; [18]

- Transparentní generická proxy – Jak je výše uvedeno generické proxy umožňuje klienta přesměrovat jen na jeden server. Za to Transparentní generická proxy umožňuje přepojit na různé servery, což se využívá pro firemní aplikace. [18]

Použití proxy, jako brány do intranetu

Hlavní nevýhodou proxy serveru je složitost. Pro každý webový servis musí proxy server poskytovat specializovaný modul, který poskytuje danou službu. Například pokud nebude obsahovat modul RealAudio, tak nebude možné poslechnout si písničku na Internetu. Také nechrání proti vnitřním ohrožením sítě. Proxy server naopak umožňuje jednoduše logování provozu a kontrolu provozu dat. Naopak filtr paketů je jednodušší, rychlejší ale bez možnosti logování. Výhoda proxy serverů spočívá v skrytí skutečné IP adresy uživatele a řeší nedostatek IP adres. [19]

Gateway

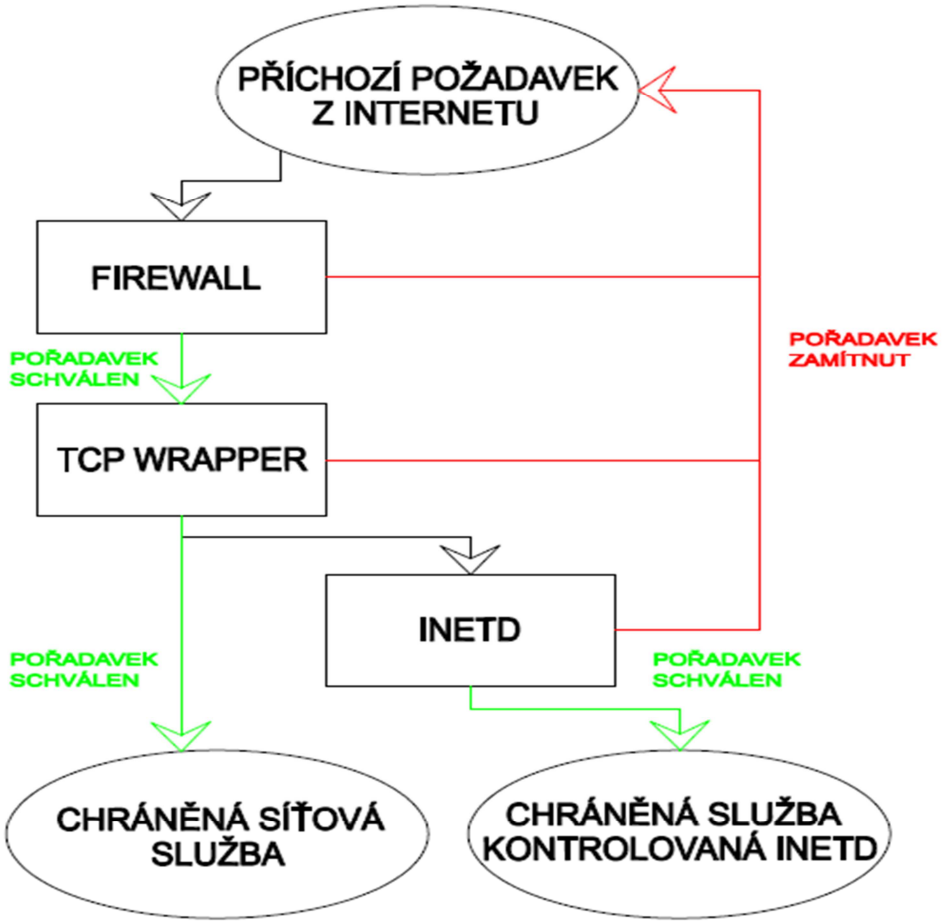
Gataway, v překladu brána, je aktivní zařízení, které má v počítačové síti nejvyšší postavení. Gataway spojuje dvě sítě s odlišnými komunikačními protokoly, to znamená, že převádí jeden aplikační protokol na jiný. Další funkce brány je funkce směrovače – routeru.

Rozlišujeme dva základní typy Gateway:

- Pracující na aplikační úrovni modelu ISO/OSI – brána přijme celou zprávu nebo datagram, poté tuto zprávu převede do tvaru určeného pro danou síť a zprávu odešle;
- Pracující na transportní nebo síťové vrstvě ISO/OSI - v tomto případě brána nedekóduje celou zprávu, ale jen převede datagramy jedné sítě na datagramy druhé sítě. [18]

2.1.4 Wrapper

TCP Wrapper je technologie, která poskytuje kontrolu přístupu ke službě serveru na základě adresy, ze které přichází požadavky klienta. Hlavním úkolem je ochránit Intranet před nepovoleným přístupem. Spouští se automaticky před tím, než je klientovi povoleno přihlášení do serveru. Po provedení autentizace je klientovy server zpřístupněn. Součásti wrapper může být rozesílání stavových zpráv, logy správci sítě nebo určené osobě. [20]



Obr. 3, TCP Wrapper [21]

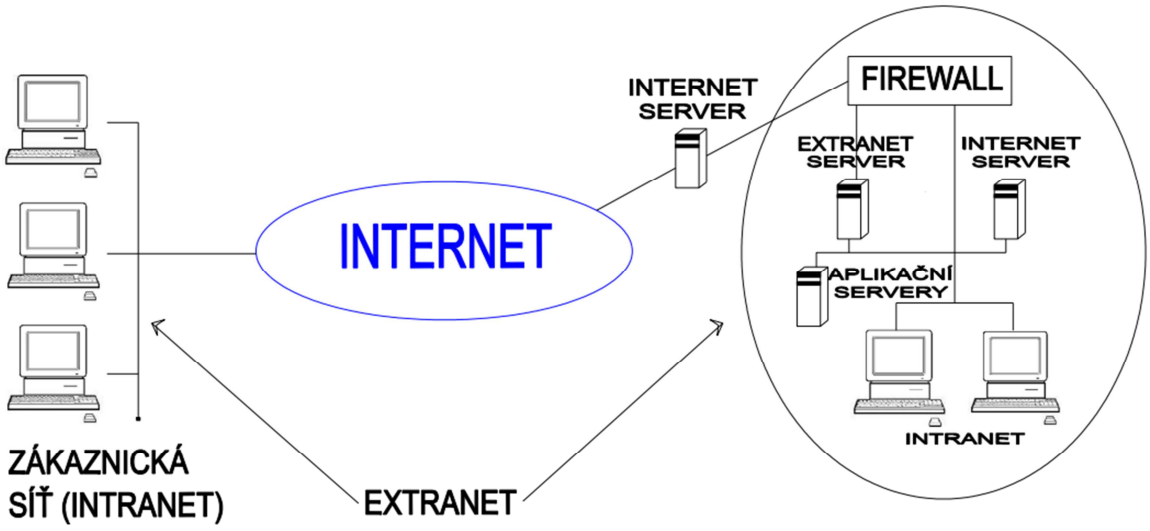
Možnosti wrapperu pro oddělení intranetu a Internetu

Velká výhoda wrapperu je nezávislost jak na klientovi, tak i na serveru. Lze je tedy využít na jakoukoli aplikaci. Další výhoda je, že wrapper je aktivní jen při iniciálním kontaktu mezi klientem a serverem, takže nevznikají žádné nadbytečné data v komunikaci. Wrapper má velkou nevýhodu v tom, že ho nelze použít pro servery, které obhospodařují více než jednoho klienta. Wrapper má totiž efekt jen pro prvního klienta, který první kontaktuje server. Poté už je neúčinný a musí být použitý jiný software. [20]

2.1.5 Firewall

Firewall je bezpečnostní brána, která odděluje provoz mezi intranetem a Internetem. Na základě nadefinovaných pravidel firewall filtruje provoz, a to v obousměrném provozu. Nabízí soubor služeb jako je proxy, filtrace, přístupy do vnitřní sítě apod. Řešen je buď softwarově, hardwarově nebo jejich kombinací. Hlavním úkolem firewallu je především uzavřít atakovanou službu, potencionálního útočníka zařadit do černé listiny, odeslat zprá-

vu správci o nastalé situaci nebo sledovat systém, na kterém firewall běží a v případě změn v systémových souborech poskytnout o tomto informaci. [18]



Obr. 4, Schéma oddělené sítí pomocí Firewallu [18]

Rozlišujeme základní tři skupiny firewallu:

- Paketový firewall – pracuje především na síťové vrstvě a často je implementován do směrovačů. Kontroluje příchozí i odchozí pakety, kde analyzuje údaje v hlavičce, jako je cílová a zdrojová IP adresa, cílový a zdrojový port;
- Aplikační brána – program, který pracuje v aplikační vrstvě. Chová se jako prostředník a kontroluje veškeré pakety pro danou službu. Díky tomu je možné komunikaci monitorovat nebo blokovat;
- Stavový firewall – pracují obdobně jako paketový filtr, ale přidává funkci logování spojení. Poté, když přijde do firewallu paket, firewall je porovná se stavovou tabulkou, a pokud mu byla již jednou povolena komunikace, tak je paket vpuštěn do sítě. [22]

Využití Firewallu jako brány Intranetu

Firewall je základní kámen bezpečnostní politiky firmy. Má velkou řadu výhod, ale i nevýhod. Firewall se často používá v kombinaci s jinou technologií, která oddělují intranet od Internetu. Výhoda firewallu je především v kontrolování přístupu k citlivým datům a aplikacím, a tedy jejich ochrana. Firewall umožňuje centrálně spravovat bezpečnostní systém, včetně logování přístupu a provozu sítě. Firewall může bránit v úniku dat. Nicméně na ochranu interního zaměstnance od externího útočníka je krátký. Vyšší rozsah bezpeč-

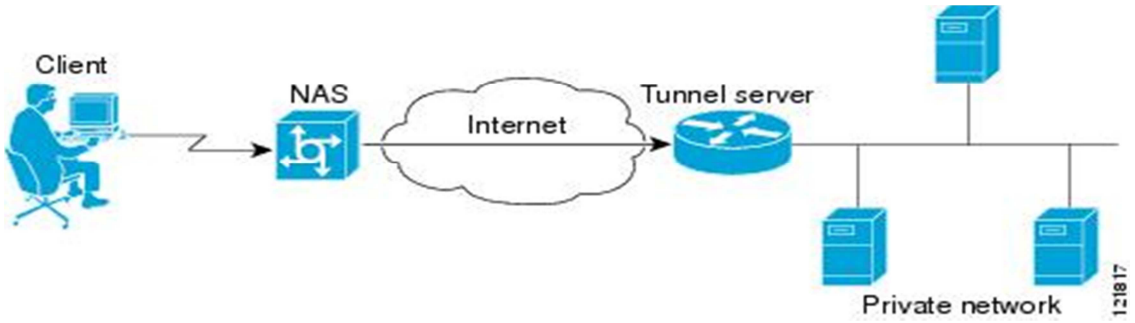
nosti intranetu za použití firewallu vede ke snížení komfortu sítě, a to především ke zpomalení sítě a k problémům s připojením ke službám. Přístup k aplikacím může být příliš komplikovaný nebo omezený. V případě nedokonalé kontroly připojení intranetu k Internetu může dojít k obejití firewallu a následné neúčinností firewallu. V současné době firewall nezaručuje úplnou a zcela účinnou ochranu proti červům, virům, trojským koním apod., které se rychle vyvíjejí a jsou čím dál sofistikovanější. Pouhá kontrola portů a IP adres nechává infrastrukturu zcela nechráněnou. Pro efektivní ochranu dat musí být zajištěna hloubková kontrola aplikací, portů, infrastruktury, zašifrovaných dat apod. [23]

2.1.6 Síťové tunelování

Tunel představuje dvoubodové spojení skrze jinou síť. Tunel se může vytvářet za účelem přenosu jiného síťového protokolu přes rozsáhlou síť nebo k účelu bezpečného spojení dvou lokalit přes Internet.

Je nutno, aby tunelování podporovaly všechny aktivní prvky na cestě, jako jsou přepínače a směrovače. Koncové body tunelu zajišťují autorizaci a řídí přístupy. Pro účely tunelování se používají protokoly:

- Layer2Forwarding (L2F);
- Point-to-Point Tunneling (PPP);
- IPSec. [18]



Obr. 5, Schéma využití síťového tunelování [24]

Protokol nejvyšších vrstev zhotoví zapouzdřený blok dat a ten se přenese sítí logickými tunely za pomocí IP adres. Tunelování se provádí především na spojové a síťové vrstvě referenčního modelu ISO/OSI.

Tunelování na 2. (spojové) vrstvě spustit může sám klient nebo spustí přístupový server NAS. Protokol druhé vrstvy sám tunel vytvoří, udržuje a ukončí.

Tunelování na 3. (síťové) vrstvě je zabalení datagramu do jiného datagramu. Konfigurace tunelů se děje předem. Tuto metodu lze využívat i ve vyčleněných IP adres pro soukromé účely.

Intranet tedy může pomocí síťového tunelování spolu přes Internet komunikovat. Není ani vyloučeno, aby jedna lokalita intranetu byla připojena k Internetu pomocí jiné výše zmiňované technologie [25].

VPN

VPN je zkratka Virtual Private Network v překladu Virtuální privátní síť, a je to bezpečné spojení vytvořené mezi koncovým zařízením jako je osobní počítač, smartphone, tablet, atd. a serverem, který je uvnitř počítačové sítě. VPN jsou vytvořené virtuální bezpečné kopie fyzických sítí, které jsou navzájem spojené kvůli sdílení souborů a dalších zdrojů. Většina moderních VPN je šifrovaná, takže se k nim počítače, zařízení a další sítě připojují skrze šifrované tunely. VPN se tedy často využívá k připojení k intranetu tak, aby byly ochráněny společné soubory, aplikace, data apod. VPN jsou také velmi užitečné pro bezpečné propojení více sítí. Velkou výhodou také je, že v případě připojení například k nedůvěryhodné Wi-Fi síti někde na vlakovém nádraží, VPN zajišťuje bezpečný a šifrovaný provoz, což zajišťuje soukromí, a je to jednoduchá bezpečnostní praktika. Poslední důvod zřízení VPN je anonymita a obejití místních represí a cenzur.

Při složité infrastruktuře intranetu může docházet k zahlcení sítě a jejímu zpomalení, dále VPN bývá nestabilní, a to především při připojení k Internetu, což je také značná nevýhoda.

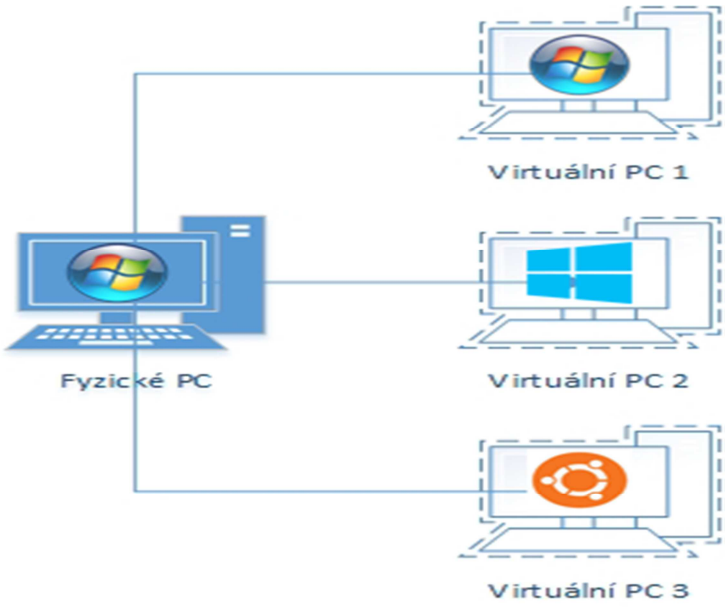
Za zmínku také stojí možnost OpenVPN. Jde o open-source VPN systém, který je založen na SSL kódu. Je to bezplatný, bezpečný systém a netrpí problémy s připojením. Nevýhodou je, že od vás bude požadována instalace klienta, protože Windows, Mac OS X ani mobilní zařízení ji nativně nepodporují. [26]

2.1.7 Virtualizace

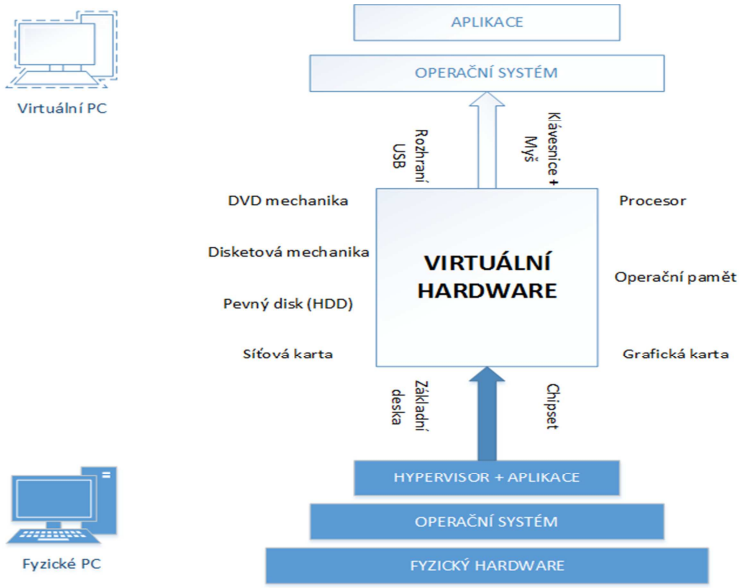
Virtualizace je další možnost, jak zpřístupnit Internet v intranetu. Tento způsob propojení intranetu s internetem je rozveden v další části diplomové práce.

3 VIRT□ALIZAC□

Technologie zvaná virtualizace dělí počítač na několik nezávislých počítačů, na kterých může běžet různé operační systémy a aplikace. Historie virtualizace sahá do období 60. let minulého století, a to ke společnosti IBM. U serverů virtualizace odstraňuje závislost mezi operačním systémem serveru a fyzickým hardwarem, což umožňuje migraci operačních systému a rychlou a jednoduchou aplikaci. V případě plánovaní údržby může virtuální server migrovat na jiný fyzický prostředek, a poté je možné provést hardwarovou údržbu bez potřeby přerušení služby virtuálního serveru. [27]



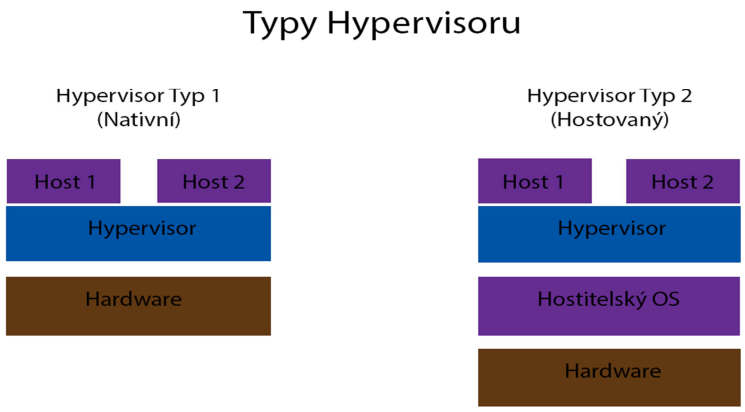
Obr. 6, Základní schéma virtuálního desktopu [28]



Obr. 7, Virtuální hardware [28]

Virtualizace reprezentuje mezivrstvu mezi hostovaným systémem a hostitelským systémem. O správu této vrstvy se stará hypervizor, a to tzv. virtualizační manager. Hardwarové zdroje jako je procesor, operační paměti, grafická karta, síťová karta jsou uděleny hostovanému systému, na kterém běží operační systém. Operační systém je pak vnímá jako hardware vyhrazený a fyzický, pro tento systém plně přístupný. Hypervizory se často spojují do dvou tříd, a to:

- Hypervizory 1 třídy – hypervizor běží přímo na systémovém hardwaru a označujeme jej jako základní hypervizor, někdy také;
- Hypervizory 2 třídy – hypervizor ke své činnosti potřebuje hostující operační systém, který zajišťuje podporu input/output, také se nazývá hostovaný. [29]



Obr. 8, Hypervisory [28]

Virtual Desktop Infrastructure

Virtualizace desktopů usnadňuje centralizaci nasazení desktopů, čímž získáme plnou kontrolu nad virtuální infrastrukturou. Uživatel pouze usedne ke koncovému bodu, ať už se jedná o stolní počítač, webového klienta nebo tenkého klienta a připojí se ke vzdálenému desktopu pomocí klienta. Z důvodu centrální správy můžeme virtuální desktopy uzamknout, a tedy mít desktop pod kontrolou. Stačí vytvořit jednu bitovou kopii systému a tu distribuovat jak jen potřebujeme. Koncové zařízení již není potřeba tolik spravovat a tím je ušetřen čas. Informace a data mohou být chráněny v datovém centru, tím získáme kontrolu nad firemními daty. Přístupy k datům mohou být řešeny centrálně a umožnit přístup jen konkrétním uživatelům. Pomocí virtualizace desktopů lze oddělit Internet od intranetu a to

tak, že koncové zařízení je připojeno do jedné sítě a virtuální desktop je připojen do jiné sítě. Jednotlivé desktopy nemusí mezi sebou komunikovat, tím dosáhneme ochrany citlivých aplikací. V současné době existuje mnoho virtualizačních systémů, které lze rozdělit na dva typy, a to na místní a centralizovaný. [27]

Místní virtualizace

Typ místní virtualizace desktopů je zahájení virtualizace vlastními zdroji koncového počítače. Někdy se také můžeme setkat s pojmenováním virtualizace na straně klienta. Software virtualizace je nainstalován na koncovém počítači. Vytvořená bitová kopie virtuálního desktopu se spustí ve virtualizačním softwaru nad svým fyzickým koncovým desktopem. Tento systém umožňuje centrální distribuci, a je tedy možnost kontroly bitové kopie, což lze označit za spravovaný produkt. Uživatel desktopu si však může vytvořit vlastní bitovou kopii a spouštět si svůj virtualizační desktop, což představuje nespravovanou část metody. [27]

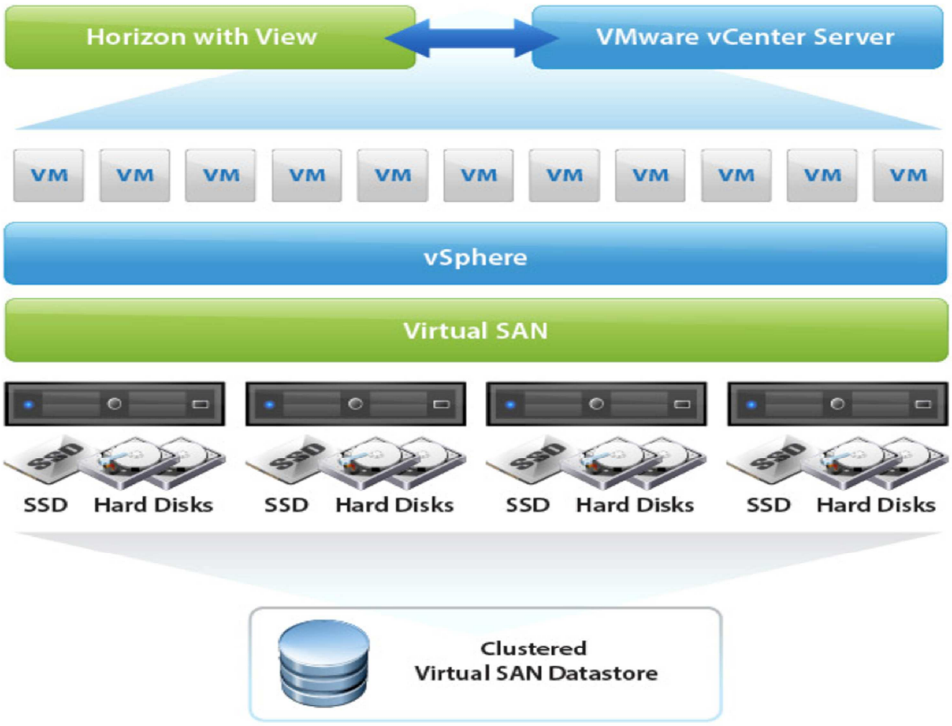
Centralizovaná virtualizace desktopů

Virtuální desktopy běží nad hostitelskými servery, kde je tzv. virtulizační manažer hypervisor pro podporu hardwarové virtualizace. Uživatel využije klienta na svém fyzickém desktopu s podporou připojení ke vzdálené ploše prostřednictvím protokolů PC-over-IP (PCoIP), Remote Desktop Protocol (RDP) nebo Independent Computing Architecture (ICA). Tyto protokoly jsou popsány v další kapitole. [27]

3.1 Software VDI

3.1.1 VMware Horizon 6

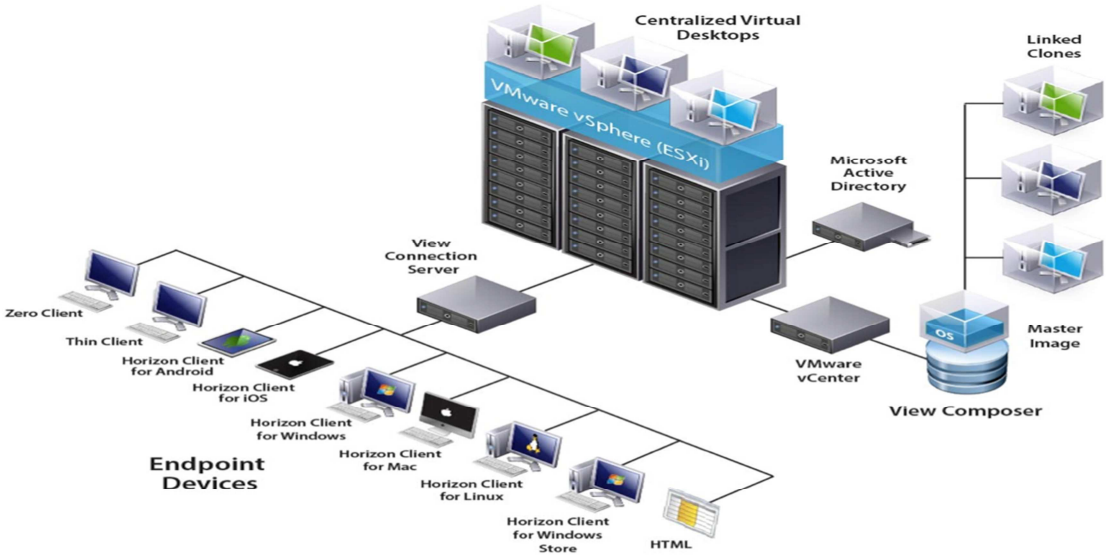
VMware Horizon 6 je platformou pro virtuální desktopy a aplikace od společnosti VMware. Poskytuje koncovým uživatelům přístup ke všem svým virtuálním desktopům, aplikacím a služeb on-line prostřednictvím VDI infrastruktury. VMware Horizon se dříve také nazýval VMware View, přičemž se s tímto názvem můžeme setkat i v současnosti. VMware Horizon 6 využívá serverové infrastruktury vSphere s hypervizorem ESX nebo ESXi a je řízen technologií vCenter. VMware Horizon pracuje s virtuálními disky a využívá je v několika formátech. Jedná se o fyzický disk nebo o logickou jednotku SAN. Dále také o Hyper-Virtual Disk (VHD), a to v možnosti dynamicky se zvyšujícího disku nebo disku pevné velikosti. [30]



Obr. 9, Virtualizace VMware Horizon [31]

Produkt dále nabízí přímou integraci se službou Active Directory (AD) společnosti Microsoft. AD musí mít přizpůsobenou infrastrukturu, a také je povinný pro zprovoznění VDI. Služba využije stávající účty v AD, a také zásady skupin a uživatelů. V případě zajištění vyšší bezpečnosti lze využít produkt RSA SecurID. Scelení AD a VMware Horizon vede k řešení jednotného přihlašování. [27] Pro zajištění správného spojení uživatele a virtuální-

ho desktopu má na starost vConnection Server, který zajišťuje kontrolu přístupu uživatele v AD a připojení ke správnému virtuálnímu desktopu. Navázání spojení mezi serverem virtualizace desktopem zajišťuje Client Horizon. Poté se lze připojit kompatibilním webovým prohlížečem HTML5, například Chrome, IE apod. Technologie Horizon vComposer využívá technologii linkovaných klonů. Tato technologie spočívá ve vytvoření základního obrazu desktopu, ke kterému jsou připojené takzvané prázdné schránky. Uživatel se připojí k prázdné schránce, a jakmile uživatel pracuje se svým virtuálním desktopem, schránka se plní rozdílnými soubory oproti základnímu obrazu. Technologie vComposer je navázána na vCenter. Komunikace mezi virtuálním desktopem a desktopem uživatele je zajištěna pomocí protokolu PCoIP, a také RDP. ThinApp slouží k virtualizaci aplikací. Pomocí této součásti lze vést management aplikací pro koncové uživatele. Horizon Persona Management spravuje jednotlivé uživatelské účty. [30]

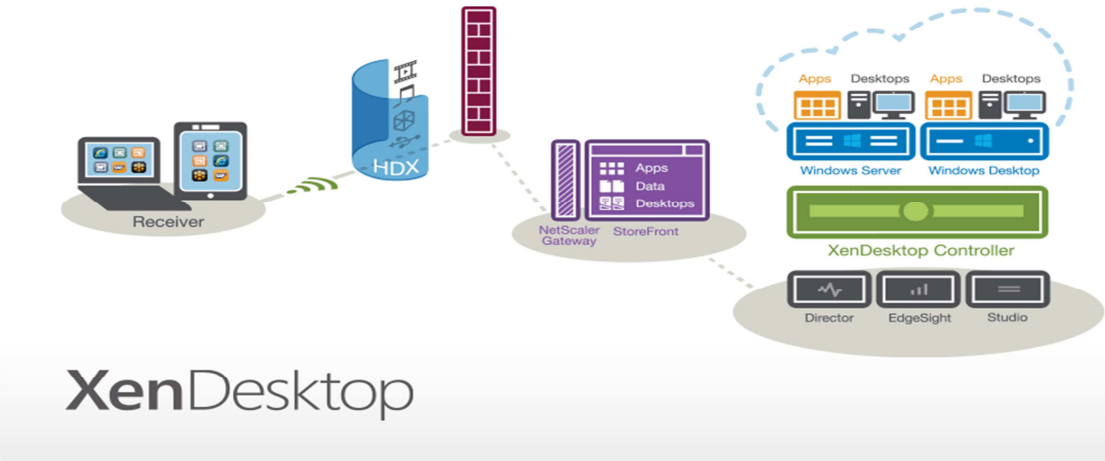


Obr. 10, Schéma struktury VDI [31]

Pro virtualizaci desktopů se využívají dva druhy virtuálních desktopů, a to dedikované a plovoucí. Dedikovaný desktop znamená, že jeden uživatel má jeden virtuální desktop a tento využívá jen on sám. Plovoucí desktop znamená, že při každém spuštění virtuálního desktopu se vytvoří nový virtuální desktop a při odhlášení uživatele se zase smaže. Virtuální desktop se v tomto případě vytváří podle vzorového operačního systému, user profilu a využívá ThinApp pro aplikace. [31]

3.1.2 Citrix XenDesktop

XenDesktop je software pro virtualizace desktopů od společnosti Citrix, který umožňuje více uživatelům přístup a spustit desktopy s OS Microsoft Windows, které jsou nainstalovány v centrálním místě odděleně od přístrojů, ze kterých jsou přístupné. Jedná se tedy o řešení VDI. Uživatelé mohou získat přístup k virtuálním desktopům a aplikacím prostřednictvím klientu Citrix Receiver, což je nainstalovaná aplikace v PC uživatele. Produktem XenApp jsou řízeny aplikace ve virtuálním desktopu. XenDesktop je schopen řídit a poskytovat aplikace a desktopy pomocí connection managera s názvem Desktop Delivery Controller. Podporuje mnoho hypervozorů pro vytvoření virtuálního desktopu jako například XenServer, VMware vSphere a Microsoft Hyper-V. Nástroj pro řízení obrazu se jmenuje Providioning Services. [32] K přenosu obrazu používá svůj vyvíjený protokol ICA místo protokolu RDP společnosti Microsoft nebo PCoIP od společnosti Teradici. Virtual Desktop Agent musí být nainstalován na virtuálním desktopu. Tato technologie zajišťuje přenos obrazu virtuálního desktopu pomocí protokolu ICA, a také obsahuje ovladače pro připojení periferií na desktopu uživatele. [32]



Obr. 11, XenDesktop [33]

Na serveru je nainstalovaná služba vController, se kterým klient komunikuje a je zde označen jako pHost. Pro komunikaci je využit protokol ICA s technologií HDX. Tato technologie optimalizuje výkon serveru a šířku pásma linky, která má za následek poskytnutí desktopu s vysokým rozlišením a plynulý chodu systému. Technologie vController má podobnou funkci jako Connection Server od firmy VMware. Connection Server slouží jako manažer přístupu, ověřuje platnosti licencí a kontroluje uživatelské přístupy. Součásti vCon-

troller je aplikace Director, která určuje uživatelům přístupy a dohlíží na to, aby každý uživatel na základě svých práv měl přístup jen k aplikacím, které potřebuje k práci. Technologie XenDesktop lze spravovat přes webové rozhraní pConsole pomocí technologie XenCenter. V současné době je nabízena verze produktu XenDesktop 7.12. [32]

3.1.3 Microsoft Hyper-V

Součástí Windows Serveru je technologie Hyper-V, která pomocí virtualizace umožňuje spravovat virtualizované výpočetní prostředí. Instalace prvku Hyper-V nainstaluje požadované prvky a volitelně nainstaluje prostředky pro správu. Požadované součásti zahrnují službu Správa virtuálních počítačů technologie Hyper-V, hypervisor systému Windows, zprostředkovatele rozhraní virtualizace WMI a další prvky virtualizace, jako například poskytovatele služeb virtualizace (VSP), ovladač virtuální infrastruktury (VID) a sběrnici virtuálního počítače (VMbus). [34]

Základní prostředky pro správu Hyper-V se skládají z nástrojů pro správu grafického uživatelského rozhraní jako je správce technologie Hyper-V, modulu Microsoft Management Console (MMC) snap-in a nakonec připojení k virtuálnímu počítači, které poskytuje přístup k výstupu videa virtuálního počítače. [34]

Konkrétní běžná praxe technologie Hyper-V pro Windows PowerShell. Windows Server 2012 zahrnuje modul Hyper-V. Přístup ke všem funkcím, i ke kterému není GUI, poskytuje příkazový řádek. [34]

II. PRAKTICKÁ ČÁST

4 POPIS SOUČASNÉHO STAVU

Tato diplomová práce se zabývá možnostmi zabezpečení připojení intranetu do Internetu. Pro potřeby této práce využijeme rozsáhlý intranet Policie ČR. Pro potřeby zajištění výkonu služby policejních útvarů bylo pro komunikaci v rámci Ministerstva vnitra, a tedy i Policie ČR, zřízena intranetová síť „HERMES“. Síť intranet je tvořena z páteřní části sítě intranet a jednotlivých lokálních částí sítě intranet. Správcem páteřní sítě je odbor provozu informačních technologií a komunikací Ministerstva vnitra.

Síť Internet slouží policii k zajištění služební komunikace s veřejností a ostatními uživateli a k získávání informací potřebných pro plnění služebních nebo pracovních úkolů Policie ČR. Z důvodu zajištění bezpečnosti je Internet zcela oddělen od intranetu. Prakticky je to provedené tak, že na každém oddělení je počítač, kde je k dispozici Internet a není připojen do intranetu. Provoz v síti Internet MV může být ze strany správce nebo provozovatelů monitorován za účelem kontroly, zda je tato síť využívána k plnění služebních nebo pracovních úkolů, popř. k činnostem souvisejícím se služební činností. Výhoda úplného oddělení sítě je, že je zajištěna vysoká míra bezpečnosti. Přístup do Internetu na tomto počítači je zajištěna buď pomocí sítě HERMES na samotné VLAN, kde je provoz veden přes firewall a připojení je řešeno pomocí centra služeb. Další možnost je lokální připojení od místního poskytovatele. Provider poskytne router, nebo gateway a následně pomocí LAN je Internet distribuován na počítače. Nevýhoda tohoto řešení je především v praktické stránce. Počítače s Internetem je jen omezené množství, kolikrát je jen jeden počítač na jedno oddělení, kde pracuje i okolo 25 pracovníků. Pracovníci se tedy musí střídat. Pro zajištění provozu Internetu je potřeba další počítač, a to včetně periférií, tvorba další lokální sítě, poplatky za připojení providerovi.

Aby byla zajištěna bezpečnost provozu počítačové sestavy, musí být vybavena antivirovým programem spouštěným po startu operačního systému, který průběžně zajišťuje automatickou kontrolu všech programů a dalších souborů spouštěných, otevíraných nebo zapisovaných při práci na počítačové sestavě, a to včetně pravidelné aktualizace. Dále musí být vytvořena uživatelská konta jednotlivých uživatelů s ověřením přístupu do intranetu pomocí domény. Necentralizované řešení připojení do sítě intranet oddělené lokální sítě od místního poskytovatele dále vede k vysokým nákladům na údržbu a k potřebě více administrátorů pro zajištění všech bezpečnostních opatření.

5 VÝBĚR METODY BEZPEČNÉHO PŘIPOJENÍ K SÍTI INTERNET

Základním požadavkem na zpřístupnění sítě Internet v intranetu bezpečnostní složky Policie ČR je bezpečnost. Do současné doby bylo toto řešeno úplným oddělení Internetu od intranetu. Toto řešení zaručuje bezpečnost sítě intranet. Důvodem tohoto řešení je především práce s citlivými daty, práce s osobními údaji nebo připravenost na krizové stavy a mimořádné události.

Technologie jako firewally, antiviry, přístupová hesla a monitoring perimetru sítě jsou důležitým základem, avšak stále častěji dochází k jejich obcházení, protože zkušení hackeři útočí přímo na aplikace a data a využívají čím dál sofistikovanější útoky. Zvýšení bezpečnosti zpřístupnění do sítě Internet může být právě pomocí virtualizace desktopů. Tímto řešením dosáhneme bezpečné oddělení intranetu od sítě Internet, avšak s velkým množství výhod. Jedná se především o zvýšení dostupnosti Internetu uživatelům, snížení administrativních nákladů, snížení zatížení IT oddělení, snížení nákladů na HW, zvýšení efektivnosti využití HW výkonu především serverů, a také snadnou obnovu dat a zálohování. Celkové zhodnocení virtualizace je uvedeno v kapitole 5.1, a to pomocí SWOT analýzy.

5.1 SWOT analýza řešení VDI

Tab. 2, SWOT analýza, 1. Část [vlastní]

Silné stránky	Slabé stránky
Bezpečnost dat díky uložení v datacentru. Oddělení sítí Internetu a intranetu. Rychlejší zálohování a obnova dat. Flexibilní přerozdělování výpočetních zdrojů a dělení výkonu. Zjednodušení vedení uživatelských operačních systémů a distribuce aktualizací Windows, firewallu a aplikací. Z důvodu flexibility a možného použití ZERO klientů a tenkých klientů je další silná stránka úspora elektrické energie. Schopnost flexibilně reagovat na náhlé okolnosti. Výpadek počítače uživatele lze vyřešit výměnou počítače, a poté se opět uživatel připojí ke svému virtuálnímu desktopu. Internet tzv. „při ruce“ na jednom PC.	Náklady prvotní investice. Vyšší nároky na znalosti IT personálů a administrátorů. V případě, že dojde k výpadku celé virtualizační infrastruktury, pracovnici nebudou mít přístup k Internetu. Některé hardwarově náročné aplikace nemusí ve virtualizačním prostředí fungovat. Nákup a implementace neznámých technologií a orientace v produktech. Nízká rychlost připojení k Internetu v případě velkého množství připojených uživatelů. Hardwarové omezení počtu připojených uživatelů.

Tab. 3, *SWOT analýza, 2. Část [vlastní]*

Příležitosti	Hrozby
Sjednocení pracovního prostředí uživatelů. Kontrola přístupu pomocí Active Directory. Centralizovaná správa připojení uživatelů do sítě Internet. Nižší časové nároky na osobní IT podporu jednotlivým uživatelům. Možnost integrace zálohování. Zamezení závislosti na HW uživatele. Možnost odstranění duplicitních dat uživatelů. Rychlejší zaučení uživatelů na nové aplikace. Umožňuje technologii BYOD. Kontrola provozu a přenosu dat a souborů.	Potřeba eliminace chyb v infrastruktuře virtualizace. Chybný počáteční návrh infrastruktury. Nepochopení potřeb uživatelů. Nízký výkon HW a nízká rychlost sítě. Nekompatibilní síťové prvky. Technologie BYOD je v rámci intranetu Policie ČR nemyslitelná a proti interním nařízením.

5.2 Snížení rizika

Eliminace chyb v infrastruktuře virtualizace

Snížení na co nejmenší možnou úroveň chyb v infrastruktuře dosáhneme spoluprací s externí nebo dodavatelskou firmou, která zajistí kvalitní návrh struktury VDI. Další opatření je kvalitní a pravidelné školení interní zaměstnanců, a to především administrátorů na oddělení informačních systémů. Důležitý je také výběr samotného systému VDI na základě požadavků výkonu služby. Dalším krokem eliminace chyb v infrastruktuře je kvalitně zpracovaná dokumentace a samotná realizace. Při této realizaci musí spolupracovat dodavatelské firmy s interními zaměstnanci s ohledem na zvláštní okolnosti práce v prostorách s neobvyklým režimem, který se týká výkonu služby Policie České republiky.

Chybný počáteční návrh infrastruktury

Oddělení mající za úkol rozvoj informačních systémů nejprve musí vypracovat kvalitní návrh a soupis požadavků, než osloví dodavatelskou firmu. S vypracováním návrhu instruktory může pomoci odborná firma, která dodá návrhy, ze kterých lze vybrat nejlepší možné řešení.

Nepochopení potřeb uživatelů

Hledáme řešení připojení Internetu v uzavřené firemní síti pro pracovníky Policie ČR. Tato práce je velmi specifická a je zde kladen velký důraz na bezpečnost provozu Internetu. Neméně důležitým požadavkem jsou potřeby uživatelů. VDI budou využívat jak řadoví policisté, tak pracovníci Služby kriminální policie a vyšetřovaní, nebo pracovníci celorepublikových orgánů. Tito policisté mohou mít zvláštní požadavky na práci s Internetem. Může se jednat především o rychlost připojení, navštěvování rizikových stránek nebo zajištění anonymity. Je tedy nutné brát na tyto požadavky při realizaci VDI zřetel a zapracovat je do prvotního návrhu.

Nízký výkon HW a nízká rychlost sítě

Technologie VDI se bude implementovat do již vybudované infrastruktury, která musí být na toto připravená a dostatečně výkonná. Nově pořízený HW musí odpovídat zatížení VDI s ohledem na počet připojených uživatelů a způsobu práce na VDI. Dalším faktor je připojení VDI do Internetu, které musí být dimenzované na počet připojených lidí s dostatečnou stabilitou připojení včetně záložního připojení k Internetu a jinou použitou technologií pro přenos dat.

Nekompatibilní síťové prvky.

Při prvotní analýze stávající infrastruktury se zaměřit na kompatibilitu a certifikaci síťových prvků pro použití VDI. Přičemž v případě přijatelné ceny, nekompatibilní síťové prvky vyměnit novými prvky anebo v případě ceny přesahující ustanovenou míru stanovit podmínky stávající infrastruktury do podmínek výběru typu VDI. Při pořízení nových síťových prvků klást důraz na certifikaci pro danou technologii VDI.

Technologie BYOD

Připojení neznámých zařízení nebo zařízení, které si přinesou zaměstnanci do zaměstnání, do firemní sítě intranet není možné. Do intranetu je možné připojit jen služební zařízení, a to především desktopy a notebooky. Bezdrátové sítě jsou v rámci intranetu zakázány až na

výjimečné případy, například při mimořádných událostech, především v těžko dostupných oblastech.

5.3 Výběr produktu pro VDI

Jak je již uvedeno v teoretické části diplomové práce, na trhu existuje řada společností, které se zabývají technologií virtualizace. Pro potřeby Policie ČR byl výběr zúžen na tři největší společnosti na trhu. Jedná se Microsoft, VMware a Citrix. Jednotlivé produkty mají řadu výhod a nevýhod oproti konkurenci. Výběr produktu pro Policii ČR je především ovlivněn cenou a výběrovým řízením. Pro porovnání spíše na velmi obecné rovině z pohledu administrátora a uživatele.

5.3.1 VMware Horizon

VMware má velmi vyspělou serverovou virtualizaci a věnuje se tomu již dlouhou dobu, čím těží pro řešení VDI. Protokol PCoIP, které si zakoupil od společnosti TERADICI je na velmi dobré úrovni. Díky tomu je jejich technologie VDI na velmi dobré úrovni a je vhodná pro použití i v Enterprise prostředí.

Výhody:

Podpora hardwarové akcelerace protokolu PCoIP. Dobrý systém sdílení imagů, který usnadňuje instalace. Jednoduchá implementace do sítě HERMES. Snadná a intuitivní administrace desktopů a stabilní, dobře optimalizované virtuální prostředí.

Nevýhody:

Jako nevýhodu lze považovat závislost na prostředí Active Directory, což v případě architektury intranetové sítě Policie ČR není ani tak vnímáno a je využíváno pro tvorbu domén a organizaci skupin. Nevýhoda tohoto řešení je především v podpoře koncového zařízení technologie PCoIP, a to především procesor musí mít minimálně instrukční sadu SSE2.

5.3.2 Citrix XenDesktop

Citrix má již velmi dobrou funkcionalitu hypervisoru, nicméně ještě mu chybí pokročilá funkcionalita, vyladění stávajících funkcí a kompletní správu těchto funkcionalit z grafického správního nástroje XenCenter.

Výhody:

Citrix je nejstarší společností zabývající se VDI řešeních. Toto se projevuje na komplexnosti a vyzrálosti tohoto produktu. Velkou výhodou je i zmiňovaný hypervizor. Další výhodou je použitý protokol pro přenos obrazu a zvuku Citrix HDX.

Nevýhody:

Mezi základní nevýhodou je cena řešení. Dále celková vyladěnost architektury je mírně za konkurencí. Jako nevýhodu lze uvést složitou instalaci a konfiguraci.

5.3.3 Microsoft Hyper-V

Microsoft těží výhodu především v rodině produktů System Center, které dnes podporují jak fyzické tak virtuální prostředí, ale usilovně pracuje na důležitých enterprise funkcionalitách hypervisoru. Produkty rodiny System Center se používají v intranetu Policie ČR.

Výhody:

Z důvodu sdílení technologií pro fyzické a virtuální desktopy a používání produktů Microsoft v intranetu Policie ČR je především výhoda v ceně pořízení. Další výhoda je komplexní řešení.

Nevýhoda:

Celková konfigurace systému je roztříštěna do několika nástrojů, což v celkovém pohledu ztěžuje administraci celého řešení. Velká nevýhoda je v absenci sdílení image.

5.3.4 Závěrečný výběr

Výběr technologií není jednoduchý, a i když se všechny platformy snaží nabízet stejnou funkcionalitu, pak se významně liší v propracovanosti a vyspělosti jednotlivých funkcionalit. VMware je jasným leaderem a obsahuje ucelenou virtualizační platformu vhodnou pro nasazení do prostředí vybudované intranetové sítě Police ČR. Výběr metody a technologie byl především v gesci Policejního prezidia. Z důvodu sjednocení pracovního prostředí v informačních systémech, unifikace práce s těmito systémy a spojení dostupnosti sítě Internet po celé České republice v rámci intranetu Policie ČR se musela jednotlivá krajská ředitelství policie se přizpůsobit a převzít tyto technologie. Policejní prezidium tedy vybralo technologii od společnosti VMware a následně jednotlivým krajským ředitelství předali licence. Tyto důvody vedly k tomu, že pro potřeby zpřístupnění sítě Internet ve služební síti intranet v Krajském ředitelství policie Jihomoravského kraje byla vybrána technologie virtualizace desktopů od společnosti VMware, a to konkrétně VMware Horizon.

6 IMPLEMENTACE ŘEŠENÍ VDI VMWARE HORIZON

V této kapitole se budeme věnovat nasazení technologie VMware Horizon 7 a její implementaci do uzavřené sítě intranetu Policie ČR. Síťová topologie bude převzata z již vytvořené topologie sítě. Pro potřeby nasazení technologie bude využit blade šasi HP C7000 obsazeno zdroji a ventilátory, dva blade LAN switch HP 6125 XLG 10 Gb/s, dva blade SAN switch Brocade 8/24, dále blade server HP BL460c Gen9 datacentrum HP StorageWorks MSA 2040FC a druhé diskové pole EVA4400 od společnosti HP. V tabulce č. 4. jsou uvedeny základní technické údaje blade serveru HP BL 460c 9. generace.

Tab. 4, Server HP [vlastní]

HP C 7000 Blade	2 x ProLiant BL460c Blade typ
Procesor	2x Intel Xeon CPU E5-2650 @ 2,3 GHz (10 Cores)
RAM	524288 MB, DDR4
Síť	10 GB, 2 port Adapter

V následné tabulce č. 5. jsou uvedeny základní informace o hardwaru diskového pole.

Tab. 5, Diskové pole [vlastní]

I/O Controller	2 x controller SAN, 16/8 Gb/s Fibre Channel ports
Úložný prostor	2 x 200 GB SSD 24 x 600 GB SAS, 15 tis. otáček 24 x 4 TB, SAS, 7,5 tisk. otáček
Zdroj	4 x 432 Watů

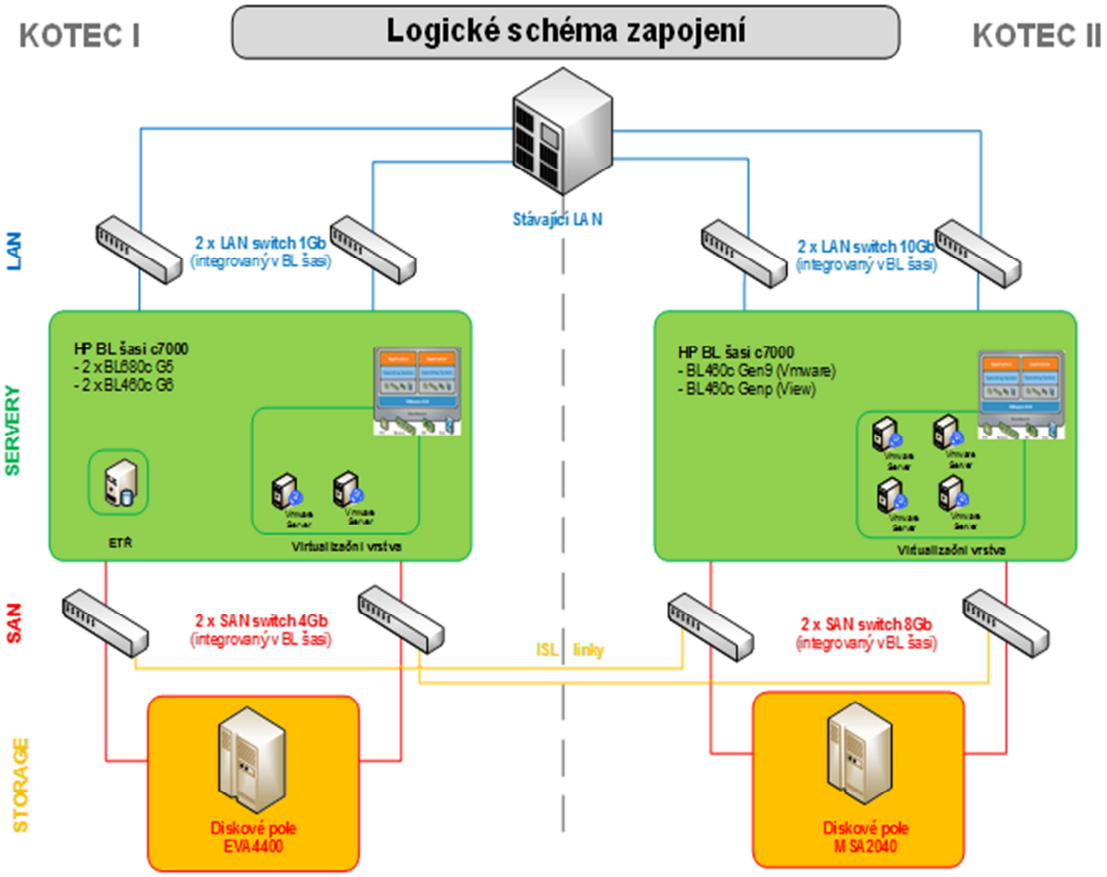
Jako administrativní počítač bude využit stolní počítač s operačním systémem Windows 10 Enterprise, hardwarové vlastnosti jsou uvedené v tabulce č. 6. Počítač bude sloužit k administraci VMware Horizon, a také zde poběží virtuální PC, kde budeme testovat připojení k virtuálnímu desktopu s přístupem do sítě Internet.

Tab. 6, Administrátorské PC [vlastní]

Základní deska	HP FXN1
Procesor	Intel Core i3-2100 CPU, 3,1 GHz
RAM	20 GB, 1060 MHz
HDD	4 TB, SSDH Seagate
Síťová karta	Intel 82579 LM Gigabit Network Connection

6.1 Logické zapojení a implementace do intranetu

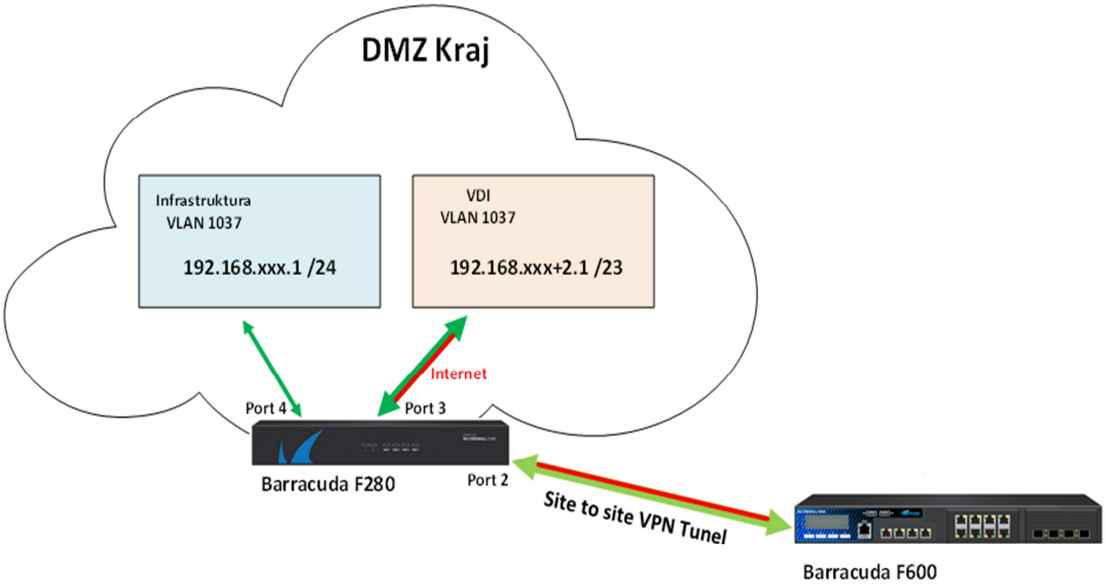
Logické schéma propojení jednotlivých částí je uvedeno na obrázku č. 12. Topologie sítě intranetu Policie ČR je velmi složitá, proto zde nebude uvedena celá. Každá budova Policie ČR má několik síťových prvků, podle její velikosti a počtu koncových zařízení zapojený do sítě. Struktura VDI je rozdělena do dvou racků (kotců), která je propojena se stávající sítí pomocí dvou LAN switchů integrovaných v blade šasí, typu HP BL 460c 9. generace. Následně podle schématu jdou rozdělené servery na dva. Poté jsou v každém racku dva SAN switche Brocade 8/24, které slouží ke spojení s diskovými poli. Tyto switche jsou propojeny ISL linky mezi jednotlivými racky.



Obr. 12, Logické schéma zapojení [vlastní]

6.2 Konfigurace Next Generation firewallu

Pro potřeby VDI využijeme hardawarové firewally od firmy Barracuda. Tyto firewally využíváme z důvodu dobrých zkušeností. Připojení VDI k Internetu je založeno na systému VPN. Firewally se nacházejí na dvou místech v Praze a pro Krajské ředitelství policie Jihomoravského kraje v Brně. Mezi těmito, jak je vidět na obrázku č. 13, je VPN Tunel, a to konkrétně mezi firewally Barracuda TINA. V Brně je umístěna Barracuda F280 a v Praze v centru služeb je Barracuda F600. Povolené služby jsou HTTTP/s a FTP. Na kraji jsou povoleny služby NGF, konkrétně brána, DHCP, firewall demitilirazed zone (DMZ) a VPN. Na obrázku č. 13 je uvedeno základní schéma připojení k Internetu. Komunikace je řešena logickými nezávislými sítěmi, známé jako VLAN.



Obr. 13, Základní infrastruktura Firewallů [vlastní]

6.3 Základní architektura VDI

Následně si uvedeme architekturu VDI VMware Horizon:

A. vCenter server ve verzi 6.0.

B. vRealize Operations Manager

C. Connection server

D. Composer

E. Secure server

F. Persona Management

G. ThinApp

H. Microsoft SQL Server 2014

I. Workspace

J.Group Policy

K. Active direktory Windows 2012 R2

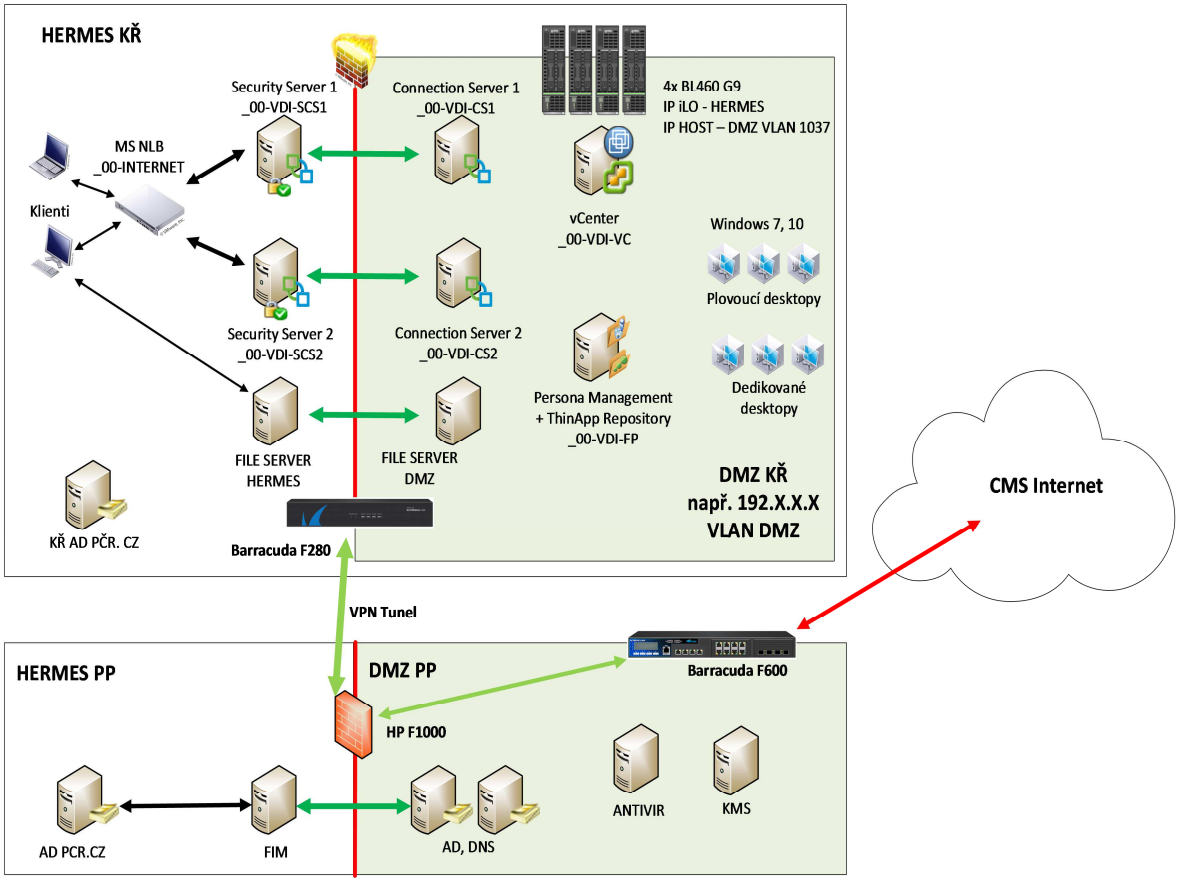
L. Key Management Service

M. WSUS

N. Antivir

O. VUM Repository

Na obrázku č. 14 je zobrazeno schéma rozložení architektury VDI. Obrázek je rozdělen na čtyři díly. Síť Hermes kraje s DMZ kraje je na horní části, zde si připojují klienti VDI a v DMZ je připojen vCenter. Ve spodní části je část struktury umístěná v Praze v distribučním centru.



Obr. 14, Architektura VDI [vlastní]

7 INSTALAC□ ZÁKLADNÍCH PRVKŮ VMWAR□ HORIZON

7.1 Nasazení hypervizoru VMware ESXi

Hypervizor ESXi ve verzi 6.0., jehož instalace je v interaktivním módu velmi jednoduchá, lze instalovat ze sítě nebo přímo z DVD média.

A. Instalaci provedeme lokálně pomocí DVD média. Tento způsob instalace musí být povolen, jinak nedojde ke správnému načtení DVD média.

B. Pokračujeme podle pokynů na obrazovce. Akceptování smluvních podmínek, pomocí kláves F11 se dostaneme do dalšího koku.

C. Následně musíme zvolit disk v zobrazeném seznamu dostupných disků pro instalaci. Zvolíme lokální disk. Tento je zapojen sběrnicí SAS.

D. Poté zvolíme administrátorské heslo, nick a rozdělení klávesnice. Toto vše budeme potřebovat později.

Obr. 15, Instalace ESXi, [vlastní]

E. Po potvrzení stisknutím tlačítka F11 dojde k samotné instalaci software včetně restartu serveru, přičemž po restartu je software ESXi nainstalovaný.

F. V intranetu MV používáme statické IP adresy. Dynamické přidělování IP adres pomocí protokolu DHCP se využívá jen zcela výjimečně. Defaultně je toto zakázáno. ESXi server

však je nastaven právě tak, aby získalo IP adresu automaticky. Takže musíme změnit nastavení a zadat statickou IP adresu. Zvolíme tedy konzolu Direct Console Uset Interface a v nabídce Customize Systém, dále zvolíme bod Configure Management Network. Zde zvolíme volbu Set static IP address and network configuration, která se nachází v položce IP Configuration 10.208.xxx.xxx Zde nastavíme IP adresu, masku podsítě a výchozí bránu.

Obr. 16, Nastavení IP adres ESXi [vlastní]

G. Dalším krokem je instalace vSphere Clienta na administrátorském PC. VMware instalaci přichystal velmi intuitivně a instalace je tedy velmi jednoduchá. Pro instalaci vShere Clienta je potřeba nainstalovat NET Framework, který je pro funkci vShere Cleinta nezbytný. Spustíme tedy instalační soubor, vybereme jazyk instalace a následně souhlasíme s licenčním ujednáním.

H. Pro správu softwaru ESXi serveru musíme po jeho spuštění zadat několik hodnot. Jedná se o zadanou IP adresu nebo Hostname. Dále po nás software bude požadovat administrátorské heslo a uživatelské jméno. Po ověření hodnot se načte prostředí vSphere pro správu ESXi serveru.

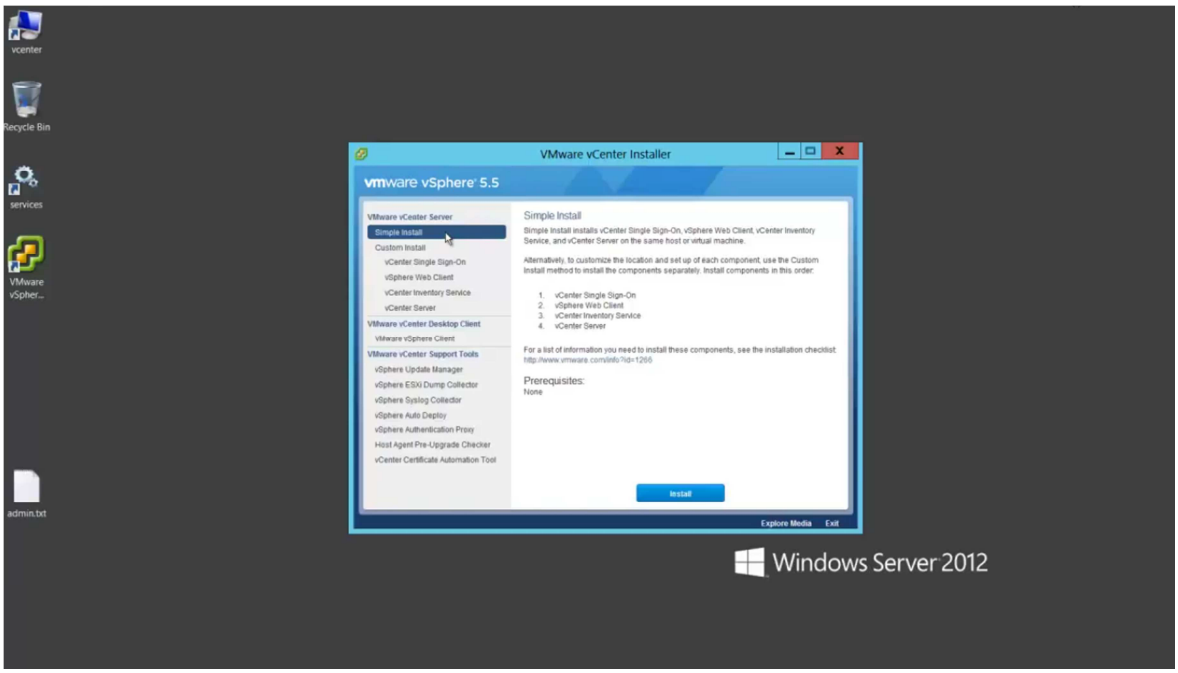
7.2 Instalace vCenter Server 5.5.

A. K běžícímu serveru se lze připojit několika způsoby. Jeden způsob je pomocí softwaru pro správu klientů Systém Center Configuration Manager, a to pomocí nástroje Remote Control. Další možnost je využití Remote Desktop Clienta, která je součástí OS Windows

10 Enterprise. Tuto konzoli získáme zadáním příkazu mstsc.exe. Třetí možnost je pomocí nainstalované konzole dostupné v prostředí vSphere. Ke konzoli se dostaneme tak, že označíme server, na který chceme vCenter Server nainstalovat, a následně otevřeme záložku Console.

B. Použijeme aplikaci Remote Desktop Clienta pro vzdálenou správu (RDC). Po spuštění aplikace jsme vyzvání k zadání IP adresy serveru, administrátorského jména a hesla. Soubory potřebné pro instalaci vCenter Server je součástí instalačního packu vSphere 5.5, který je uložen na disku.

C. SW vCenter instalátor obsahuje čtyři základní instalace, a to vCenter Single Sign On, vCenter Inventory Service, vCenter serveru a Microsoft NET 3.5 SP1 framework. První instalovanou službou je ověřovací služba vCenter Single Sign On, která zabezpečuje spolehlivější spojení mezi prvky vSphere zprostředkováním tokenového mechanismu směny informací na místo toho, aby každá složka musela být samostatně ověřována s adresářovou službou Active Directory. Druhá položka je vCenter Inventory Service, která snižuje požadavky vCenter serveru, a tím i jeho vytížení. Poté se instaluje vCenter server a nakonec NET Framework, který je potřeba pro spouštění grafického rozhraní vCenter serveru.



Obr. 17, Instalace vCenter [vlastní]

D. Prvně instalované vCenter Single Sign On vyžaduje souhlas licenčních práv a nastavení osmimístného hesla pro administrátorský účet.

E. Pro naše řešení využijeme Microsoft SQL Server 2012, který je již implementovaný v síti intranet. SQL server je potřebný pro organizaci a ukládání dat serveru.

F. V další části instalace v sekci Local System Information v oblasti Fully Qualified Domain Name or IP address je hodnota automaticky uvedená. Server se nazývá B00-internet a doménové jméno je pcr.cz

G. Z důvodu přihlášení na serveru jako doménový administrátor, v části Security Support Provider Onterface Services Information neuvádíme uživatelské jméno a heslo, ale jen potvrdíme volbu Use network services account.

H. Defaultně nastavený šifrovaný port HTTPS a adresář, ponecháme ve výchozím stavu. Následně software nainstalujeme volbou tlačítka Install.

I. Po dokončení instalace se zahájí instalační proces vCenter Inventory Services, zde v sekci Licence Key vložíme licenční klíč.

J. Z důvodu existující databáze SQL a většího množství připojených lidí není vhodné využít volbu Microsoft SQL Server 2012. Proto zvolíme možnost Use An Existing Supported Database a v nabídce si vybereme ODBC DSN, který je předem nachystaný.

K. V části vCenter Server Service a Configure Ports necháme defaultní nastavení. V sekci vCenter Server JVM Memory zvolíme volbu Medium Inventury (hosts 100-400), a to z důvodu licenčních omezení připojených lidí v jedné chvíli na počet 200 hostů. Následně zvolíme políčko install, čímž se začne vCenter Server instalovat. Po dokončení server restartujeme. Může nastat situace, že po restartu vCenter se nelze přihlásit k serveru pomocí vSphere klienta. Pravděpodobná příčina je, že ne všechny služby SW vSphere byly spuštěny. Po zadání příkazu services.msc (Služby) v nabídce Start systému Windows Server 2012 Enterprise s aplikací vCenter Server spustíme seznam služeb. Zde si prohlídneme, zda všechny služby VMware jsou spuštěné. Pokud nejsou, spustíme je. Poté se vyzkoušíme opět přihlásit do služby vCenter.

Tab. 7, vCenter Server Inventory [vlastní]

vCenter Server Inventory	VMware vCenter Management Web-services	Inventory Service	Profile-Driven Storage Service
Small inventory (1-100 hosts or 1-1000 virtual machines)	512 MB	3 GB	1 GB
Medium inventory (100-400 hosts or 1000-4000 virtual machines)	512 MB	6 GB	2 GB
Large inventory (More than 400 hosts or 4000 virtual machines)	1 GB	12 GB	4 GB

L. Ve službě vCenter Server vytvoříme data centrum s názvem VD-internet. Na vytvořená datacentra klikneme pravým tlačítkem myši a zvolíme Add Host. Spustí se jednoduchý proces pro přidání nového hosta. Zadáme IP adresu serveru a přihlašovací údaje systému ESXi.

7.3 Instalace služby View Composer

Na server, kde je nainstalována služba vCenter Server nainstalujeme aplikaci Horizon View Composer pro podporu linkovaných klonů. Instalace je poměrně jednoduchá. Spustíme instalační soubor, potvrdíme licenční ujednání a adresář instalace necháme stejný. V části Database Information je potřeba nastavit Data Source Name (DSN) pro databázi sw View Composer. Toto nastavení se provádí pomocí tlačítka ODBC DSN Setup. Kde v záložce DSN uvedeme systémový zdroj dat s názvem, který se vytvořil při instalaci vCenter Server. Všechny ostatní hodnoty necháme ve výchozím stavu. Po dokončení instalačního procesu se server restartuje.

7.4 Konfigurace serverů v Horizon View Administrator

Pro tvorbu virtuálních desktopů, a také proto, aby se na tyto desktopy mohli přihlašovat, musí být na serveru nainstalován Connection Server. V intranetu Policie ČR pro část policie Jihomoravského kraje máme Connection server nainstalovaný na serveru s operačním

systémem Windows Server 2012 Enterprise. Následně uvedeme krátký popis konfigurace serverů.

A. Na systémové ploše desktopu spustíme webovou aplikaci View Administrator Console, která pomocí prohlížeče Internet Explorer 11 spustí aplikaci Vmware Horizon View. Vypíšeme administrátorské heslo a jméno. V části Inventory pokračujeme položkou View Configuration, kde otevřeme záložku Server.

B. Klikneme na tlačítko Add, kde přidáme nový vCenter Server a View Composer. V položce vCenter Server Settings vyplníme IP Adresu serveru, pak uživatelské jméno a heslo. Zbytek ponecháme v defaultním nastavení.

C. Poté pokračujeme v nastavení View Composer, a to v položce Settings. Zde zvolíme volbu View Composer co-installer with vCenter Server, a to z důvodu umístění sw na stejném serveru.

D. Dalším krokem jsme pokročili až do sekce View Composer Domain. Zde přidáme doménová jména, uvedeme administrátorské jméno a heslo. Zbytek položek necháme ve výchozím nastavení. Poté zvolíme položku Finish a nyní vidíme v konzoli VMware Horizon View Administrator server vCenter Server.

7.5 Vytvoření vzorového desktopu pro linkový klon

Na začátku musíme vytvořit vzorový desktop, který nastavíme a upravíme tak, aby byl vhodný pro použití ve virtuálním prostředí a vhodně sloužil svému účelu. V případě našeho virtuálního desktopu, který bude sloužit pro připojení k síti Internet, obsahuje mimo jiné prohlížeče Google Chrome, Internet Explorer a Firefox. Tento připravený desktop, v našem případě Windows 7 Enterprise, musí být vložen v doméně. Na každém fyzickém desktopu uživatele běží v pozadí systému agent, který běží jako služba. Tato služba má za úkol prostřednictvím protokolů PCoIP nebo RDP přenést obraz virtuálního desktopu uživateli. Tato služba také poskytuje informace Connect serveru o stavu fyzického desktopu, obsahuje ovladače pro lecjaké periferie. Pro zvýšení grafického komfortu bude také nainstalován balíček VMware Tools.

A. Spustíme správu vCenter Server pomocí aplikace vSphere Clienta. Poté pravým kliknutím myši v kontextové nabídce vybereme položku Guest a následně Install VMware Tools.

B. V položce Console se nalogujeme do systému. Spustíme instalační souhlas v instalačním médiu, který se nachází ve virtuálním DVD-ROMu a VMware Tools, pomocí jednoduchého průvodce nainstalujeme.

C. VMware Horizon View nainstalujeme do vzorového virtuálního desktopu pomocí instalačního souboru a virtuální desktop restartujeme.

7.6 Klonování vzorového desktopu

A. Abychom mohli začít klonovat vzorový desktop, musíme se přihlásit jako administrátor k serveru s aplikací Connection server, kde otevřeme VMware Horizon View Administrator konzoli.

B. Zde se nachází položka Inventory a položka Pools, kde vedeme vytvořené druhy desktopů. Pro přidání klikneme na tlačítko Add a vybereme Automated Pool.

C. V další části User Assignment vybereme položku Dedicated Desktop pro desktop, který má uživatel stále stejný, a pokračujeme tlačítkem Next. Z důvodu vytvoření linkovaných klonu vybereme položku Composer linked clones a opět klikneme na Next.

D. Pojmenujeme skupinu virtuálních desktopů B00-VDI.

E. V části Provisioning Settings konfigurujeme pojmenovávání virtuálních desktopů. Jména se tvoří automaticky. V našem případě budou desktopy pojmenovány B00-VM-F-001 až B00-VM-F-199.

F. V další části konfigurace Dispozable File Redirection a Replica Disk zůstanou ve výchozím nastavení.

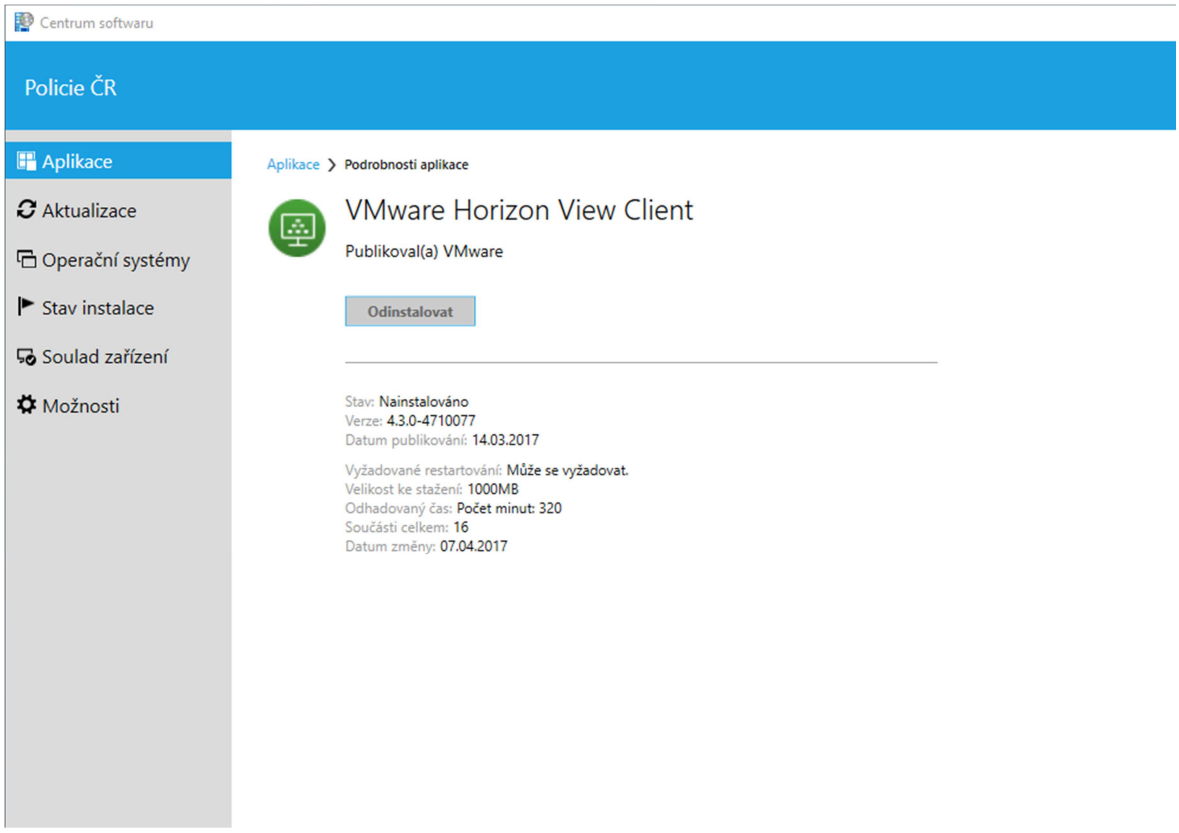
G. V kroku vCenter Settings konfigurujeme 3 věci. V první části Default Image vybereme hlavní obraz pro virtuální desktop, ten co jsme si dříve nachystali. V našem případě OS Windows 7. V druhé části s názvem Virtual Machine Location vybereme lokaci našeho datacentra a ve třetí části konfigurace s názvem Recource Settings vybereme adresu námi vytvořeného ESXi serveru. Nakonec zvolíme lokaci, kam se data virtuálního desktopu budou ukládat. Vše ostatní můžeme nechat v defaultním nastavení.

H. V grafickém rozhraní View Administrator se nám zobrazí v záložce Pool skupina virtuálních desktupů s názvem B00-VDI a desktopy B00-VM-F-001 až B00-VM-F-199. V případě, že jsou desktopy připravené k použití, je u nich status Available. V případě, že

status je Customizing, je potřeba nastavit IP adresu virtuálního desktopu. Nakonec v záložce Pools nastavíme Entitlements pro skupinu uživatelů, která ji bude využívat podle přístupu v AD.

7.7 VMware Horizon View Client na fyzickém desktopu

Instalace VMware Horizon Clienta na fyzickém desktopu je potřebný pro připojení k virtuálnímu desktopu. K instalaci využijeme nástroj Centrum softwaru, který je součástí SCCM. Instalace se provede buď automaticky na základě přidělených práv z AD, Centrum software nainstaluje aplikaci VMware Horizon View Client. Druhá možnost je manuální vyvolání instalace. Po spuštění klienta je uveden název serveru B00-internet.pcr.cz, uživatelské jméno a heslo. Dále lze zvolit některou z domén. U nás je k dispozici doména pcr.cz.



Obr. 18, Instalace Horizon View Client [vlastní]

8 PRVKY BEZPEČNOSTI VMWARE HORIZON

8.1 Přístupová práva do virtuálních desktopů

Přístupy do virtuálních desktopů jsou řízeny pomocí centralizované bezpečnostní adresářové služby Active Directory protokolem LDAP. Zde jsou vytvořené logické skupiny uživatelů a desktopů na základě struktury Policie ČR. Každému uživateli jsou přiděleny práva nebo přístupy do různých informačních systémů. Stejným způsobem je přistupováno i k této službě. Uživateli, který získá na základě rozhodnutí jeho nadřízeného pracovníka přístup do tohoto systému, jsou přiděleny přístupy v Active Directory, čímž získá í přístup do virtuálního desktopu. vCenter Server využije uživatele a skupiny definované touto službou včetně přístupů.

8.2 Snímkování

Administrátor má možnost vytvořit v určitých časových bodech kopie virtuálních počítačů, čemuž se říká snímky virtuálních počítačů. Tento snímek zaznamená stav virtuálního počítače v určitém stanoveném čase. Tato funkce slouží administrátorovi k navrácení změny provedené na virtuálním desktopu od posledního snímku. Abychom mohli vytvořit snímek, který budeme potřebovat pro vytvoření linkovaných klonů, musíme snímek pořídit. Snímek pořídíme, když je virtuální desktop vypnutý. Postupujeme následovně.

A. Konfiguraci provedeme ve správě vCenter Server, který otevřeme prostřednictvím vSphere Client.

B. Vypneme desktop a pravým tlačítkem myši klikneme na desktop, kde dále zvolíme položku Snapshot a zde Take Snapshot. Zobrazí se okno Take Virtual Machine Snapshot, kde vyplníme název snímku a snímek potvrdíme.

8.3 Modul správce aktualizací

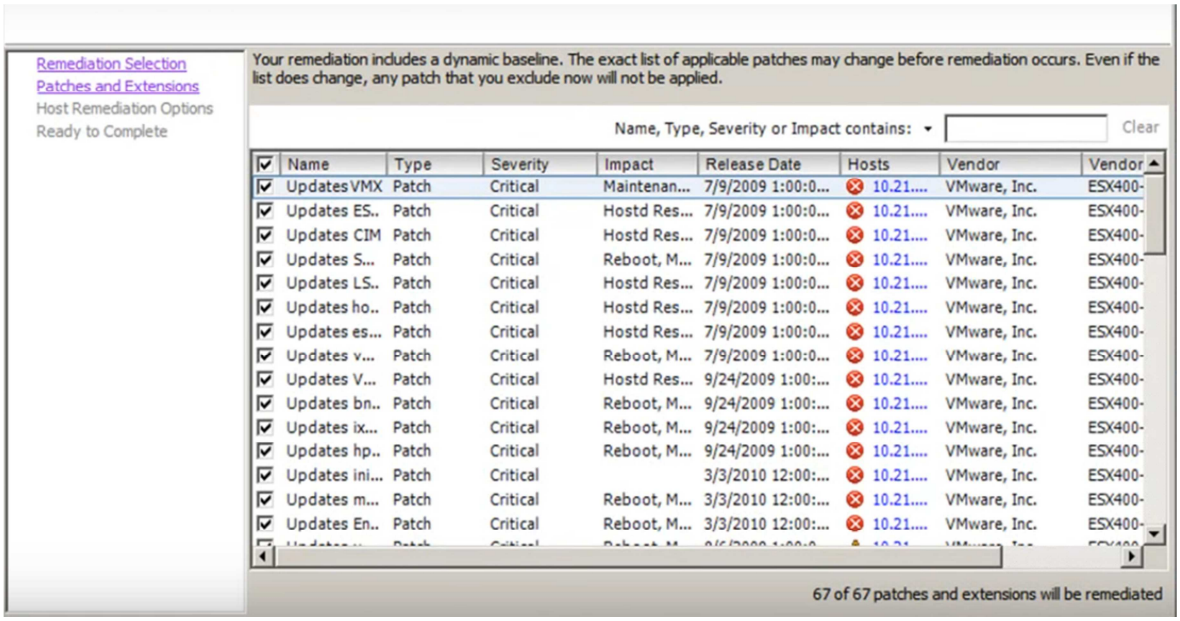
Nástroj a správce aktualizací je plně integrován do podobně zásuvného modulu v serveru vCenter Server i klienta v Sphere Clienta. Musíme jej však nainstalovat. Update Manager. Postup je jednoduchý:

A. Spustíme klienta vSphere Client a připojíme se k vCenter Serveru. V nabídce zásuvných modulů Plug-ins vybereme položku Manage plug-ins.

B. Následně zvolíme rozšíření správce aktualizací a klikneme na položku Download and Install, přijmeme licenční podmínky a dokončíme instalaci.

C. Po dokončení instalace se stav modulu změní na Enable.

Poté máme dispozici nástroj pro vyhledávání aktualizací softwaru vSphere. Na obrázku č. 20 je výpis aktualizací pro provedené analýze modulem Update Manager.



Obr. 19, Seznam aktualizací v Update Manager [vlastní]

8.4 Zabezpečení virtuálních počítačů

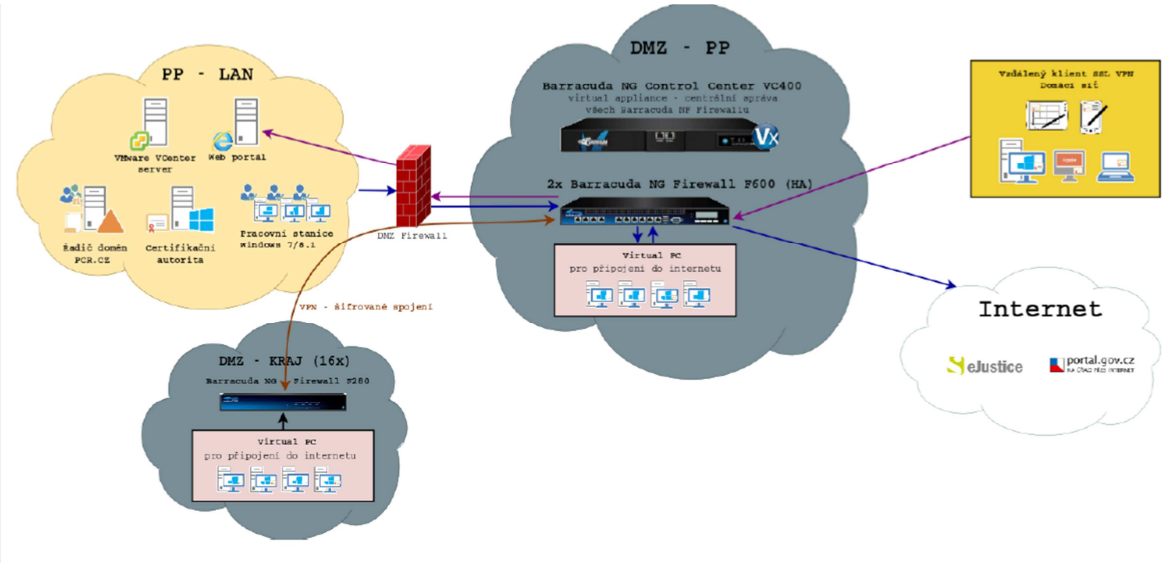
Otázka zabezpečení virtuálních počítačů je založena na zabezpečení operačních systémů běžících na virtuálních desktopech. Pravidla zajištění zabezpečení virtuálního OS Windows 7 Enterprise jsou stejná jako na běžném desktopu. V našem prostředí to znamená pravidelná aktualizace všech nainstalovaných programů, operačního systému a antivirové ochrany. Další prvek bezpečnosti je nastavení uživatelských práv a místních zásad. Každý uživatel má na základě pracovních úloh přidělena práva a oprávnění. Běžný uživatel nemá administrátorské práva.

V prostoru virtuálních sítí vSphere jsou defaultně nastavené pravidla promiskuitního režimu, změny adresy MAC a falešné přenosy. Všechny tyto pravidla vypneme. Deaktivovaným promiskuitním režimem znesnadníme packet sniffing. V případě IDS/IPS povolíme promiskuitní režim jen na určitém portu pro konkrétní virtuální desktop. Deaktivace změny adresy MAC a falešných přenosů, hostitel porovná zdrojovou MAC adresu, která je přená-

šena operačním systémem s MAC adresou adaptéru, aby zjistila, zda se shodují. Pokud se adresy neshodují, vCenter server komunikaci přeruší.

8.5 Firewall

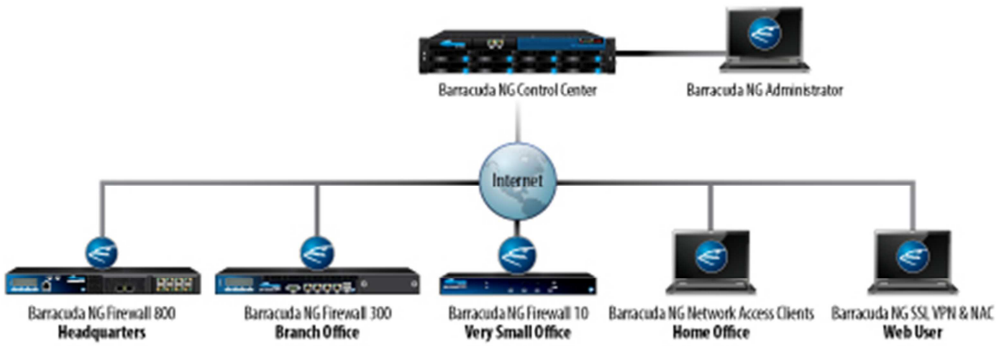
Pro zajištění dostatečné ochrany přístupu do Internetu jsou použity hardwarové firewally od firmy Barracuda. Na každém kraji se nachází typ Barracuda F280. V distribučním centru v Praze jsou poté dva firewally Barracuda F600. Oba dva se navzájem nahrazují. Jeden je tedy záložní. Datový tok vede jen přes jeden. V distribučním centru je dále Barracuda NG Control Center VC400. Tento firewall slouží jako centrální správa všech Barracud, které jsou k ní připojeny.



Obr. 20, Firewall Barracuda [vlastní]

Na obrázku č. 20 je znázorněna architektura provedení demilitarized zone (DMZ). Ta je řešena jako fyzická oddělená síť od ostatních síťových prvků. V této zóně jsou jak na centrální úrovni v Praze, tak na krajské úrovni. Jednotlivé DMZ jsou odděleny firewallem. V jednotlivých DMZ se nacházejí podle architektury různé prvky VDI. V centrální části se nachází vCenter server, webové portály, AD, certifikační autority a pracovní stanice. Na krajské úrovni je to podobné, jen se zde nenacházejí některé centrální prvky správy systému.

V případě připojení uživatele mimo intranet MV, musí uživatel použít firewall Barracuda a připojit se k síti VDI pomocí VPN. V jiném případě nebude spojení navázáno.



Obr. 21, Baracuda NG Control Center [35]

8.6 VPN

Mezi jednotlivými firewally, které leží na krajích a v centru služeb v Praze, je provedeno spojení pomocí virtuální privátní sítě, tedy VPN. Firewally od firmy Barracuda používají svůj systém tunelování, který nazývá TINA. Mezi firewallem Baracuda a jiným výrobcem firewallu je použit systém bezpečnostního rozšíření IPsec. Dále si uvedeme postup instalace VPN TINA.

A. Přihlásíme se do Barracuda NG Firewall.

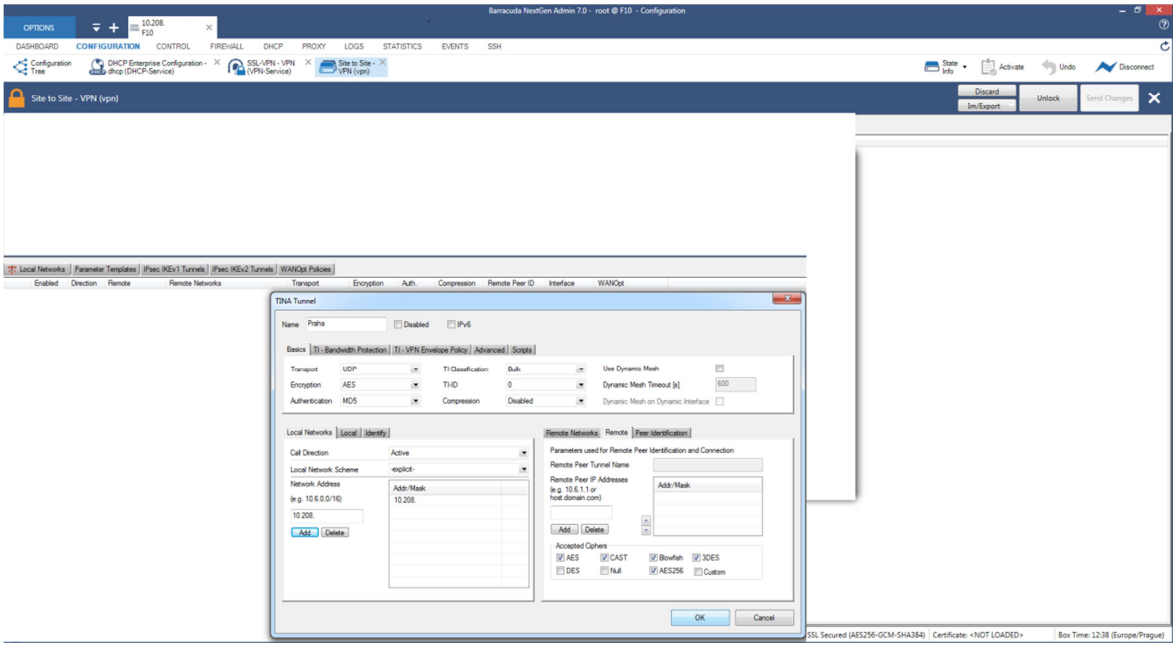
B. Klikneme na položku Site to Site, kde vybereme položku TINA tunnels. Následně klikneme pravým tlačítkem a zvolíme New TINA tunnel. V levé horní polovině nové spojení pojmenujeme v našem případě Praha.

C. V tomto okně, v jeho levé části, provedeme nastavení spojení. Zavedeme Local Network Address, a to 10.208.XXX.XXX/XX, pak klikneme na Add. V pravé části klikneme na Remote a zde uvedeme 10.208.XXX.XXX/XX, a také klikneme Add.

D. Dále klikneme na záložku Local a zde IP Location nastavíme na Dynamic.

E. V této části nastavení musíme vložit Public Key. Pokračujeme na položku Identify, kde zvolíme Export Public Key to Clipboard a vložíme key.

F. Poté vše potvrdíme a klikneme na Active.



Obr. 22, Nastavení Firewallu [vlastní]

8.7 Protokol PCOIP

V každé DMZ je pro podporu vzdáleného přístupu další komponenta, a to View Security Server. Tento server zajišťuje spojení mezi firemním počítačem a virtuálním desktopem. Pomocí tohoto serveru se můžeme připojit i z Internetu. Pro spojení využívá protokol PCoIP. Tento protokol slouží k zapouzdření zobrazovacích paketů v UDP a ne v TCP. Abychom mohli využívat View Securty Server a zabezpečení PCoIP, musíme toto nakonfigurovat:

A. Přihlásíme se do View Administrator, kde klikneme na položku Servers. Vybereme v položce View Connection Servers server, kde chceme Secure Getaway spustit.

B. Klikneme na Edit a poté zvolíme položku Use PCoIP Secure Getaway for PCoIP connections to desktop.

C. V položce http/s Secure Tunnel uvedeme externí URL adresu nebo IP adresu pro připojení vytvoření tunelu. V našem případě, tedy https://x26-internet.pcr.cz, port uvedeme 443.

D. Do políčka PCoIP Secure Getaway uvedeme IP adresu serveru, a to 10.208.xxx.xxx a port 4172.

E. Tlačítkem OK potvrdíme konfiguraci.

8.8 Systém prevence narušení

Systém prevence narušení (IPS) je spuštěn na všech hardwarových firewallech Barracuda použitých v architektuře VDI. Celý systém IPS je řízen centrálně pomocí Barracuda NG Control Center, kde dochází k automatickým aktualizacím databáze. V případě potřeby je možné na jednotlivých firewallech nastavit vlastní politiku IPS. V centrálním firewallu je vytvořen vzor, který je potom dodán do všech připojených firewallů. Defaultně je IPS zapnuto. V případě, že chceme mít provoz bez IPS, musíme zvolit NO Scan Policy, což v našem v případě není nastaveno.. Pro zvýšení bezpečnosti však můžeme provést změny v konfiguraci IPS:

A. Přihlásíme se do firewallu a zvolíme položku IPS Policies, kde klikneme na LOCK.

B. Poté zvolíme Enable IPS. Pro filtraci škodlivého provozu zakážeme Report Only. Je vhodné vše provést až v zaběhlém systému, aby nedocházelo k blokaci i neškodlivé komunikace.

C. Pro kontrolu SSL komunikace zvolíme políčko Scan SSL – Intercepted Traffic.

D. Následně nastavíme politiku IPS. Rozdělena je pro klienta (for client) a pro server (for server). Dále jsou události rozděleny podle vážnosti, a to na kritický, vysoký, střední, nízký a informační (Critical, High, Medium, Low, Informational). Zde můžeme volit možnosti a to zastavení provozu (Drop) nebo logování (Log) a dále způsob upozornění na Aler, Warn nebo Notice. V kritických a vysokých stupních události nastavíme akci zastavit a vysoký stupeň upozornění. Ve středním, nízkém a informačním stupni události nastavíme logování a stupeň upozornění warm, a to jak pro uživatele, tak pro server.

E. Vše potvrdíme, čímž zpustíme IPS politiku.

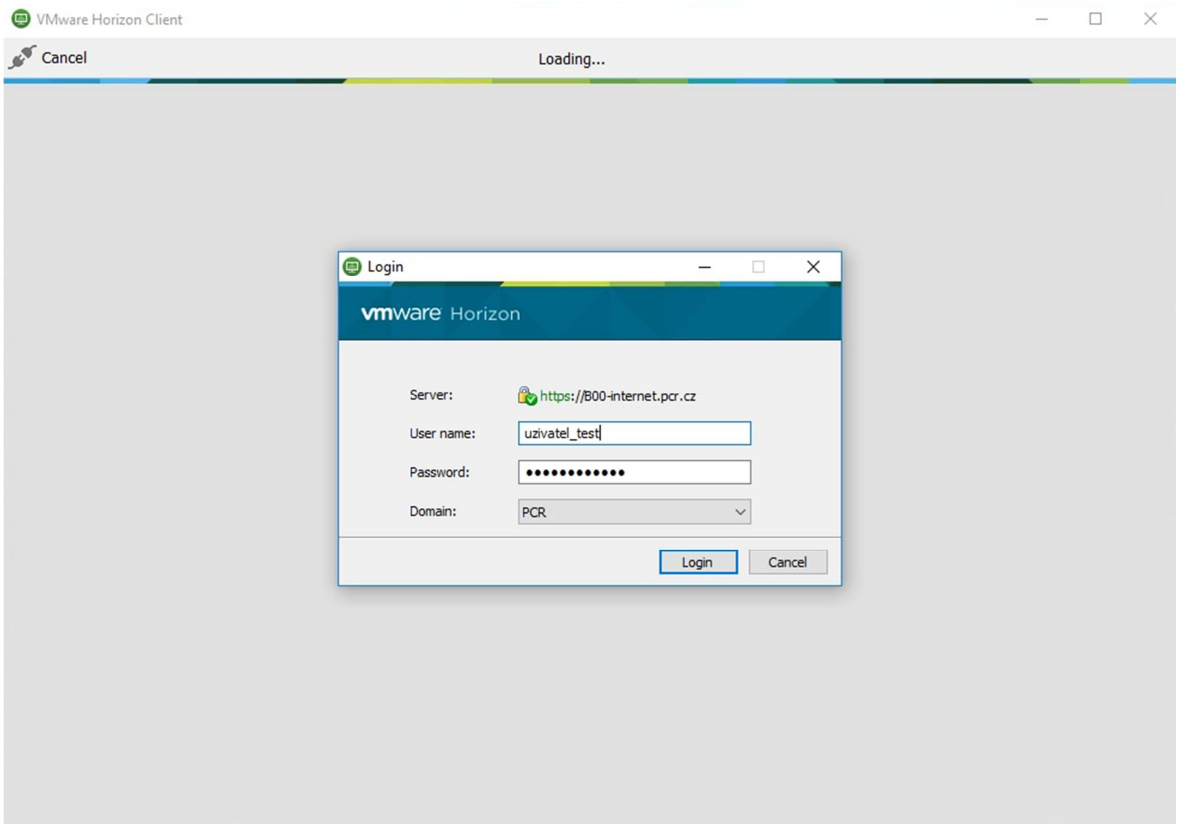
Propustnost IPS na firewallu Barracuda F280 je 450 Mb/s a firewallu Barracuda F600 je 3,9 Gb/s.

9 T□STOVÁNÍ Ř□Š□NÍ VDI V R□ÁLNÉM PROVOZ□

Technologii virtuálních desktopů máme nainstalovanou a naimplementovanou v intranetu a nyní naše řešení můžeme otestovat. Testování budeme provádět na běžícím systému VDI a na administrátorském počítači.

Přihlášení uživatele s uděleným přístupem v Active Directory

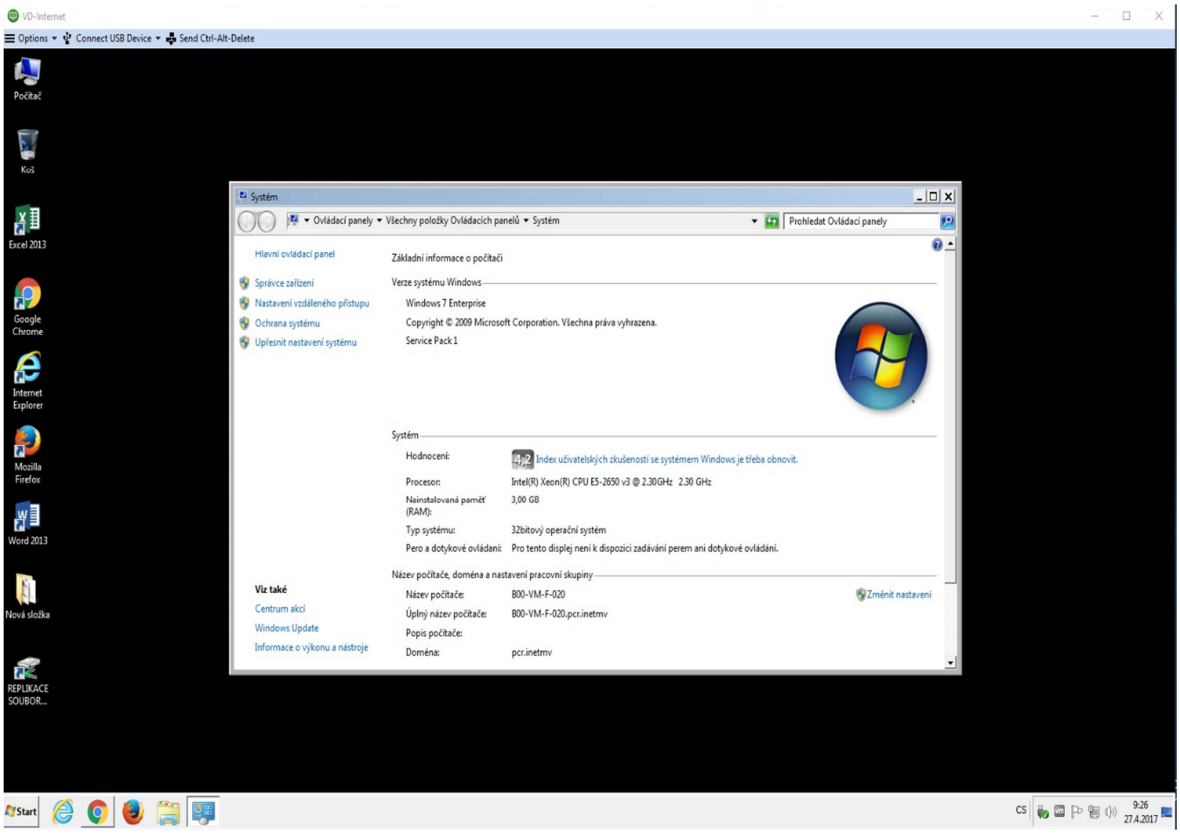
Prvně se pokusíme přihlásit pomocí klienta uživatele, který má přístup. Na obrázku č. 24 je zobrazen uživatel pod názvem uzivatel_test, který má vložené oprávnění v AD pro přístup do VMware Horizon jako běžný uživatel bez administrátorských práv. VMware Horizon client se uživateli nainstaloval po restartu systému automaticky a bezobslužně pomocí Centra softwaru, který je součásti System Center Configuration Manager. Společně s tímto klientem je nainstalován i VMware Tools. Poté byl proveden pokus o přihlášení k virtuálnímu desktopu. Toto přihlášení bylo úspěšné. Uživateli byl vygenerován virtuální desktop s celým názvem B00-VM-F-020. S doménou pro Internet pcr.inetmv. Virtuální desktop má přidělen 3 Gb operační paměti a 30 Gb místa na diskovém poli pro ukládání souborů. Pokusem jsme zjistili, že prvky architektury VDI jsou funkční.



Obr. 23, Přihlášení do systému VDI [vlastní]

Test plovoucího desktopu a ThinAppu

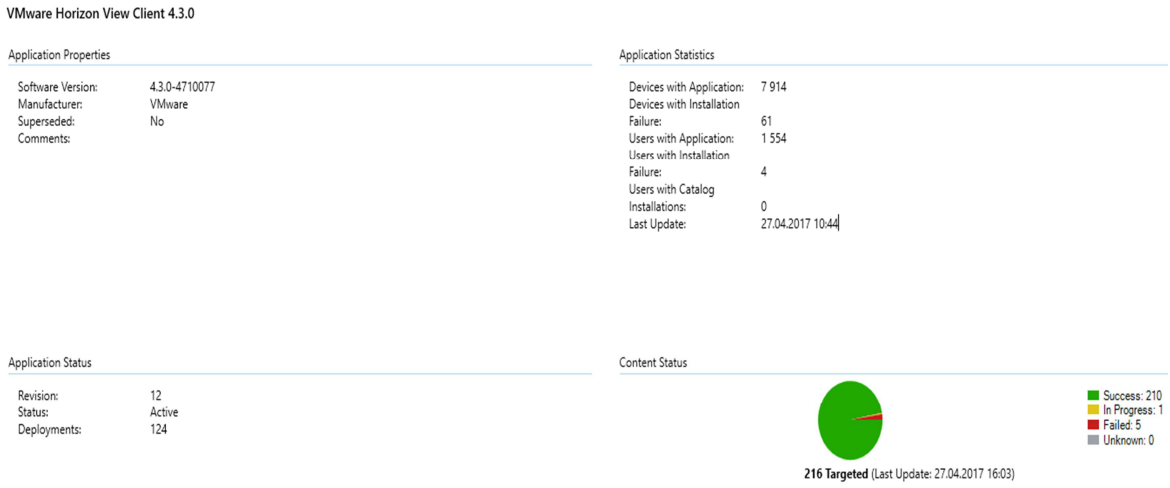
Po odhlášení a opětovném přihlášení uživatele již mámě virtuální desktop B00-VM-F-145 se stejnými vlastnostmi, ale se změnami, které jsme provedli na ploše operačního systému. Jedná se například o nakopírování složky se soubory na plochu desktopu. Vše nám dokazuje, že plovoucí desktop funguje v pořádku a skládání virtuálního desktopu ze vzorového desktopu aplikací ThinApp a uživatelského profilu se podařil. Test vyšel pozitivně a podle předpokladu výsledku.



Obr. 24, Virtuální desktop [vlastní]

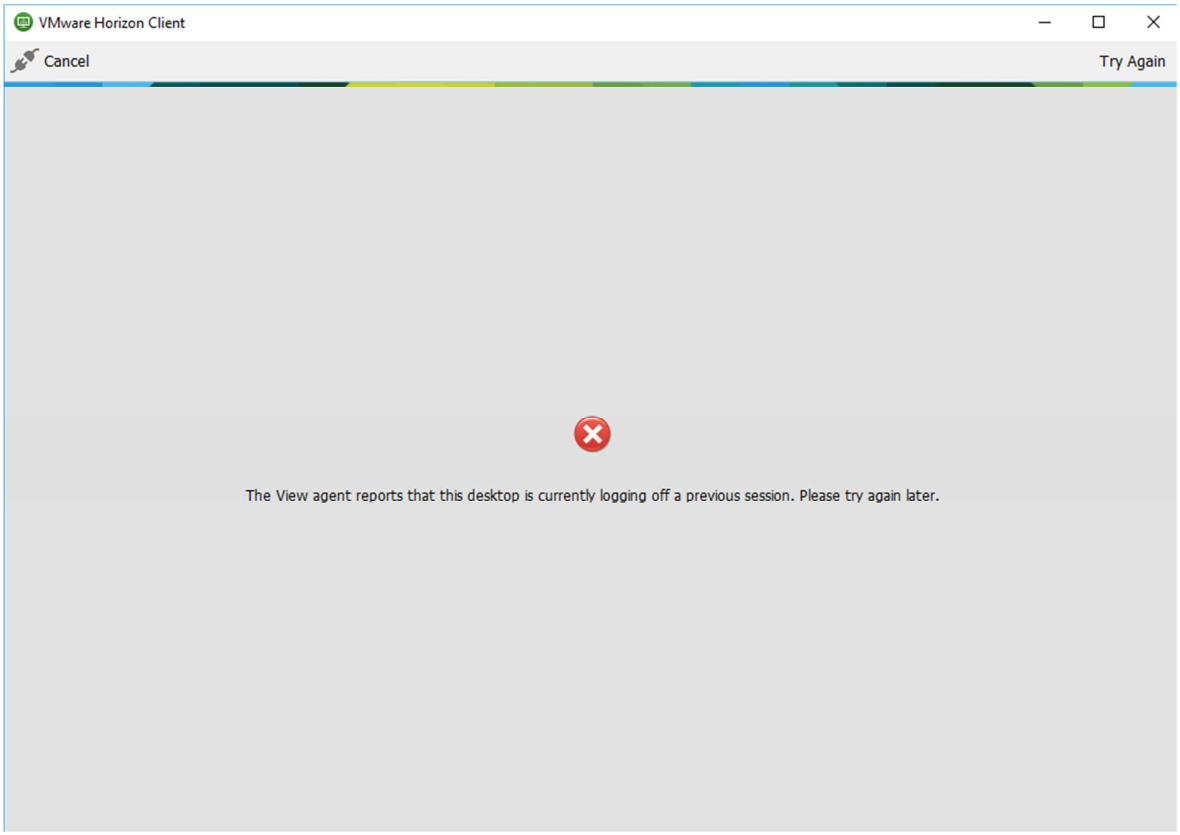
Výkon serveru a automatická instalace klienta

Výkon serveru by měl být dostatečný pro připojení 200 uživatelů, na které jsou uděleny licence. Ke dni 27.4.2017 byl klient nainstalován na 7914 desktopů v celém intranetu v oblasti Jihomoravského kraje. Uživatelů s oprávněním ke vstupu do VDI je 1554 ke stejnému výše uvedenému datu. Instalace selhala u 61 zařízení a 4 uživatelů.



Obr. 25, Statistika instalace klientů [vlastní]

Certifikace je pro 200 připojených uživatelů v jednom okamžiku. Testováním provozu bylo zjištěno, že výše uvedený server od firmy HP bez potíží zvládne do 160 připojených uživatelů. Následně při pokusu o připojení pomocí klienta dle obr. 27 oznámí klient hlášení, že se nemohl přihlásit k virtuálnímu desktopu. Stejně jako když je kapacita plně obsazena. Zátěžovým testem bylo zjištěno, že server dodaný od společnosti HP je schopen v jednom okamžiku pracovat se 160 připojenými uživateli. Tento výsledek nebyl očekáván.

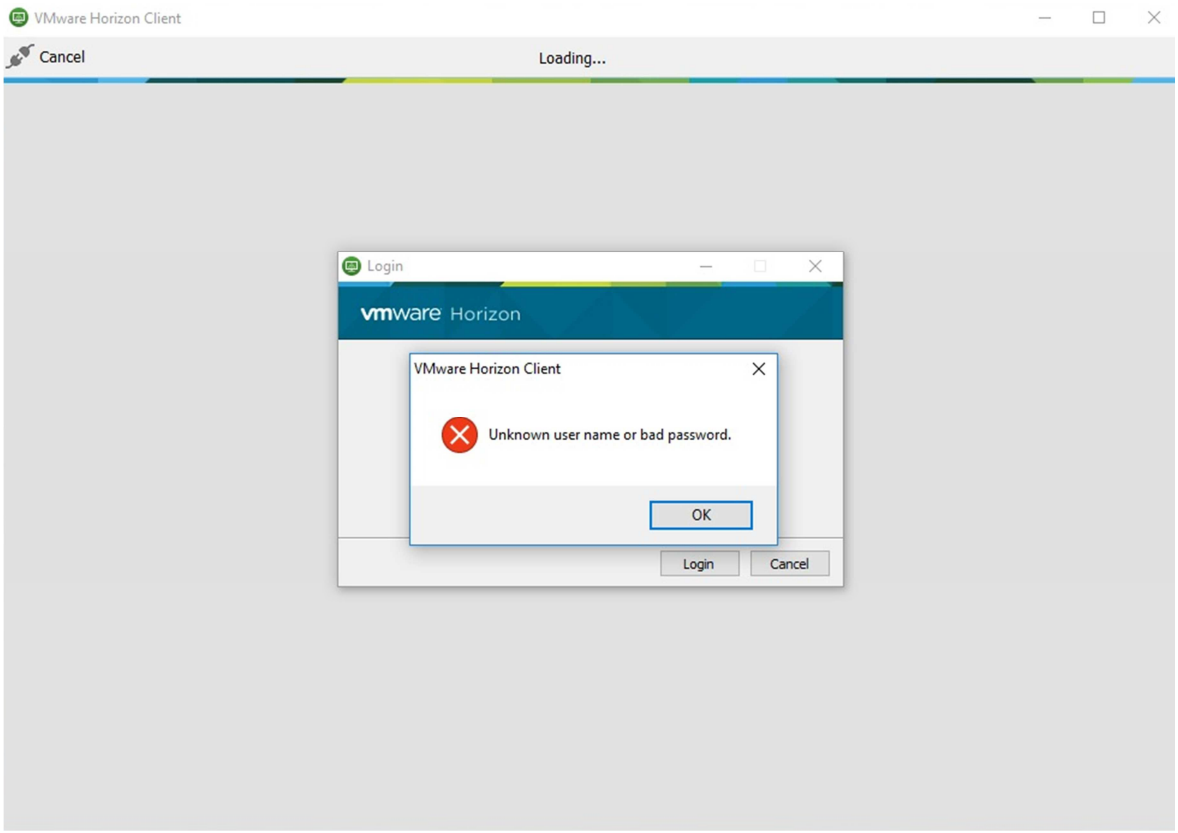


Obr. 26, Nedostupný virtuální desktop [vlastní]

Přihlášení do VDI bez udělení přístupových práv

Následně jsme v AD vytvořili uživatele uzivatele_test2, který nemá přístup do VMware Horizon, a pokusíme se přihlásit do virtuálního desktopu. Zde nastává první problém, a to že uživatel nemá nainstalovaného klienta pro přihlášení VMware Horizon Client. Tento problém lze vyřešit přihlášením pomocí webového portálu zadáním adresy b00-internet.pcr.cz. Zde si může stáhnout klienta nebo se rovnou přihlásit pomocí webového klienta. Běžný uživatel v intranetu nemá práva na instalaci softwaru, takže si klienta sám nenainstaluje. Přes webový portál se však pokusit může. V našem případě se uživatel_test2 do virtuálního desktopu přes webový portál nepřihlásil.

Může nastat situace, že se na jednom fyzickém desktopu po sobě přihlásí uživatel, který má přístup do VDI a poté uživatel, který nemá přístup. Při přihlášení prvního uživatele dojde k nainstalování klienta. Ikona toho SW se vloží do c:\Users\Public\Desktop\ a je tedy viditelná pro všechny přihlášené uživatele. V tomto případě se může pokusit uživatel pomocí klienta přihlásit do VDI. Tento pokus jsme nasimulovali a byl neúspěšný, jak je vidět na obr. č. 28.



Obr. 27, Neoprávněné přihlášení [vlastní]

Přihlášení do sítě Internet

Nyní vyzkoušíme zda-li, máme přístup z virtuálního desktopu do sítě Internet a otestujeme rychlost připojení a stabilitu. Opět se přihlásíme na uživatele uzivatele_test a pokusíme se přihlásit do sítě Internet. V našem případě se nám to podařilo. Poté otestujeme rychlost připojení. Do vyhledávače Mozilla Firefox zadáme www.rychlost.cz a spustíme test. Dozvíme se, že výsledná rychlost je 46,5Mbit/s download a 42,0 Mbit/s upload s pingem 36,0 ms. Což je výsledek v době 9:38 hodin v pracovní den s připojenými uživateli. Internetové připojení v Praze má rychlost 1 Gbit/s. Tento výsledek byl očekávaný a dopadl tedy pozitivně.

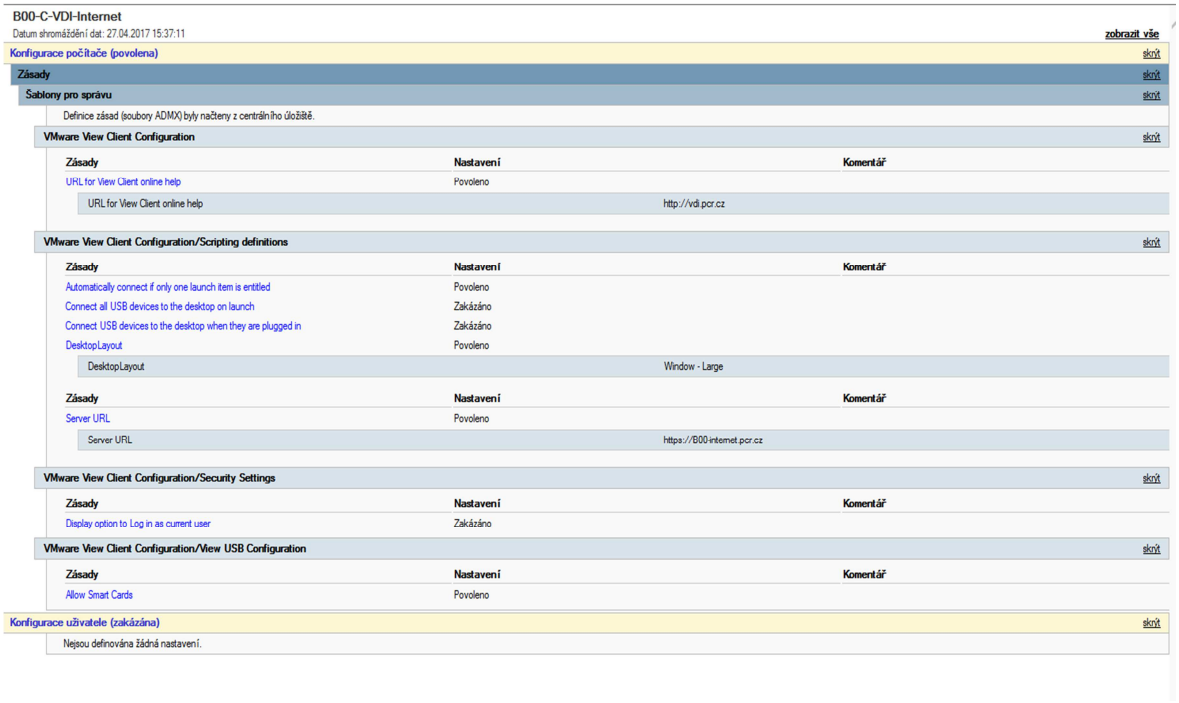
Přenosy souborů mezi sítěmi

Dále se pokusíme provést přenesení souboru mezi virtuálním desktopem a fyzickým desktopem. K čemuž slouží složka Replikace souboru, která je sdílená mezi virtuálním desktopem a fyzickým desktopem. Je vázaná na uživatele a je umístěna na diskovém poli. Celá složka je kontrolována firewallem. Složky jsou dvě, jedna je replikace souboru do intranetu a druhá je naopak. Složky pro replikace souboru jsou do fyzického desktopu vloženy při

instalaci klienta. Ve fyzickém desktopu vložíme do složky, která je replikovaná s virtuálním desktopem, soubor. Tento soubor o velikosti 5 MB se nám během 9 s objevil ve virtuálním desktopu. Výsledek splnil očekávání.

Test VMware Tools

Následně ověříme funkčnost VMware Tools a pokusíme se vytisknout libovolnou fotografii. Před tímto pokusem nahlídneme ve virtuálním desktopu do nastavení Zařízení a tiskárny, kde v sekci Tiskárny a faxy je tiskárna, která je nainstalovaná ve fyzickém desktopu. Poté jsme se pokusili vytisknout fotografii, což se nám podařilo. Ve virtuálním desktopu v horní části je položka Connect USB Device. Zde je možnost připojení USB paměťového média k virtuálnímu desktopu. Toto však našemu testovacímu uživateli je zakázáno. Vše lze ověřit v Group Policy, kde je zásada pro VDI a ve kterém je to zakázáno. Výsledek opět souhlasil s očekáváním.



Obr. 28, Group Policy [vlastní]

Pokus o spojení virtuálního desktopu s fyzickým desktopem pomocí nástroje TeamViewer

Do virtuálního desktopu jsme z webové stránky www.teamviewer.com stáhli software TeamViewer Portable ve verzi 12, což je software pro vzdálené ovládání. Následně jsme provedli pokus o spojení s jiným fyzickým desktopem ležící mimo služební intranet, na kte-

rém je také spuštěn klient TeamViewer. Spojení jsme nejprve vyzkoušeli ve směru od virtuálního desktopu do fyzického, a to pozitivním výsledkem. Následně jsme pokus provedli opačně a též se nám podařilo s virtuálním desktopem spojit. TeamViewer pro spojení využívá síťový tunel, kterým propojí oba desktopy. Využívá klíče RSA 2048, šifrování relace end-to-end AES (256 bitu) a TCP/UDP port 5938, a pokud se nespojí, využije TCP port 443, které jsou na firewallech povoleny. Propojení intranetu s Internetem nedošlo, tudíž se nejedná o prolomení bezpečnosti. Přesun souborů mezi intranetem a Internetem je replikovaný před firewall, kde dochází ke kontrole a logování. Proto spojení virtuálního desktopu s jiným fyzickým desktopem není bezpečnostní hrozbou. Administrátoři tento nástroj používají pro administraci softwaru na dálku, proto je povolen a výsledek testu se očekával.

Shrnutí testování

Tab. 8, Shrnutí testování [vlastní]

Test	Předpoklad	Reálný stav	Shoda
Přihlášení uživatele s uděleným přístupem	Přihlášení do virtuálního desktopu	Autorizovaní uživatelé se přihlašují	✓
Plovoucí desktop a ThinApp	Automatické přidělení virtuálního desktopu a stažení profilu	Virtuální desktopy se přidělují přihlašovaným uživatelům včetně profilů	✓
Výkon serveru	Výkon serveru dostačuje pro 200 uživatelů.	Server zvládá okolo 160 uživatelů.	✗
Automatická instalace klienta	Automatická instalace, dle přidělených práv	U nepatrného množství uživatelů nedošlo k instalaci	✓
Přihlášení bez udělení přístupových práv	Nepřihlášení do virtuálního desktopu	Neautorizovaní uživatelé se nepřihlásí	✓
Přihlášení do sítě Internet	Funkční Internetové připojení	Internetové připojení je uživatelům k dispozici	✓
Přenosy souborů mezi sítěmi	Sdílení složek mezi virtuálním a fyzickým desktopem	Soubory lze replikovat.	✓
Test VMware Tools	Předání ovladačů, nástrojů, periferií apod.	Virtuální desktopy mají k dispozici USB porty, periférie, tiskárny a jiné	✓
Pokus o spojení virtuálního desktopu s fyzickým desktopem pomocí nástroje TeamViewer	Spojení virtuálního desktopu a fyzického desktopu v Internetové síti a opačně.	Spojení lze uskutečnit.	✓

ZÁVĚR

Cílem této diplomové práce je především najít vhodný nástroj a metodu jak zpřístupnit síť Internet ve firemním intranetu se zajištěním vysoké ochrany celé infrastruktury intranetu. Vybrané řešení musí reflektovat skutečnost, že bude implementováno do intranetové sítě, který je součásti intranetu Ministerstva vnitra s názvem sítě Hermes. K tomuto intranetu jsou připojeny servery zpracovávající velké množství osobních i citlivých údajů a proto jsou tyto sítě odděleny a je kladen důraz na jeho zabezpečení.

V první teoretické části jsme uvedli a zhodnotili možnosti oddělení sítí, přičemž jsme kladli důraz na ochranu sítě intranet. V třetí kapitole jsme se blíže věnovali virtualizaci desktopů jako jednoho z pravděpodobných řešení pro zpřístupnění Intranetu zaměstnancům Policie České republiky.

Na začátku praktické části jsme zhodnotili současný stav. V následující kapitole praktické části jsme se zabývali výběrem nejvhodnější metody pro zjednodušení práce v síti Internet. S ohledem na komplexnost řešení a zajištění vysoké míry bezpečnosti byla vybrána architektura virtuálního desktopu jako nejvhodnější technologie pro zpřístupnění sítě Internet ve firemní síti Intranet.

V této kapitole jsme také provedli SWOT analýzu, aby navrhované řešení odpovídalo potřebám zaměstnancům a bylo vhodné pro implementaci do již vytvořené intranetové sítě. Z analýzy vyšlo najevo několik slabých stránek, na které jsme se zaměřili a navrhli opatření pro eliminaci rizika. SWOT analýza nám také pomohla se závěrečným výběrem produktu pro virtualizaci a to na produkt Horizon od společnosti VMware.

Než jsme začali s instalací jednotlivých prvků architektury virtuálního desktopu bylo potřeba tuto technologii vhodně implementovat do již vytvořené intranetové sítě. Touto implementací se zabývá šestá kapitola. V začátku kapitoly se věnujeme hardwarovým vlastnostem technických prvků, kde jsme následně provedli instalaci softwarů. Hardware serverů splňují kritéria společnosti VMware pro instalaci jejich technologií. Logické zapojení a uskutečnění systému ve firemní síti intranet je součásti další části této kapitoly. Topologie systému je upravena na technické vlastnosti intranetu a na potřeby pracovníků.

V kapitole číslo sedm se již věnujeme instalaci a základních částí systému Horizon. Instalace je uvedena postupně od základních částí jako je hypervizor až po klienta na fyzickém desktopu, kterým se do virtuálního desktopu přihlašujeme. V době psaní této diplomové

práce je celý systém stále ve zkušebním provozu. Tudíž se konfigurace mění poměrně často a stále se ladí různé nedostatky systému. Přesto již je v plném provozu a využívají jej zaměstnanci Policie ČR v celé České republice.

V následující kapitole se věnujeme bezpečnosti provozu VDI a připojení k síti Internet. Přesto, že celý systém virtualizace vykazuje vysokou ochranu proti vnitřním a vnějším hrozbám firemního intranetu, bez pečlivé konfigurace bezpečnostních prvků se můžou vyskytovat v celém systému bezpečnostní trhliny. V diplomové práci uvádíme osm základních bezpečnostních prvků, které využíváme pro zajištění bezpečnosti.

V závěru diplomové práce se věnujeme testování celého navrženého systému. Celý navržený systém funguje a nevykazuje časté poruchy. Z pozitivní stránky celého systému musíme především uvést zjednodušení a daleko komfortnější přístup k Internetu, kdy zaměstnanec nemusí přecházet k jinému počítači a vše zvládne na jednom desktopu. Naopak jako negativum musíme uvést nízký výkon serveru od firmy HP, kde byl hardware navržený pro 200 připojených uživatelů, ale z praxe se ukazuje, že server zvládá připojit přibližně 160 lidí.

Jako pracovník Policie České republiky ve služebním poměru s osmi letou zkušeností, přičemž jsem začínal jako řadový policista, velmi pozitivně hodnotím tento systém z důvodu zjednodušení hledání informací pro služební potřeby na Internetu. V současné době pracuji na pozici IT technika na Odboru informačních a komunikačních technologií a mimo jiné spolupracuji na zavádění technologie VDI. Celý systém je velmi složitý a hlavní gestor je zde Policejní prezidium. Na implementaci navíc spolupracovala externí firma. Dalším úkolem bylo školení uživatelů systémů a zpětná vazba zkušeností uživatelů.

Závěrem uvádím, že dle mého názoru byly v práci všechny body zadání splněny. Obecně jsem problematiku oddělení sítí Internetu a intranetu popsal a následně navrhl a otestoval navržené řešení. Celá infrastruktura systému je aplikovatelná i do jiných firemních intranetových sítí.

SEZNAM POUŽITÉ LITERATURY

[1] MATOUŠEK, Petr. Síťové aplikace a jejich architektura. Brno: VUTIUM, 2014. ISBN 978-80-214-3766-1.

[2] Extranet. Adaptic [online]. Praha: Adaptic, s. r. o. – tvorba webu, webdesign, 2017 [cit. 2017-05-01]. Dostupné z: https://goo.gl/JQfpfd

[3] Intranety. *Cognito* [online]. Brno: cognito.cz, 2017 [cit. 2017-05-01]. Dostupné z:goo.gl/pfgfUa

[4] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika. 2., přeprac. a aktualiz. vyd. Praha: Grada, 2009. Expert (Grada). ISBN 978-80-247-2615-1.

[5] Bezpečnost provozu intranetu. *System Online* [online]. Brno: CCB, spol., 2003 [cit. 2017-05-01]. Dostupné z: https://goo.gl/NGZKiQ

[6] Recommended Deployment Configurations. *Oracle* [online]. Redwood Shores: Oracle Corporation, 2016 [cit. 2017-05-01]. Dostupné z: https://goo.gl/m7rikI

[7] Zákon č. 273/2008 Sb., o Policii České republiky. In: . Česká republika: Parlament České republiky, 2008, ročník 2008, číslo 273. Dostupné také z: goo.gl/veI5k4

[8] JANDEČKA, Aleš. *Informační systémy Policie České republiky* [online]. Ústav informačních studií a knihovnictví, U Kříže 8, 158 00 Praha 5-Jinonice-Praha 5, 2009 [cit. 2017-05-01]. Dostupné z: https://goo.gl/1WgOx6. Diplomová práce.

[9] Největší hrozby pro digitální firmy v roce 2016? *Hospodářské noviny* [online]. Praha: Economia, 2016 [cit. 2017-05-01]. Dostupné z: https://goo.gl/Fo9wJJ

[10] KYBERNETICKÉ ÚTOKY. *CESNET-CERTS* [online]. Praha: CESNET, z. s. p. o., 2016 [cit. 2017-05-01]. Dostupné z: https://goo.gl/lemBU2

[11] E-mailový červ. *Správa sítě* [online]. Praha: Aira GROUP, 2016 [cit. 2017-05-01]. Dostupné z: https://goo.gl/AEVBF2

[12] Automatičtí červi útočí. *PC World* [online]. Praha: IDG Czech Republic, 2016 [cit. 2017-05-01]. Dostupné z: https://goo.gl/7gdhNz

[13] Spam. *Bezpečný internet* [online]. Praha: Bezpečný internet, 2016 [cit. 2017-05-01]. Dostupné z: https://goo.gl/ml5LyW

[14] Typy detekovaných síťových útoků. *Bezpečný internet* [online]. Budapest: HelpMax Software Help & Shop, 2011 [cit. 2017-05-01]. Dostupné z: https://goo.gl/rYNaui

[15] Jak se dělá phishing. *Lupa.cz* [online]. Praha: Internet Info, 2008 [cit. 2017-05-01]. Dostupné z: https://goo.gl/F8tQCE

[16] Počítačový virus. *ManagementMania.com* [online]. Wilmington, New Castle County Delaware: MANAGEMENTMANIA.COM, 2016 [cit. 2017-05-01]. Dostupné z: https://goo.gl/f0jsSB

[17] Jak zjistím, že mám v počítači vir nebo jiný škodlivý software? *Eset* [online]. Praha: ESET, spol. s r.o, 2017 [cit. 2017-05-01]. Dostupné z: https://goo.gl/l5dU6N

[18] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[19] Plná moc pro vaše připojení -- proxy server. *Smart World* [online]. Praha: IDG Czech Republic, 2000 [cit. 2017-05-02]. Dostupné z: https://goo.gl/dHk8j5

[20] PROSISE, Chris a Kevin MANDIA. *Počítačový útok: detekce, obrana a okamžitá náprava*. Praha: Computer Press, 2002. Komunikace a sítě. ISBN 8072266829.

[21] TCP Wrappers and xinetd. *CentOS* [online]. Raleigh, USA: Red Hat, 2017 [cit. 2017-05-02]. Dostupné z: https://goo.gl/Ufwq35

[22] Firewall Evolution. *Symantec* [online]. USA: Symantec Corporation, 2017 [cit. 2017-05-02]. Dostupné z: https://goo.gl/N8A8sJ

[23] BURIAN, Pavel. *Internet inteligentních aktivit*. Praha: Grada, 2014. Průvodce (Grada). ISBN 978-80-247-5137-5.

[24] VPDN Technology Overview. *VPDN Configuration Guide* [online]. San Jose: Cisco Systems, 2015 [cit. 2017-05-02]. Dostupné z: https://goo.gl/5jGy3G

[25] Jak (a proč) nastavit VPN ještě dnes. *PC World* [online]. Praha: IDG Czech Republic, 2015 [cit. 2017-05-02]. Dostupné z: https://goo.gl/pQejd4

[26] Různé typy VPN sítí a kdy je použít. *VPN Mentor* [online]. Arizona, USA: VPN Mentor, 2017 [cit. 2017-05-02]. Dostupné z: https://goo.gl/NKHZpG

[27] RUEST, Danielle a Nelson RUEST. *Virtualizace: podrobný průvodce*. Brno: Computer Press, 2010. ISBN 978-80-251-2676-9

[28] Úvod do virtualizace na desktopu. *Michal Zobec: Virtuální PC Blog // ZOBEC Consulting* [online]. Brno: Michal Zobec, Lightning Group Company, 2017 [cit. 2017-05-02]. Dostupné z: https://goo.gl/aD7TMF

[29] LOWE, Scott. *Mistrovství ve VMware vSphere 5: kompletní průvodce profesionální virtualizací*. Brno: Computer Press, 2013. Mistrovství. ISBN 978-80-251-3774-1

[30] Horizon 7. *VMware* [online]. Kalifornie, USA: VMware, 2017 [cit. 2017-05-02]. Dostupné z: https://goo.gl/YfDk5C

[31] VMware Horizon 6 with View: Performance Testing. *VMware EUC BLOG* [online]. Kalifornie, USA: VMware, 2017 [cit. 2017-05-02]. Dostupné z: https://goo.gl/dXOfap

[32] XenApp a XenDesktop. *Citrix* [online]. Fort Lauderdale, USA: Citrix Systems, 2017 [cit. 2017-05-02]. Dostupné z: https://goo.gl/Xkr6vW

[33] Citrix XenDesktop 7. *Ervik a.s.* [online]. Norsko: Alexander Ervik Johnsen, 2017 [cit. 2017-05-02]. Dostupné z: https://goo.gl/FWWPbJ

[34] Microsoft Hyper-V. *Microsoft TechNet* [online]. Washington, USA: Microsoft Corporation, 2017 [cit. 2017-05-02]. Dostupné z: https://goo.gl/ioP3lm

[35] Barracuda NextGen Control Center VC400. *Barraguard.com* [online]. Irvine, USA: Virtual Graffiti Inc, a Diamond Barracuda Networks reseller., 2017 [cit. 2017-05-06]. Dostupné z: https://goo.gl/39Pwjv

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

TCP	Transmission Control Protocol
IP	Internet Protocol
UDP	User Datagram Protocol
WWW	World Wide Web
HTTP/S	HyperText Transfer Protocol – Secure
FTP/S	File Transfer Protocol – secure
SMTP	Simple Mail Transfer Protocol
RFC	Request For Comment
LAN	Local Area Network
PČR	Policie ČR
HTML	HyperText Markup Language
DOS	Disc Operating Systém
SSL	Secure Sockets Layer
MS	MicroSoft
HW	HardWare
PC	Personal Computer
POP	Post Office Protocol
ISO/OSI	lnternational Organization for Standardization/ Open Systems Interconnection
L2P	Layer2 Forwarding
PPP	Point-to-Point Protocol
VPN	Virtual Private Network
WIFI	Wireless Fidelity
PCoIP	PC over IP
RDP	Remote Data Processing

ICA	Independent Computing Architekture
SAN	Storage Area Network
VDI	Virtual Device Interface
AD	Active Directory
RSA	Rivest -Shamir –Adleman
HDX	Half DupleX
WMI	Windows Management Instrumentation
MV	Ministerstvo vnitra
VLAN	Virtual Local Area Network
SWOT	Strengths, Weaknesses, Opportunities, Threats analýza
IT	Information Technology
CPU	Central Processing Unit
IPS	Intrusion Prevention Systém
DHCP	Dynamic Host Configuration Protocol
DMZ	demilitarized zone
SQL	Structured Query Language
OBDC	Open Database Connectivity

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ