Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Virtualizace a kybernetická bezpečnost

Maximilian Chilcenco

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Maximilian Chilcenco

Systémové inženýrství a informatika
Informatika

Název práce

Virtualizace a kybernetická bezpečnost

Název anglicky

Virtualization and Cyber Security

Cíle práce

Bakalářské práce je tematicky zaměřena na užití virtualizace z pohledu kybernetické bezpečnosti. Hlavním cílem je uvést a zhodnotit samotné výhody virtualizace, dále demonstrovat realizaci pomocí virtualizačního nástroje VMware.

Dílčí cíle:

- Definice pojmu virtualizace
- Představení hlavních platforem pro virtualizaci (VMware, HyperV)
- Kybernetická bezpečnost
- Správa a konfigurace virtuálního stroje
- Závěry a doporučení

Metodika

Při zpracování teoretické části bude vycházeno z odborné literatury, internetových zdrojů a vlastních zkušeností autora. Za pomocí analýzy, syntézy a studiu dané problematiky.

V praktické časti bude realizován vlastní návrh řešení, který bude danou problematiku demonstrovat. Následuje vytvoření virtuálního stroje a jeho konfigurace při použití softwaru VMware. Samotné vyhodnocení teoretické a praktické části řešení problematiky bakalářské práce je shrnuto v závěru a doporučení.

Doporučený rozsah práce

40 – 50 stran

Klíčová slova

Virtualizace, Kybernetická bezpečnost, VMware, Hyper-V, konfigurace, Windows server

---

Doporučené zdroje informací

RUEST, D., RUEST, N. Virtualizace: Podrobný průvodce. 1. vyd. Brno: Computer Pres, a.s., 2010. 408 s. ISBN 978-80-251-2676-9

SCOTT, L., Mistrovství ve VMware vSphere 5: Kompletní průvodce profesionální virtualizací. Brno: Computer Press, 2013, 1. vydání, 728 s. ISBN: 978-80-251-3774-1

Singer, P. W. Cybersecurity and cyberwar: what everyone need to know. Oxfor; New York: Oxford University Press, 2014. ISBN 978-0-19-991809-6

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 27. 8. 2020

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 08. 03. 2021

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci Virtualizace a kybernetická bezpečnost jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15. 03. 2021 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D., za odborné připomínky a rady při vedení bakalářské práce. Zároveň bych rád poděkoval Ministerstvu spravedlnosti České republiky, které mi poskytlo materiály a potřebné zdroje k vypracování této práce.

Virtualizace a kybernetická bezpečnost

Abstrakt

Hlavním předmětem bakalářské práce je představit a následně demonstrovat virtualizační technologii z pohledu kybernetické bezpečnosti. V bakalářské práci je obsažen nejen základní princip fungování této technologie, ale i její klasifikace, popis samotného fungování, představení a uvedení hypervizorů a následné demonstrování realizace ve vybraném virtualizačním nástroji. Díky provedené cenové kalkulaci bylo dosaženo klíčového aspektu při rozhodování, zdali se vyplatí tuto technologii provozovat, či zůstat u fyzické varianty.

Klíčová slova: Virtualizace, kybernetická bezpečnost, VMware, Hyper-V, konfigurace, Windows server, Microsoft

Virtualization and Cyber Security

Abstract

The main subject of the thesis is to introduce and demonstrate virtualization technology from the perspective of the cyber security. Thesis also contains the basic principle of its operation functionality, detail description, introduction hypervisors and subsequent demonstration of implementation in a selected virtualization tool. There is a price calculation, which will be the main aspect in deciding whether it is worth operating in this technology or if we should use the physical variant.

Keywords: Virtualization, cyber security, VMware, Hyper-V, configuration, Windows server, Microsoft

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

Technologický progres se v IT neustále posunuje kupředu. Hlavním trendem jsou decentralizované a bezdrátové technologie. Zvyšují se nároky na dostupnost a spolehlivost služeb. Firmy se neustále snaží minimalizovat svoje náklady. Jedním z hlavních východisek může být zavedení a efektivní využívání virtualizačních technologií.

Virtualizace jako taková není pro nás vcelku nová technologie, jak se na první pohled může zdát. Její počátky sahají již od 60. let minulého století.

V dnešní době můžeme virtualizovat skoro všechno. Od serverové virtualizace, přes virtualizaci stolních počítačů a aplikací až po datové uložiště. Tato bakalářská práce pojednává o virtualizaci na úrovni serveru. Dnes využívané platformy pro virtualizaci jsou například VMware, Microsoft Hyper-V a XenServer. V praktické části budeme využívat virtualizační nástroj VMware. Získané poznatky mohou posloužit jako rozhodovací kritérium při volbě správného hypervizoru a také k plnému porozumění a použití virtualizační technologie.

O tuto eskalující technologii jeví zájem převážně malé a střední podniky, ve snaze snížit náklady na provoz, optimalizovat výpočetní kapacitu, lépe rozvrhnout zátěž a spravovat fyzické či virtuální servery.

V bakalářské práci budou shrnuty teoretické poznatky, samotná aplikace, realizace a konfigurace vybraného hypervizoru. Prostředí, ve kterém se vše bude odehrávat si, jakožto autor práce zvolil kybernetickou bezpečnost. Bakalářská práce nastíní využití virtualizačních technologií z pohledu kybernetické bezpečnosti.

2. Cíl práce a metodika

2.1. Cíl práce

Bakalářské práce je tematicky zaměřena na užití virtualizace z pohledu kybernetické bezpečnosti. Hlavním cílem je uvést a zhodnotit samotné výhody virtualizace, dále demonstrovat realizaci pomocí virtualizačního nástroje VMware.

Dílčí cíle:

- Definice pojmu virtualizace
- Představení hlavních platforem pro virtualizaci (VMware, HyperV)
- Kybernetická bezpečnost
- Správa a konfigurace virtuálního stroje
- Závěry a doporučení

2.2. Metodika

Při zpracování teoretické části bude vycházeno z odborné literatury, internetových zdrojů a vlastních zkušeností autora. Za pomocí analýzy, syntézy a studiu dané problematiky.

V praktické časti, bude realizován vlastní návrh řešení, který bude danou problematiku demonstrovat. Následuje vytvoření virtuálního stroje a jeho konfigurace při použití softwaru VMware. Samotné vyhodnocení teoretické a praktické části řešení problematiky bakalářské práce je shrnuto v závěru a doporučení.

3. Teoretická východiska

3.1. Virtualizace

Virtualizace je technologie dnešní doby, se kterou se informatici denně setkávají při své činnosti. Schopnost virtualizovat nám umožnuje vytvářet několik virtuálních výpočetních prostředí na jedné fyzické jednotce. To znamená, že v reálném čase může fungovat více virtuálních strojů na jednom fyzickém počítači či serveru. Přičemž tyto virtuální jednotky na sobě pracují nezávislé, dokonce mohou mít i odlišné operační systémy. (1)

Jediné omezení, ke kterému zde dochází, je sdílení fyzického výkonu hostitelské jednotky. Virtuální stroje si mezi sebou rozdělují jak operační paměť, tak i procesor a uložiště. V dnešní době jsme schopni virtualizovat již samotné počítače, ale i jejich hardwarové i softwarové součásti. Jedním z hlavních důvodu, proč virtualizujeme je vysoká dostupnost služeb, které provozujeme. Máme nepřetržitý přístup k hardwarovým prostředkům nehledě na jejích aktuální polohu. Jako druhým hlavním důvodem jsou ušetřené náklady na provoz těchto fyzických jednotek, kdy se ušetří peníze za provoz, chlazení, zabezpečení a údržbu. (1)(2)

Nyní je celková správa vnitropodnikové infrastruktury o hodně lehčí a přehlednější. Jakožto firma nemusíme kupovat tolik fyzických jednotek ale využívat dostupné zdroje na 100 %. Veškeré nové změny, které bude firma implementovat, se dají lehce a s přehledem řídit. Pomocí virtualizace si podnik může vytvořit simulační prostředí, kde dané řešení nejdříve otestuje a dále plošně implementuje. (1)(6)

Celkově virtualizace je pro dnešní podniky nesmírně důležitá. Firmy nyní mohou bezproblémově zálohovat jak svoje data, tak i celé virtuální jednotky. Pokud by došlo k výpadku nebo poškození této virtuální stanice, lze jí bezztrátově zkopírovat nebo nahradit za jinou, bez jakéhokoliv nutnosti fyzického zasahování. To všechno lze provádět v reálném čase, kdy uživatel nemusí nepocítit žádné změny nebo výpadky a tím lze dosáhnout plynulého běhu celé infrastruktury. (1)(3)

Toto byl hrubý náhled na pojem virtualizace. V dalších částech bakalářské práce si určitě podkapitoly rozeberme dopodrobna. Uvedeme další výhody a nevýhody této technologie, proč bychom jí měli provozovat a jaké další druhy virtualizace ještě existují.

V samotné praktické části bude demonstrováno, jak takový virtuální stroj vytvořit, co k tomu je zapotřebí, samotná konfigurace a následně správa v denním provozu a užívání.

3.1.1. Hypervizor

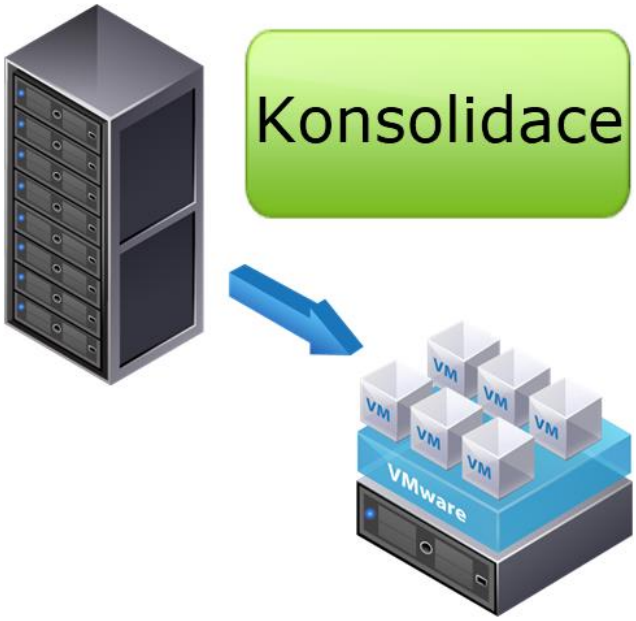
Jedná se o primární a nejdůležitější prvek při vytváření virtualizace. Hypervizor odděluje fyzický hardware od toho virtuálního a tím vytváří vlastní virtualizační vrstvu, na které pak působí. Jedná se o software, který zprostředkovává zdroje mezi hostitelským a virtuálním strojem. Následně navazuje a zajišťuje komunikaci mezi fyzickým

či virtuálním hardwarem. Od hypervizoru záleží celková rychlost a stabilita celé virtuální jednotky. [1][2]

3.1.2. Konsolidace

Hlavní myšlenkou a cílem konsolidace je přesunout fyzické stroje do virtuálního prostředí. Jedná se o první krok při zavádění virtualizace do vnitropodnikové infrastruktury. Bývá již dlouhým trendem a pomalu se i stává pravidlem na jednom stroji provozovat jednu službu. To z důvodu bezpečnosti a plynulého chodu. Ve většině případech stroj poskytující nějakou službu je maximálně vytěžován na 35 %. Zbylý výkon se nevyužije, nebo slouží jako rezerva, pokud by nastaly komplikace či změna zátěže.

Při vytváření konsolidace je dobré si rozmyslet a dále rozumně rozprostřít virtuální jednotky tak, aby docházelo k rovnoměrné zátěži. Například nedávat hodně složitých a náročných služeb na jeden fyzické stroj, ale rozházet podle možností. Tím nám konsolidace poskytne rovnoměrné zatížení fyzických strojů a lepší přehled o celkové zátěži. Na to se také váže servis a výměna hardwaru za běhu systémů, bez nutnosti jejich vypínání. Z ekonomické stránky nám konsolidace šetří náklady za nákup nových fyzických strojů a dále i jejich udržování (energie, chlazení, servis). [1][3][4]



Obrázek 1 - Konsolidace serverů
Zdroj: http://www.oldanygroup.cz/virtualizace-vmware-zakladni-informace-9

3.1.3. Historie virtualizace

Počátky virtualizace sahají do 60. let minulého století. Tato technologie umožnovala vylepšeného užití výpočetních prostředků u tehdejších sálových počítačů. Osobní počítače tehdy dosahovaly astronomických částek a jejích výkon nebyl zcela dostačující. Hlavní přelom nastává, kdy se tyto sálové počítače začínají rapidně rozšiřovat a tím klesá i jejich pořizovací cena. Nastávají zde ale problémy, jako například provozní náklady za elektřinu a chlazení serverů. IT technici si tuto realitu začínají postupem času uvědomovat a hledají alternativní řešení. [8]

Jako první s virtualizací přichází firma IBM, která v 60. letech představuje hardwarovou virtualizaci na úrovni procesoru. Důvodem bylo zvýšení výkonu pro jejich tehdejší sálové počítače CP – 40. Další etapu progresu virtualizace zde máme již zmíněný masivní nárust výpočetní technologie a to za účelem lepší konsolidace a úspornější využívání fyzických serverů. S tím je i úzce spjata idea ušetření nákladů při provozu. (8)

V roce 1998 vzniká firma VMware, která později v roce 1999 přináší svůj produkt VMware Virtual Platform 1.0 (dnes označován jako VMware Workstation). Později na přelomu roku 2001 uvádí na trh produkt VMware ESX, který má sloužit k virtualizaci serverového prostředí. Přesně o dva roky později přichází s řešením vMotion, které zajišťovalo plynulou migraci v reálném čase bez nutnosti fyzického zasahování a nutnosti vypínání serverů. (8)

Současně v této době vzniká i konkurenční firma Citrix s jejím produktem XEN, avšak jejich technologie nebyly zdaleka tak dostačující a výkonné jako VMware. Postupem času, si výrobci procesorů začínají uvědomovat, jak je virtualizace podstatná i pro jejich produkty. Začínají tedy implementovat podporu pro virtualizační technologie do procesorů Intel a AMD. Díky tomuto kroku se virtualizace začíná rozšiřovat i mezi střední a malé podniky. (8)

V roce 2007 přichází na trh KVM (Kernel Virtual Machine). Jedná se o řešení, které funguje na operačním systému Linux. Jedná se ale o opensource[1] řešení, kdy kvality prozatím nedosahovaly konkurence, ale díky své formě jsou neustále vyvíjeny. Nakonec zde máme velkého hráče, který přichází v roce 2008. Jedná se o firmu Microsoft a hodlá konkurovat stávajícím firmám VMware a Citrix. Svůj produkt pojmenoval jako Microsoft Hyper-V. (8)(9)

3.1.4. Typy virtualizace

Kvůli novým a neustále přibývajícím potřebám uživatelů, základní myšlenka virtualizace nepokryla veškeré tyto požadavky. Bylo nutné jí tedy rozvíjet dále a rozdělit do potřebných subkategorií, kdy určité typy virtualizace slouží k jednotnému účelu a řeší danou problematiku. (5)

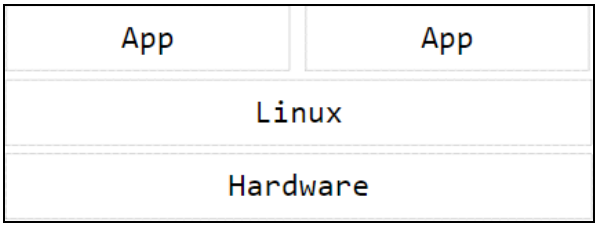
3.1.4.1. Kontejnerová virtualizace

Kontejnerová virtualizace funguje na úrovni operačního systému. V jednom operačním sytému (hostitelském) se vytváří samostatné kontejnery, které jsou od sebe nezávislé a oddělené. Toto řešení nám umožnuje poskytovat několik různých služeb na jednom stroji s rozdílnými operačními systémy.

Výhoda tohoto řešení je menší technická náročnost a nevytěžování prostředků. Na druhou stranu se však nejedná o opravdovou virtualizaci, jádro zůstává stejné a oddělení je jen „imaginární“.

[1] Program, jehož zdrojový kód byl poskytnut dalším vývojářům, kteří jej mohou studovat a upravovat.

Ukázkovým příkladem je aplikace Docker. Zabaluje jednotlivé aplikace včetně jejich nastavení do kontejnerů. Tyto kontejnery lze pak jednoduše přenášet mezi stroji a nasazovat rovnou s předefinovaným nastavením. (7)

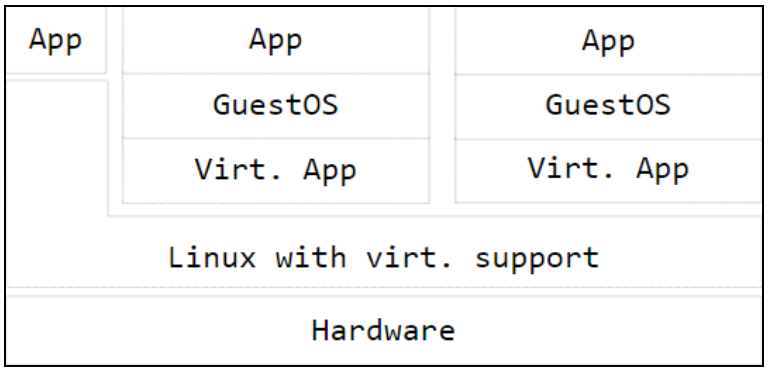


Obrázek 2 - Princip fungování kontejnerové virtualizace
Zdroj: https://www.fi.muni.cz/~kas/pv090/referaty/2016-podzim/virt.html#cast2

3.1.4.2. Paravirtualizace

Paravirtualizace působí jen na úrovni virtuálního počítače a poskytuje prostředí podobné tomu fyzickému, na kterém právě běží. S tímto typem virtualizace se můžeme setkat jedině, když komponenty fyzického a virtuálního stroje budou shodné (hardware hostitelského počítače). Hostovaný systém, o sobě ví, že funguje ve virtuálním prostředí. Komunikuje s hypervizorem, který mu přiděluje zdroje a výkon HW dle potřeby. Aby tato komunikace probíhala efektivně, je zapotřebí mít upravené jádro hostitelského systému. Toto řešení však nelze použít ve všech případech. Některé operační systémy mají uzavřené zdrojové kódy a to celou situaci výrazně komplikuje. Částečného řešení lze dosáhnout za použití speciálních ovladačů.

Výhodou tohoto typu virtualizace je vysoký výkon, kdy výpočty probíhají na skutečných komponentech. Hlavním nedostatkem tohoto řešení je nutnost instalování ovladačů na hostitelský stroj a případnou úpravu operačního systému. Tento typ virtualizace využívají hypevizoři VMware, Virtualbox, XenServer a další. (7)



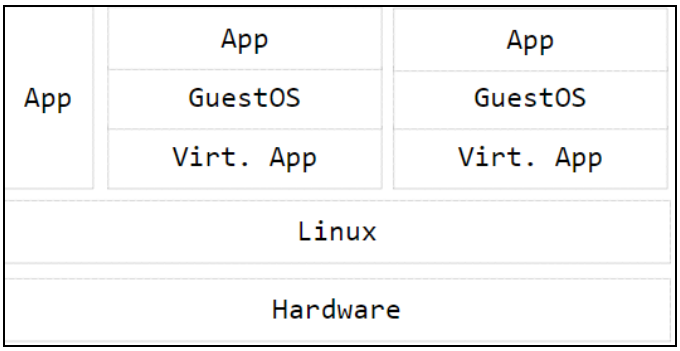
Obrázek 3 - Princip fungování paravirtualizace
Zdroj: https://www.fi.muni.cz/~kas/pv090/referaty/2016-podzim/virt.html#cast2

3.1.4.3. Emulace

Emulace jako jediná, z předešlých uvedených typů virtualizace umožnuje provozovat virtuální stroj odlišené architektury na hostujícím systémů. Všechny operace jsou převáděny do patřičné nebo odlišné formy a to zapříčiňuje snížení výkonu. Proto se emulace výrazně liší od ostatních virtualizačních technik a využívá se jen v určitých případech.

Samotná interpretace příkazů může být prováděná ze statických ale i dynamických překladů. Při provádění interpretace, emulátor prochází zdrojový kód programu instrukci za instrukcí a na základě toho mění aktuální stav hostovaného systému. Každou instrukci nejdříve načte, dekóduje a zavolá na základě toho odpovídající operaci. Statický překlad celý program načte a rovnou i provede. Nedochází k žádným dodatečným úpravám. Kdyžto dynamický překlad se provádí až za běhu programu. Postupně načítá bloky instrukcí a ty rovnou provádí. Na rozdíl od nativního typu prostředí je toto řešení virtualizace velmi zpomalené a to 2-3 násobně.

Hlavní a jedinou výhodou je schopnost provozovat tento typ virtualizace na libovolné platformě, kdy systém může obsahovat odlišnou architekturu. Hlavním nedostatkem je zmíněný výkon emulovaného systému, kdy se musí jednotlivé instrukce a procesy převádět. Ideálním příkladem je software QEMU. (7)



Obrázek 4 - Princip fungování emulace

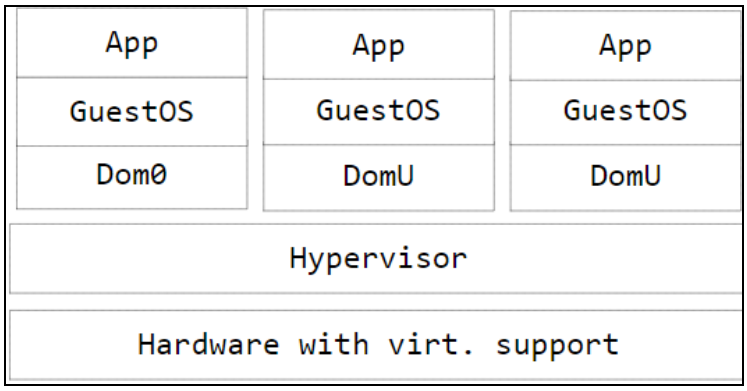
Zdroj: https://www.fi.muni.cz/~kas/pv090/referaty/2016-podzim/virt.html#cast2

3.1.4.4. Plná virtualizace (nativní)

Pokud dochází k virtualizaci všech součástí počítače, lze hovořit o virtualizaci plné, také nazývané jako nativní. Hostitelský i hostovaný počítač musí disponovat stejnou architekturou. Díky tomu může dojít k vytvoření identického obrazu fyzické architektury a tím hostovaný systém dosahuje identické instrukční sady. Díky tomuto postupu se virtuální stroj tváří jako fyzický a ani on sám neví, že funguje ve virtuálním prostředí.

I když se toto řešení zdá jako bezchybné a ideální, nemusí tomu tak být ve všech případech. Je nutno rozeznávat kdy a v jakém případě použít správný typ virtualizace. Plná virtualizace odděluje fyzickou vrstvu od té programové a díky tomu dochází ke snížení výpočetní výkonu. Hypervizor emuluje fyzické vybavení stroje a výpočty provádí ve svém softwarovém prostředí, namísto toho, aby výpočty byly prováděný na hardwaru.

Hlavní a jedinou výhodou tohoto typu virtualizace je jednotný a neupravený operační systém. Nevýhoda, již zmíněná emulace, která výrazně zatěžuje výpočetní výkon stroje. Je tedy dobré si rozmyslet, jaký typ virtualizace použijeme a zdali se nerozhodneme raději pro paravirtualizaci. Ukázkovým příkladem jsou hypervizory KVM, VMware ESX Server a XEN. (7)



Obrázek 5 - Princip fungování plné virtualizace

Zdroj: https://www.fi.muni.cz/~kas/pv090/referaty/2016-podzim/virt.html#cast2

3.1.4.5. Kernel-based Virtual Machine (KVM)

Jedná se o nástroj umožňující plnou virtualizaci. Je součástí linuxového jádra a je kompatibilní s x86 architekturou, podporuje tedy procesory jako Intel a AMD. Samotná koncepce fungování KVM je založena na přeměně linuxového jádra do virtuální vrstvy a dále vložení modulu do jádra. Díky tomu má každý virtuální stroj svoje virtuální HW vybavení (síťová karta, hard disk atd.). Hlavní podmínkou uskutečnění této virtualizace je aby procesor zvládal a podporoval HW virtualizaci, bez této schopnosti nelze KVM využít. Princip fungování lze přirovnat, ke zmíněnému emulátoru QEMU. Hypervizor zachycuje a následně emuluje veškeré dotazy hostujícího operačního systému, tím pádem můžeme říct, že se zde nachází i některé QEMU moduly a zároveň jsou součástí linuxového jádra. (6)(7)

3.1.5. Důvody virtualizovaní

Již od roku 1999 se jedná o velmi rychle expandující službu, o kterou je veliký zájem. V dnešní době se spíš setkáváme s virtualizací serverů než softwarovou či desktopů. To vše díky špatnému řešení v oblasti licenčních politik. Kdy je opravdu těžké a nákladné udržovat své produkty zalicensované a hlavně kvůli nedostačující podpory ze strany dodavatelů softwaru. (11)

Při otázce, proč vlastně tedy virtualizovat, dostaneme skoro vždy jednu a tu samou odpověď. Konsolidace serverů. Konsolidace serverů je v dnešní době jedna z primárních a klíčových záležitostí, kterou musí informatici neustále řešit. To vše díky novým, náročnějším požadavkům uživatelů na nové služby, nákladům na provoz, nevyužitých výpočetních kapacit a mnoho dalších aspektů. Vše se v posledních letech zlepšuje díky cloud computingu, kdy pomocí této technologie konsolidace datových center nabírá nový směr. Jaké jsou tedy důvody a výhody virtualizace? (10)

3.1.5.1. Technologické přínosy virtualizace

Spolehlivost a vysoká dostupnost - Virtualizace nabízí neustálý provoz služeb a aplikací, ke kterým uživatelé potřebují nepřetržitě přistupovat. Tato technologie umožnuje přesouvat virtuální servery mezi fyzickými, bez nutnosti jejich vypínání či jakékoliv manipulace s fyzickými prvky. K tomu dochází nejčastěji při údržbě hardwarových částí. Díky dnešním hypervizorům máme neustálý přehled a statistické údaje o zátěži. Umožnují nám

nastavit zautomatizovaná pravidla o přesouvání virtuálních prvků mezi fyzickými clustery na základě aktuální zátěže. (7)(10)

Zálohování dat - Virtualizační prostředí jako například VMware nebo Hyper-V umožnují funkci snapshot. Při pořízení takzvaně „snapshotu“ hypervizor zaznamená veškerá data na pevném disku, běžící aplikace či aktuální nastavení v daném okamžiku. Při jakékoliv ztrátě dat nebo komplikacím administrátor virtuálního stroje nahraje daný snapshot na server, následně se virtuální jednotka vrátí do bodu, kdy byl daný snapshot pořízen. (7)(11)

Úspora nákladů - Jeden z hlavních důvodu virtualizace je zmíněná konsolidace serverů. Konsolidace nám umožnuje seskupit více virtuálních jednotek na jeden fyzický stroj a díky tomu firma nemusí vynakládat takové finance za energie, chlazení a prostory. (7)

Migrace - Migrace virtuální jednotky mezi fyzickými servery, bez nutnosti restartu či přerušení běžících služeb. (7)(10)

Bezpečnost - Pro každou službu můžeme vytvořit virtuální jednotku. Například budeme mít jiný virtuální stroj pro databázi a Exchange[2]. Každému virtuálnímu stroji nastavíme oprávnění, aby k němu měl, přistup autorizovaný uživatel. V praxi bez využití virtualizace bychom musel každý fyzický server zabezpečit v serverovně či jinými fyzickými prostředky. (7)(11)

Testovací jednotky - Virtuální stroje můžeme v rozhraní hypervizorů vypínat, restartovat či jakkoliv odstavovat podle potřeb. Tato vymoženost nám nabízí ideální podmínky pro testování či provádění změn ve vnitropodnikové infrastruktuře. IT administrátor nasadí nové technologie či služby na virtuální testovací jednotku a pozoruje, zdali řešení plní daná očekávání. (7)(11)

Ekologické hledisko - Na jednom fyzickém serveru lze podle průzkumu spustit 8 aktivních virtuálních jednotek. Samozřejmě údaje se můžou lišit dle hardwarových specifikací fyzického serveru. Hlavní problém ale nastává při vydávání tepla. Vezmeme v potaz tedy, že bez použití virtualizace bychom měli zapnutých 8 fyzických strojů, které by aktivně vydávaly teplo. Pokud se jedná o malé, soukromé firmy tak si řekneme, že to není až tak hrozné. Nesmíme ovšem zapomínat na světové korporace jako například Google a jiná datacentra kdy těchto fyzický jednotek tam může být stovky až tisíce. Planetu máme jen jednu. (11)

Řízení výpočetního výkonu - Ne každá virtuální jednotka spotřebovává 100 % výkonu fyzického stroje. Při vytváření virtuálního serveru mu lze přiřadit přesné parametry a potřebné zdroje dle dané služby, která na něm bude fungovat. V praxi nikdy nelze využít výkon fyzického stroje na 100 %, proto zde máme virtualizaci, která se k tomuto optimu alespoň přibližuje. (7)

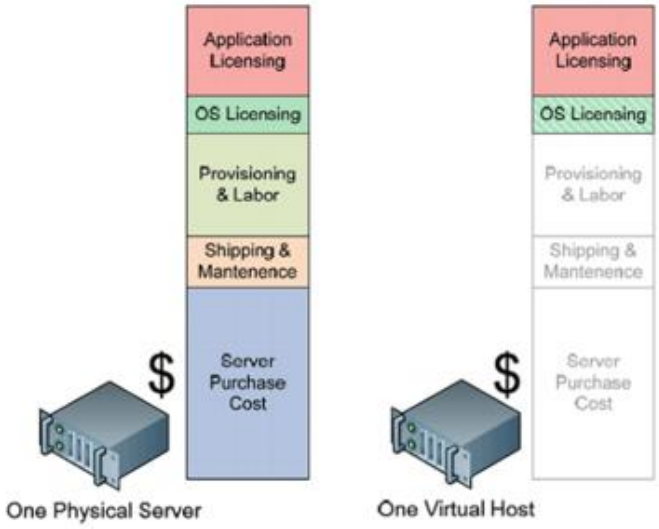
[2] Microsoft Exchange Server je produkt od firmy Microsoft, slouží k posílání e-mailových zpráv.

3.1.5.2. Ekonomické přínosy virtualizace

Při zavádění virtualizačních technik do vnitropodnikové infrastruktury se vedení podniku vždy zeptá na tu samou otázku. Pomůže nám tato technologie v budoucnu ušetřit nějaké náklady? Odpověď zní jednoznačně ano. Jednoduchým argumentem lze odpovědět, že virtualizace šetří finance. (11)

Další důvody proč zavádět virtualizace z ekonomického hlediska:

- Lepší produktivita zaměstnanců, díky neustále dostupným prostředkům
- Ušetřené náklady za provoz (energie, prostory, zabezpečení)
- Díky testovacímu prostředí a možnosti migrace v reálném čase může podnik efektivně reagovat na trendy a nové technologie
- Konsolidace serverů umožní zvýšit celkové systémové řízení a ušetří finanční prostředky na nutnost nákupu nových fyzických serverů a hardwarového vybavení
- Úspora nákladů na potřebnou podporu (servis serverů a hardwaru)
- Úspora nákladů při provozování IT oddělení (zaměstnanci)
- Úspora nákladů při obnově vnitropodnikové infrastruktury (krádež, únik dat, světové katastrofy) (11)



Obrázek 6 - Finanční porovnání fyzické a virtuální varianty řešení
Zdroj: https://fallbackstatus.com/implementing-virtualization-in-the-small-environment/

3.1.6. Platformy pro virtualizaci

Následuje představení několik komerčních hypervizorů, které budou rozebrány a následně porovnány. Jako hlavní a dominující hráč na trhu s virtualizační technikou se považuje firma VMware s jejím produktem vSphere. Toto tvrzení je ovšem neoficiální, ale čísla a technologický progres mluví za sebe. Jako dalšího velkého hráče lze považovat firmu Citrix s jejím produktem XEN. Nesmíme zapomínat na rychle prosperující konkurenční firmu Micsrosoft se svým rychle rozšiřujícím hypervizorem Hyper-V. Vyskytují se zde i menší hráči jako firma Oracle a její Virtualbox, tyto produkty ovšem nedosahují takových kvalit, jako nabízí firmy VMware nebo Microsoft. To je jedním z důvodu, proč nejsou tak rozšířené a užívají se převážně k osobním účelům. (6)

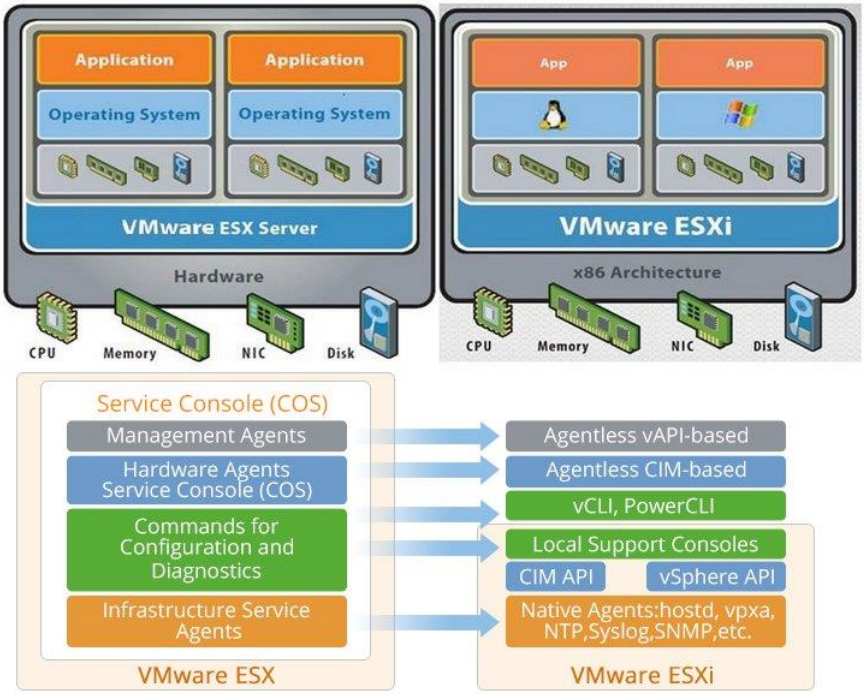
3.1.6.1. VMware

Jako hlavní produkty používané v serverovém prostředí od firmy VMware jsou ESX a vSphere. Společnost VMware nyní dodává na trh přes 150 svých produktů a řešení. Firma VMware se považuje za prvního zakladatele dnešní virtualizace. Dlouhá léta si společnost držela přední místo díky svým průkopnickým technologiím. V posledních letech se však objevují jisté konkurenční společnosti jako například Microsoft se svým hypervizorem Hyper-V. VMware dokázal jako první virtualizovat operační systémy Windows a Linux zároveň. Produkt vSphere v sobě zahrnuje velkou škálu funkcí a vymožeností, které mohou být aplikované od malých až po enteprisové[3] podniky. (12)(13)

Společnost VMware nabízí 2 hypervizory pro serverové prostředí. Produkt pod názvem ESX, kdy se jedná o tlustého klienta a produkt ESXi, tenký klient. ESX vyniká schopností servisní konzolového prostředí. Samotná instalace a konfigurace je tedy náročnější než u tenkého klienta. Hypervizor ESXi neobsahuje zmíněnou konzoli a tím je jeho celková velikost zredukována. To mu umožnuje rychlejší instalaci a samotný start aplikace. Když porovnáme tyto dva hypervizory, tak ESXi je levnější a nevyžaduje tolik bezpečnostních prvků. Na druhou stranu ESX má díky své konzoli rozsáhlejší funkcionality a širší spektrum nastavení. Funkcionality těchto dvou hypervizorů jsou sice dostačující, využívají se ale převážně v malých a středních podnikách. Pro datacentrovou virtualizaci a podniky větších rozměrů VMware nabízí vSphere a vSphere Hypervizor. Produkt vSphere Hypervizor je bezplatný a obsahuje jen omezené funkce. Slouží především jako taková „ochutnávka“ pro IT administrátory, kteří by tento produkt rádi otestovali a v případě zájmu i zakoupili plnou, placenou verzi. (12)(13)

Balíčky, které společnost VMware nabízí, jsou typu ALL-IN-ONE. Neobsahují technickou podporu, ta se musí později na každý produkt dokupovat zvlášť. Například je zde možnost pořízení ke svému stávajícímu balíčku i edici SUSE Linux Enteprise Server. Veškeré licence se pořizují na základě fyzických procesorů. Například u jednoho serveru se třemi procesory bude zapotřebí zakoupení 3 licencí, abychom pokryli všechny procesory. Pokud bychom zakoupili balíček s vSphere, máme zde možnost ho nainstalovat maximálně na 3 servery s dvěma procesory. (12)(13)

[3] Podnik nebo také nazývaný jako enteprise. Enteprisový produkt je určený ke komerčním účelům a většinou ve velkých měřítkách. Máme na mysli podnik s velkým počtem zaměstnanců.



Obrázek 7 - Porovnání hypervizoru ESX a ESXi
Zdroj: https://www.eukhost.com/kb/vmware-esx-vs-vmware-esxi-functionalities/

3.1.6.2. Microsoft Hyper-V

Firma Microsoft vstupuje na trh s virtualizníčmi technologiemi poměrně pozdě. Při vstupu čelí velké konkurenci od firem VMware a Citrixu. Tehdejší laťka byla nastavená opravdu vysoko a Microsoftu nezbývalo nic jiného než jen překvapit. Představuje svůj první hypervizor pod názvem Hyper-V Server 2008. Začíná se rychle vyvíjet a expandovat všemi směry. Hlavním úkolem je vytvořit konkurence schopného hypervizora za co nejmenší čas. Soustředí se jak na malé a střední podniky, tak i složité enterpsiové prostředí, kdy nároky a požadavky na ucelení vnitropodnikové infrastruktury jsou zcela jiné. (14)

Současná verze hypervizoru je Hyper-V Server 2019 a je nabízená ve dvou variantách. Jako bezplatnou verzi Microsoft nabízí Hyper-V Server 2019 Core edici. Bezplatná verze opět slouží jako testovací a zkušební pro IT administrátory. Neobsahuje veškeré prvky jako ta placená. Chybí zde například grafické rozhraní, ovládání je možné tedy jen přes příkazovou řádku (PowerShell). Ovládání je zcela složité a neumožnuje rozsáhlé konfigurace jako je tomu u té placené verze. (14)

V současné době Microsoft nabízí 2 základní verze Windows Serveru 2019. Obě tyto verze obsahuj funkci hypervizora a umožnují virtualizaci. Jedná se o edice DataCenter a Standart. Standartní edice umožnuje provozovat maximálně dvě virtuální instance, přičemž DataCenter edice žádná taková omezení nemá. Umožnuje tedy provozovat neomezený počet virtuální instancí na dané instanci. (14)

Funkcionality, které jsou nabízeny produktem Hyper-V umožnují od konsolidace serverů v malých a středních firmách, až po využívání v obrovských datacentrech.

Tím pádem může konkurovat virtualizačnímu obrovi VMware v tomto odvětví. Hyper-V Server 2019 umožnuje taktéž virtualizaci na odlišných operačních systémech. Podporuje architektury jako UNIX, LINUX, FreeBSD a mnoho dalších. Hyper-V můžeme využívat i pro virtuální servery, které budou provozovány na jiných operačních systémech nežli jakákoliv verze Windows Serveru. (14)

3.1.6.3. XenServer

Společnost Citrix nabízí své řešení a to v podobě produktu XenServer. Dnes se již jedná plně virtualizované prostředí, které funguje na samotném hardwaru. Dříve tomu tak nebylo. Hypervizor XenServer poskytoval jen paravirtualizaci. S příchodem nových virtualačních vymožeností, kdy začínají podporovat virtualizaci i procesory Intel a AMD, XenServer začíná poskytovat i plnou virtualizaci. Jako hlavní funkce, které XenServer umožnuje je možnost virtualizace na operačních systémech Windows i Linux. Samotný XenServer vychází z Linuxu a tím pádem nepotřebuje žádný podřazený operační systém. (15)

Marketing XenServeru je uspořádaný tak, aby uspokojoval firmy všech velikostí. Proto je nabízen celkem ve čtyřech edicích. Samotné licencování se odlišuje od firem VMwere a Microsoftu. XenServer je opensource produkt, řídí se proto licenční politikou GPI. Základní a bezplatnou verzi, kterou firma Citrix poskytuje, je primárně opět pro IT administrátory a jejich testovací účely. Jsou zde funkce jako snapshot, migrace fyzických serveru do virtuálního prostředí a mnoho dalších. Placená verze obsahuje možnost vysoké dostupnosti virtuální infrastruktury, možnost reportování, statistik a optimalizace paměti. Placený produkt se jmenuje Advance, obsahuje všechny výše zmíněné funkce a stojí 24 420,- Kč včetně DPH. Nejrozsáhlejší a nejdražší verze je Enterprise, která poskytuje schopnost flexibilního rozdělování zátěže, detailnější administraci a rozšířenou konfiguraci hypervizora. Cena jedné license pro jednoho hosta činí 60 500,- Kč včetně DPH. (3)(15)

Features included at no cost	Citrix XenServer	VMware ESXi
Bare-metal hypervisor	64-bit	32-bit
Max virtual CPUs	8	4
Windows® and Linux guests	✓	✓
Unlimited servers, VMs, memory	✓	✓
P2V & V2V conversion	✓	✓
Shared SAN and NAS storage	✓	✓
Centralized multi-server management	✓	
Resilient distributed management architecture	✓	
Live motion	✓	
Shared VM template library	✓	
Centralized configuration management	✓	
Virtual infrastructure patch management	✓	
Intelligent initial VM placement	✓	
Intelligent server maintenance mode	✓	
Fine-grained CPU resource controls	✓	
Hot-swappable disks and NICs	✓	

Obrázek 8 - Porovnání XenServer Enteprise s WMware ESXi

Zdroj: http://www.virtualizationteam.com/server-virtualization/citrix-xenserver-enterprise-for-free.html

3.2. Kybernetická bezpečnost

3.2.1. Úvod

Odvětví, které má za úkol zabezpečování informací a majetku před zneužitím, se v oboru informačních technologiích nazývá kybernetická bezpečnost (cyber security). Toto zabezpečení platí jak pro lokální počítače, servery tak i veškeré sítové komunikace. Nutno podotknout, že kybernetická bezpečnost má na starost jak virtuální útoky, tak i samotné případy fyzického poškození. Například vandalismus, žhářství, krádež a další. Hlavní pointa a myšlenka zůstává zabezpečení informací a dat na strojích výpočetní techniky, aby nemohlo dojit k úniku a zároveň aby tyto prostředky byly dostupné a produktivní pro patřičné uživatelé. (17)(18)

Termín „bezpečnost informačních systémů“ představuje metodiky a postupy, které slouží k prevenci proti poškození, zveřejnění, kolapsu, či přístupu neoprávněné osoby k citlivými informacím a službám. Metody a praktiky se liší podle účelům a potřebám zabezpečení. Standardy kybernetické bezpečnosti přišly v účinnost teprve nedávno, tak jak nárůst potřeby zabezpečovat informace je problematika převážně dnešní doby. Mnoho dat a informací jsou ukládaná převážně jen na výpočetních přístrojích a dochází zde ke komunikaci přes internet. Také mnoho úkolů a činností dnes nabývají jiného směru a neobejdou se bez těchto technologií. Zvýšenou poptávku po tomto odvětví IT nejvíce projevily obchodní korporace a firmy. Potřebují dennodenně zajištovat nespočetné objemy dat, obchodní tajemství a různé citlivé informace o své instituci či svých zaměstnancích. Ukázkovým příkladem je naše vláda. (17)(18)

Jedním z primárních a nejrozšířenějším standardem je ISO 27001. Pojednává a definuje požadavky, jak by měl samotný bezpečnostní managment vypadat a hlavně fungovat. Dále řízení bezpečnostní důvěry, bezpečnostní informace pro zaměstnance, vnitropodnikové procesy a IT systémy, které s těmito informacemi pracují. Všechny tyto normy a předpisy vydává a řídí Mezinárodní organizace pro normalizaci, známá pod zkratkou ISO (International Organization for Standardization). Pro Českou republiku zde máme Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). NÚKIB zaujímá pozici ústředního správního orgánu pro kybernetickou bezpečnost a jeho hlavním cílem je bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních sytému. Sídlo tohoto orgánu se nachází v Brně. (17)(19)

Další činnosti toho úřadu jsou:

- Provozování Vládní CERT České republiky (GovCERT.CZ)
- Vzdělávání a kontrola ostatních institucí v oblasti kybernetické bezpečnosti
- Ochrana tajných a státních informací
- Výzkum a vývoj v oblasti kybernetické bezpečnosti
- Spolupráce s mezinárodními týmy při vytváření nových bezpečnostních standardů pro informační systémy

Obrázek 9 - Životní cyklus v kybernetické bezpečnosti
Zdroj: https://www.kybez.cz/

3.2.2. Zásady kybernetické ochrany

Většina podniků nebo obyčejných uživatelů dnes jen reagují na kybernetické útoky. Snaží si držet krok s vývojem technologií, ale malá část uživatelů se snaží útoky preventivně elimininovat. Tato problematika se netýká se jen velkých či malých podniků, ale i dat obyčejného uživatele. Jakékoliv data mohou být pro útočníka přínosné.

Jedná se o prosperující trend, díky kterému komunita začala více dbát na ochranu svých dat, ale ne všechny složky naší komunity pro to dělají své maximum. Není tomu tak dávno, kdy před pár lety velké státy, či organizace byly napadeny a miliony uživatelů přišli o své data či jejich data byla zneužita. Velké organizace, i přes jejich milionové roční obraty nevkládají dostatečné finance do zabezpečení jejích infrastruktury, školení zaměstnanců či nových technologií. Reagovat na aktuální hrozby nestačí. Hlavní myšlenkou kybernetické bezpečnosti je být dynamický, rychle se přizpůsobovat trendům, implementovat nové technologie kde to bude zapotřebí a hlavně dbát na školení svého personálu.

Přitom to nemusí být až tak náročné, jak se může na první pohled zdát. Stačí dodržovat základní pravidla kybernetické bezpečnosti a tím docílit celkové vnitřní ochrany. Jedná se o základní techniky, postupy a principy se kterými by měl být obeznámen každý uživatel. Nejedná se jen o jednorázový případ, či školení, které by mělo být absolvováno, ale o principy uplatňované na denní bázi.

Oprávnění - Uživatel by měl disponovat dostačujícími oprávněními k jeho pracovní činnosti. Není nutné, aby obyčejný uživatel měl vyšší oprávnění, než potřebuje. S vyššíma oprávněními je i úzce spjata zodpovědnost za ně. Správné delegování oprávnění je jedním z klíčových aspektů k výraznému omezení rizika zneužití. [20]

Šifrování - Jakékoliv vnější komunikace či sdílení dat přes služby by měly být jedinečně zašifrovány. Klíče, či hesla by se nikdy neměla zasílat stejnou cestou jako ostatní zasílané dokumenty. Pokud se útočník dostal skrz všechny obrané prvky a došlo k úniku dat, nebude možné tyto data bez příslušeného dešifrovacího klíče přečíst či jakékoliv další manipulace. Nejedná se jen o šifrování, ale i zabezpečení komunikace, aby bylo zabráněno odposlechu. (20)

Segmentace - Segmentace, dělení podniku na menší vnitropodnikové části se nedělá jen z důvodu delegování ale i bezpečnosti. Pokud se útočník dostal přes vnější ochranné systémy a nachází se uvnitř, nemá hned dostupné veškeré celky struktury. Jednotlivé celky jsou od sebe odděleny, tak aby útočníka zpomalily, či zabránily k plošnému napadení celé infrastruktury. Velkým doporučením je nesoustředit veškeré prostředky a zdroje na vnější ochranu, ale rovněž nezapomínat na části vnitřní bezpečnosti. (20)

Aktualizace - Je nezbytné udržovat všechny systémy aktuální na té nejnovější verzi. Aktualizace je především vylepšení, často spjatá s doplněním nových funkcí, ale také oprava zjištěných chyb či prevence vůči nadcházejícím útokům. (20)

Ověřování - Různé druhy dvoufaktorového ověření, mohou útočníka značně zpomalit, či eliminovat možnost získat citlivé data. Technologie typu od rozpoznávání otisku nebo tváře, až po externí certifikáty mohou značně zabezpečit vnitřní strukturu podniku. (20)

3.2.3. VMware v kybernetické bezpečnosti

VMware jak již bylo uvedeno v předešlé teoretické části, je jeden z nejlepších nástrojů pro virtualizování. Jeho bohatá historie a kvality, dosahující dlouhou dobu prvního místa mezi konkurencí. Tak jako ostatní hypervizoři se snaží držet krok s dobou a nesoustředit své zdroje jedním směrem. (20)

Firma VMware si moc dobře uvědomuje, jak velkou roli hraje kybernetická bezpečnost v IT sektoru a jak důležité je tento druh odvětví podporovat. Jako jedna z mála virtualizačních organizací úzce spolupracuje s některými bezpečnostními organizacemi. Přizpůsobuje tomu i své produkty a poskytované služby. Pro své zaměstnance či partnerské organizace pravidelně organizuje různá školení na téma kybernetická bezpečnost. Na jejich oficiálních webových stránkách, můžeme najít nemalý počet školících dokumentů právě na tuto problematiku. (20)

Virtualizační nástroj VMware je dle autora bakalářské práce nejlepší volbou pro malé i velké podniky, pokud je zapotřebí účinný virtualizační nástroj za přiměřené peníze.

3.2.3.1. Testovací prostředí

Hypervizor VMware podporuje možnost vytvoření testovacího prostředí, které bude zcela izolované od firemní infrastruktury.

Tuto schopnost nelze jen tak přehlédnout, jelikož se jedná o základní prvek při testování či zavádění nové technologie do podniku. Testovací prostředí by mělo být izolované, ideálně provozované na jiném hardwaru a nemělo by se nacházet ve stejné sítí jako prostředí produkční.

3.2.3.2. Funkce využívané v kybernetické bezpečnosti

Produkt VMware se snaží být optimalizovaný pro jakékoliv prostředí a jejich uživatelé. Proto nabízí velkou škálu možností a funkcí, které lze vykonávat celopodnikově, či jen v soukromém užívání. Například se jedná o tyto funkce:

Snapshot – Možnost zaznamenání časového úseku, kdy se do souboru uloží aktuální stav stroje i s danou konfigurací. Tato funkce slouží převážně k zálohování, obnově dat nebo migraci stroje na jiný server.

Migrace – Možnost přenášení virtuálního stroje mezi servery. Funkce využívána především při výpadku fyzické jednotky, kdy se virtuální stroj přenese na jiné fyzický či virtuální stroj a dosáhne se tím plynulý běh služby bez nutnosti odstávky či výpadku. Veškeré úkony se provádí v reálném čase, uživatel nemusí pocítit žádné změny.

Šifrování dat – Hypervizor VMware umožnuje šifrování dat, jak na samotném virtuálním stroji, tak při přenosu mezi servery.

Oprávnění – Oprávnění lze delegovat a nastavovat ve vCentru, kde se nachází administrace a přehled celé virtualizační infrastruktury. Dělíme zde oprávnění do vCentra nebo na samotné virtuální stroje. Uživatel s oprávněními do vCentra může vytvářet či spravovat virtuální stroje, přidělovat jim technické zdroje, migrovat a další funkce na základě udělených oprávnění. Uživatel disponujícími oprávněními jen do virtuálního stroje má možnost přístupů a dále práce jen na daném stroji.

4. Vlastní práce

Praktická část této bakalářské práce bude realizována na Ministerstvu spravedlnosti České republiky. Přesněji v ekonomickém odboru, v oddělení kybernetické bezpečnosti. Bude dodrženo zadání práce realizace virtuálního stroje, jeho následná konfigurace, zabezpečení a ve výsledcích rozebrané varianty, či rady, jak docílit nejlepšího hledaného řešení. Tato bakalářská práce má posloužit jako vnitropodnikový materiál pro zaměstnance Ministerstva spravedlnosti v oddělení kybernetické bezpečnosti. Autor bakalářské práce podotýká, že se nemá jednat o návod, či dokument podobný tomuto typu, ale o pomůcku sloužící s obeznámením s touto problematikou a jejího řešení v denním běžném provozu ministerstva. Ve vnitropodnikové infrastruktuře se používá hypervizor VMware. Vlastní práce bude demonstrována právě pomocí tohoto hypervizoru. Data použitá v praktické části nemusí být vždy pravdivá v důsledku utajování a zveřejňování citlivých informací ministerstva.

Pokud chceme zavádět virtualizační technologii do podniku, musíme zvážit veškeré aspekty tohoto rozhodnutí. Zdali nám opravdu přinese větší užitek než doposud využívané technologie a zároveň ušetří finance. K tomu nám poslouží toto jednoduché schéma, na základě kterého budeme postupovat:

1) Analýza vnitropodnikové struktury
2) Cenová kalkulace
3) Testovací prostředí
4) Varianty zapojení v praxi
5) Vytvoření a konfigurace virtuální stroje

4.1. Analýza vnitropodnikové struktury

V důsledku utajování informací nemohou být v tomto kroku praktické části uvedená přesná data ministerstva. Budou zde použita demonstrační data k nastínění průběhu řešení.

Analýza vnitropodnikové struktury je prvním a nejdůležitějším krokem k zavedení této technologie do podniku. Podnik by měl mít přehled o svém majetku a jeho využití. Zdroje vynaložené na nepoužívaný majetek by mohly být využity efektivněji. K tomu je zapotřebí provedení analýzy podnikového majetku a pak následná inventarizace.

Podnik může zvolit variantu pomocí použití komerčních programů, jako například MSBA – Microsoft Baseline Securty Analyzer a k tomu doplněk Visio Connector for MBSA. Tento software vyhledá všechna konečná zařízení v infrastruktuře a vygeneruje následný přehled. Druha varianta je manuální, kdy se může jednat o menší organizaci. Tento krok bude následně demonstrován.

Umístění	Typ/Model	Název	Virtualizovat	Účel	OS	Adresa
Vyšehradská	IBM System x3650 M5	VM01	Vhodný pro virtualizaci	Servis Cam	Win server 2003 R2	192.68.101.1
Vyšehradská	IBM System x3650 M5	VM02	Vhodný pro virtualizaci	Servis Cam	Win server 2012 R2	192.68.101.2
Vyšehradská	IBM System x3650 M5	VM03	Vhodný pro virtualizaci	DT + SQL	Win server 2012 R2	192.68.101.3
Vyšehradská	IBM System x3650 M5	VM04	Vhodný pro virtualizaci	DT + SQL	Win server 2012 R2	192.68.101.4
Vyšehradská	Fujitsu Primergy RX1330 M4	VM05	Vhodný pro virtualizaci	DT + SQL	Win server 2012 R2	192.68.101.5
Vyšehradská	Fujitsu Primergy RX1330 M5	VM06	x	Backup server	Win server 2003 R2	192.68.101.6
Vyšehradská	IBM System x3650 M5	VM07	x	Backup server	Win server 2003 R2	192.68.101.7
Vyšehradská	IBM System x3650 M6	VM08	Vhodný pro virtualizaci	Aplikační server	Win server 2019	192.68.101.8
Vyšehradská	IBM System x3650 M7	VM09	Vhodný pro virtualizaci	Exchange server	Win server 2019	192.68.101.9
Vyšehradská	IBM System x3650 M8	VM10	Vhodný pro virtualizaci	Exchange server	Win server 2019	192.68.101.10
Pankrác	Lenovo System x3550 M6	PM01	Vhodný pro virtualizaci	Exchange server	Win server 2019	192.68.101.11
Pankrác	IBM System x3650 M5	PM02	Vhodný pro virtualizaci	Exchange server	Win server 2012 R2	192.68.101.12
Pankrác	Lenovo System x3550 M7	PM03	Vhodný pro virtualizaci	Antispam / Baracuda	Win server 2012 R2	192.68.101.13
Pankrác	Lenovo System x3550 M6	PM04	x	DNS, DHCP	Win server 2019	192.68.101.14
Pankrác	Lenovo System x3550 M7	PM05	Vhodný pro virtualizaci	Web server	Win server 2019	192.68.101.15
Míčanky	IBM System x3650 M5	MM01	Vhodný pro virtualizaci	Aplikační server	Win server 2019	192.68.101.16
Míčanky	Lenovo System x3550 M5	MM02	x	Doménový řadič	Win server 2019	192.68.101.17
Míčanky	Fujitsu Primergy RX1330 M6	MM03	x	Doménový řadič	Win server 2003 R2	192.68.101.18
Míčanky	Lenovo System x3550 M8	MM04	x	Doménový řadič	Win server 2003 R2	192.68.101.19
Míčanky	Lenovo System x3550 M9	MM05	Vhodný pro virtualizaci	PDF Convertor	Win server 2003 R2	192.68.101.20

Tabulka 1 - Analýza vnitropodnikové infrastruktury

Z tabulky lze vyčíst, že ne všechny servery budou virtualizovány. Virtualizace serveru se provádí na základě jeho poskytované služby či účelu. Servery převádíme do virtuálního prostředí za účelem docílení vysoké dostupnosti, prevenci vůči výpadkům, zabezpečení, komptabilitě a přívětivější správě serveru. Avšak některé služby musí být provozovány na fyzických serverech. Proto si podnik musí stanovit jasné cíle a směry v tomto rozvržení. Na základě toho provést důkladné plánování, dokud nepřistoupí k samotné virtualizaci. Například virtualizovat zálohovací server, který bude ještě k tomu fungovat na serveru fyzickém, nebude nejlepším rozhodnutím. Při výpadku dojde k absolutní ztrátě dat. Rozvržení vnitropodnikové struktury musí být důkladně promyšleno.

4.2. Cenová kalkulace

V tomto kroku si provedeme demonstraci cenové kalkulace, zdali za pomocí této technologie dospějeme k úsporám financí. Opět se jedná o subjektivní kalkulaci. Do cenového řešení musí být zahrnuty náklady jak na hardware, tak i software a další potřebné služby.

V následujících kalkulacích, nejsou obsaženy ceny za doplňkový materiál a prostředky, jako například kabely pro připojení, modemy atd. Budou následovat dvě varianty kalkulace, jedna bude vyobrazovat řešení pomocí virtualizační technologie, náklady spojené s ní a druhá varianta bude řešit návrh čistě za pomocí fyzických serverů.

Hlavním úkolem této kalkulace je demonstrovat jaké náklady by podnik musel vynaložit na koupi a následný provoz deseti serverů ve vnitropodnikové struktuře.

4.2.1. Cenová kalkulace virtuálního řešení

V této kalkulaci bude demonstrováno řešení za pomocí využití virtualizační technologie, potřebné náklady na její nasazení a následný provoz. Celková cena virtualizačního řešení činí 2 685 043 Kč bez DPH. Nutno podotknout, že se jedná o řešení

o třech fyzických serverech, na kterých bude provozována virtualizační technologie. Tři fyzické servery dokážou obsluhovat a poskytovat zdroje pro deset virtuálních. Toto řešení má velkou nevýhodu, a to nutnost investovat velké finance hned ze startu při zavádění této technologie do podniku. V následných tabulkách jsou uvedené ceny za hardware, služby, operační systémy a pořízení hypervizoru.

Hardware

12Core - Gold 6246	Počet
ThinkSystem SN550 - 3yr Warranty	3
Description	Počet
Lenovo ThinkSystem SN550 CLX Server	1
Intel Xeon Gold 6246 12C 165W 3.3GHz Processor	1
ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	6
ThinkSystem SATA Backplane for SN550	1
Select Storage devices - no configured RAID required	1
ThinkSystem 2.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	2
Flex System CN4052S 2-port 10Gb Virtual Fabric Adapter	1
ThinkSystem Emulex LPm16002B-L Mezz 16Gb 2-Port Fibre Channel Adapter	1
Feature Enable TPM 1.2	1
Disable IPMI-over-LAN	1
Lenovo ThinkSystem SN550 Server WW packaging - Standard	1
Lenovo ThinkSystem Server HDD Bezel Facia	1
Lenovo ThinkSystem Heatsink Filler	1
Lenovo ThinkSystem SN550 Server Service Label LI	1
Lenovo ThinkSystem SN550 Server Label	1
ThinkSystem 4R CPU HS Clip	1
Lenovo ThinkSystem SN550 Server Cover	1
Lenovo ThinkSystem SN550 Server Air Baffle	1
Lenovo ThinkSystem Server Rear CPU Heatsink	1
Intel Inside Xeon Label	1
Feature Enable TPM on MB	1
System Documentation	1

Název	Celková cena bez DPH
ThinkSystem SN550 - 3yr Warranty	**931 641,00 Kč**

Tabulka 2 - Ceny za hardware, virtuální varianta

V následující tabulce jsou uvedeny ceny za licence operačního systému a náklady spojené s migrací do virtuálního prostředí.

Operační systém + náklady potřebné na migraci do virtuální prostředí

Název	Počet	Cena
Windows Server 2019 Datacenter (16 cores)	3	151 900,00 Kč
Náklady spojené s migrací do virtuální prostředí		
Konfigurace virtuálního serveru - Exchange	3	26 000,00 Kč
Konfigurace virtuálního serveru - Antivir	3	12 000,00 Kč
Konfigurace virtuálního serveru - Bezpečnostní kamery	3	8 000,00 Kč
Konfigurace virtuálního serveru - Zálohovací server	3	22 000,00 Kč
Konfigurace virtuálního serveru - Databáze + SQL	3	10 000,00 Kč
Konfigurace virtuálního serveru - File server	3	8 000,00 Kč
Konfigurace virtuálního serveru - Testovací centrum	3	5 000,00 Kč

Celkem bez DPH	**728 700,00 Kč**

Tabulka 3 - Ceny za OS + náklady spojené s migrací, virtuální varianta [21][22]

V poslední tabulce jsou vyobrazeny ceny za nákup hypervizoru a služby nutné k jeho provozu.

VMware

Název	Cena
VMware vSphere 5 Enterprise Plus Acceleration Kit - 6 proccesors + 3 years support	598 925,00 Kč
Production Support/Subscription VMware vSphere 5 Enterprise Plus Acceleration Kit for 6 processors for 3 years	362 186,00 Kč
VMware vCenter Lab Manage for 1 processor	63 591,00 Kč

Celkem bez DPH	**1 024 702,00 Kč**

Tabulka 4 - Ceny za licence VMwaru, virtuální varianta

4.2.2. Cenová kalkulace fyzického řešení

Nyní přichází na řadu fyzické řešení, kdy podnik bude fungovat na deseti fyzických serverech.

Hardware

Název	Počet	Cena bez DPH
ThinkSystem SN550 - 3yr Warranty	10	**3 105 470,00 Kč**

Tabulka 5 - Ceny za hardware, fyzická varianta

Operační systém

Název	Počet	Cena
Windows Server 2019 Datacenter (16 cores)	10	151 900,00 Kč

Celkem bez DPH	**1 519 000,00 Kč**

Tabulka 6 - Ceny za OS, fyzická varianta

4.2.3. Vyhodnocení variant

Při porovnání fyzické a virtuální varianty dojde k značnému rozdílu v celkové ceně řešení.

Virtuální řešení nám umožnuje značnou elasticitu, při rozšiřování podnikové infrastruktury v budoucnosti. Celkové řešení této varianty nás vyjde na 2 685 043 Kč bez DPH. Nutno podotknout, že se jedná o tři fyzické servery, na kterých je nainstalovaná virtualizační technologie a lze na nich vytvářet další virtuální servery. Úkolem této demonstrace bylo dosáhnout deseti serverů. Cíl byl jednoznačně dosažen a ještě zbyly zdroje na další servery, jelikož v této sestavě jich můžeme vytvořit a následně spravovat zdaleka více než zadaných deset. Toto řešení vyšlo levněji po finanční stránce, a hlavně je i úspornější při dlouhodobém provozování. Nejsou zde započítaný náklady na elektřinu, obsluhu, chlazení a zabezpečení, ale s jistotou můžeme říct, že se bude jednat o menší částku než u fyzické varianty. Další značnou výhodou je konsolidace serverů, úspora místa v datacentru a šetrnost k životnímu prostředí.

Fyzické řešení stojí 4 624 470 Kč bez DPH. Jedná se o značný rozdíl oproti virtuálnímu řešení. Tato varianta obsahuje holé stroje se zakoupenými licencemi operačního systému. Opět se jedná o variantu bez započítaných nákladů na provoz. Zvýšené náklady na elektřinu, chlazení, zabezpečení, obsluhu a nutnost většího prostoru v datacentru. Tato varianta není šetrná k životnímu prostředí a zároveň je zde při rozšiřování infrastruktury nutnost nákupu nového hardwaru a OS.

4.3. Testovací prostředí

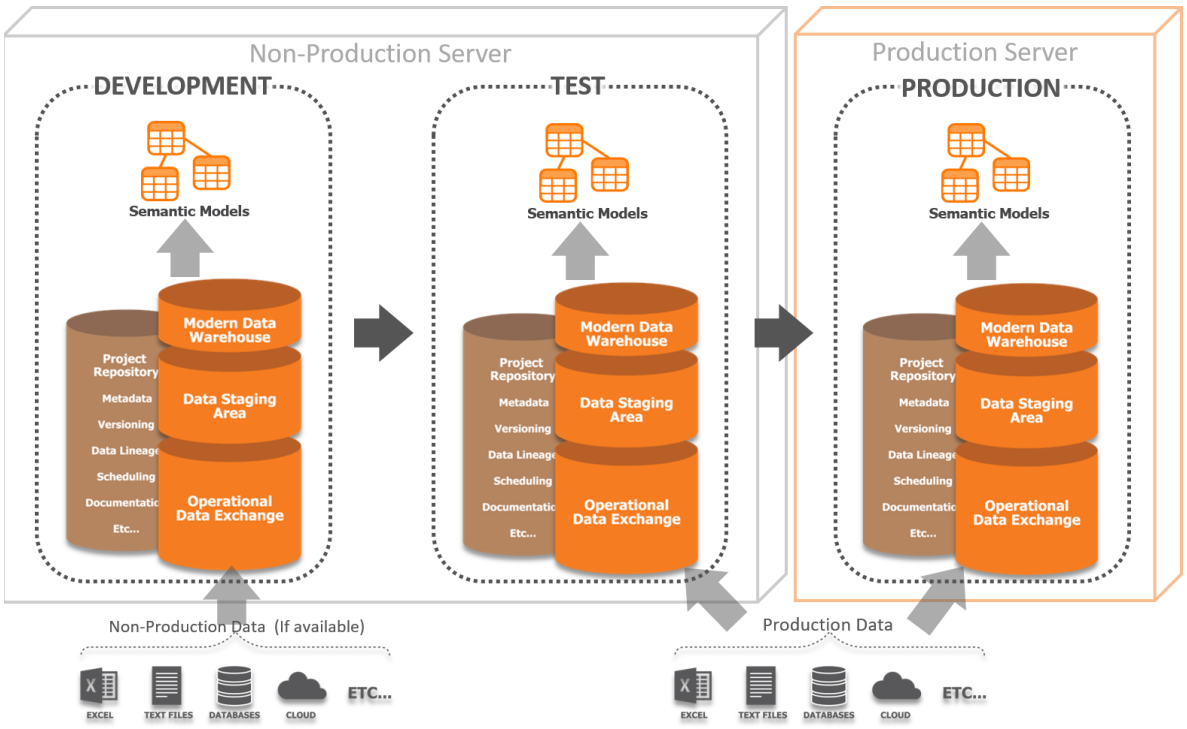
Před tím, než bude virtualizační technologie nasazená v plném rozsahu do celé infrastruktury, by se měla otestovat v testovacím prostředí. Slušný podnik by měl disponovat dvěma prostředími, testovacím a produkčním. V produkčním prostředí podnik provozuje běžný denní provoz, v testovacím prostředí testuje nové služby a technologie. Hlavní myšlenkou a úkolem testovacího prostředí je simulovat běžný provoz podniku na základě různých scénářů a následně zaznamenávat a zajišťovat jisté nedostatky, které technologie může ze začátku přinést.

Testovací prostředí je hlavním prvkem z pohledu kybernetické bezpečnosti při zavádění nových technologií či služeb do podniku. Je velmi důležité tyto nové technologie důkladně otestovat, zdali při zavedení nenaruší infrastrukturu, neobsahují škodlivý malware nebo jakákoliv zadní vrátka od dodavatele, které by mohl v budoucnosti využít. Pokud by se tyto hrozby objevily, došlo by k okamžité eliminaci a zamezení rozšíření do podnikové struktury. Oprávnění, které jsou uděleny poskytovateli služby či dodavateli v testovacím prostředí nijak neohrožují chod produkčního prostředí. Pokud by dodavatel měl nekalé úmysly, dokázal by napáchat škody na základě jeho oprávnění jen v testovacím prostředí.

Stroje, které budou určeny k provozu testovacího prostředí, nemusí být až tak výkonné jako u produkčního prostředí, avšak měly by být dostatečně výkonné pro simulaci

reálné zátěže. Testovací prostředí by mělo být od produkčního oddělené a ideálně se nacházet v jiné sítí, pokud to prostředky umožnují. Delegování oprávnění v tomto prostředí je čistě na úvaze podniku, avšak do tohoto prostředí budou nejspíš přistupovat pouze dodavatelé dané technologie a informatici.

Na následujícím obrázku lze vidět, jak taková struktura testovacího prostředí může vypadat.



Obrázek 10 - Struktura testovacího prostředí
Zdroj: https://learn.timextender.com/courses/301-advanced/lectures/4029947

4.4. Varianty zapojení virtualizace v praxi

V následující části budou demonstrovány různé varianty zapojení virtualizační technologií v praxi. Možností zapojení je hned několik a jedná se poměrně o subjektivní záležitost. Podnik by měl zvážit hned několik variant a zvolit tu nejlepší. Daná varianta by měla být flexibilní při budoucím rozšiřování, vydržet denní provoz a být schopná efektivně reagovat na vnitropodnikové změny či výpadky.

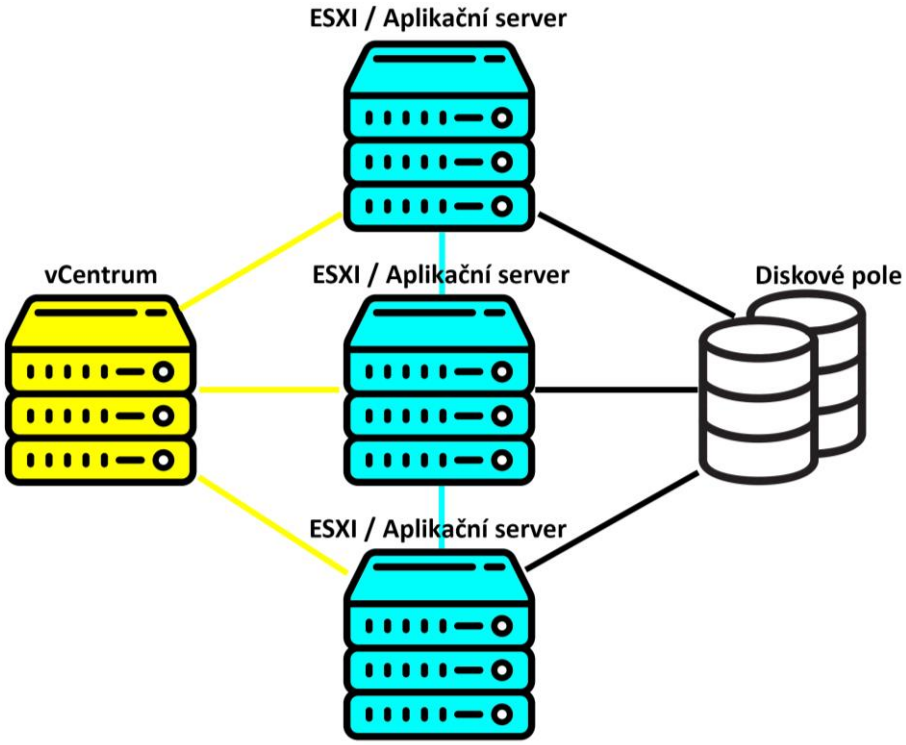
Nyní, jako názornou ukázku budou demonstrovány dvě varianty zapojení.

4.4.1. Varianta A

Tato varianta je již zastaralá a neefektivní, na ministerstvu je momentálně nasazená varianta B, ale pro názornou demonstraci bude tato varianta plně dostačovat. Jedná se o poměrně jednoduché zapojení, které je ideální při prvotním nasazení virtualizační technologie do vnitropodnikové infrastruktury.

Hlavním aspektem je vCentrum. Samotné vCentrum může být nainstalované jak na fyzickém, tak i virtuálním stroji. Pomocí vCentra administrátor ovládá a vytváří všechny virtuální stroje. Server s nainstalovaným vCentrem by měl být dostupný pro všechny virtuální stroje z důvodu správy a případnému řešení kolizí. Administrátor přiděluj zdroje nově vytvářeným virtuálním serverům dle potřeby a dostupnosti na základě fyzického výkonu. Tyto stroje mohou opět fungovat na jednom fyzickém zařízení, nebo být rozmístěny dle potřeby delegování zátěže. Samotné aplikační servery mají přístup k diskovým polím či databázím na základě jejich účelu a služby, která je serverem poskytována.

Varianta A je velmi primitivní a slouží opravdu jen k základnímu nasazení virtualizační technologie do podniku. Varianta není chráněná vůči výpadkům a neumožňuje možnost zapojení více lokalit.



Obrázek 11 - Zapojení virtualizace, varianta A
Zdroj: Autor

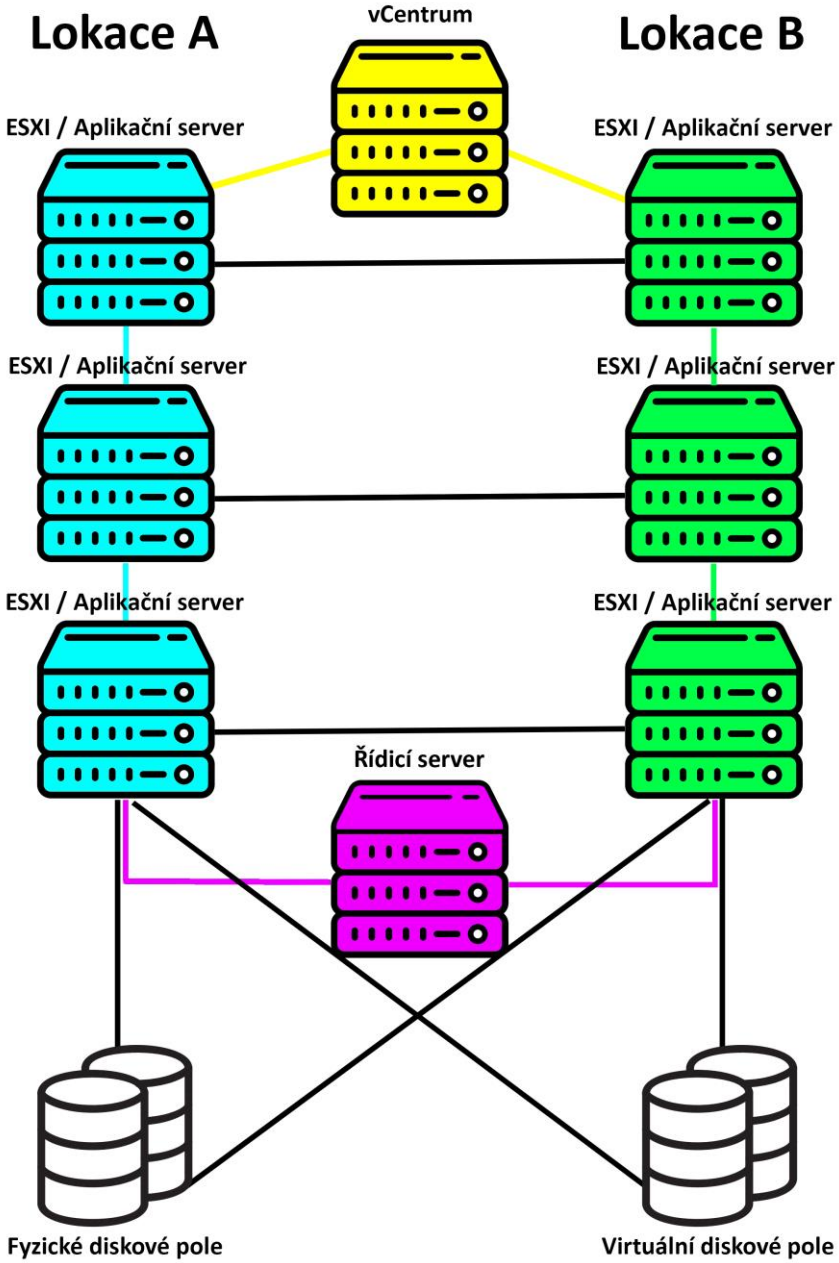
4.4.2. Varianta B

Aktuální varianta způsobu nasazení na Ministerstvu spravedlnosti ČR. Jedná o pokročilejší variantu. Zohledňuje a umožnuje přepínání serverů dle aktuální zátěže a je chráněná vůči výpadkům. Jelikož ministerstvo spravuje více budov po celé Praze, musí tyto lokace spravovat decentralizovaně, ale zároveň zachovat vysokou dostupnost všech složek. Varianta B podporuje zapojení více lokalit.

Hlavním a řídícím prvkem je opět vCentrum. Server s nainstalovaným vCentrem musí vidět na všechny ostatní servery. Ve vCentru administrátor reguluje zátěž, popřípadě vytváří nové servery a dle právě prováděné údržby či výpadku migruje mezi servery.

Aplikační servery nebo ESXI servery mají přístup k diskovým polím, která mohou být nyní jak ve fyzické, tak i virtuální podobě. Na obrázku jsou zobrazeny dvě lokace. Tento princip fungování slouží k prevenci výpadku jedné z lokalit. Pokud k takovému výpadku dojde, servery například z lokace A migrují na lokaci B, kde jsou spuštěny a fungují v normálním režimu. Tuto celou operaci řídí řídící server neboli Withnes. Withnes server monitoruje provoz obou lokalit. Na základě pingové komunikace určuje, zdali jsou lokace dostupné. Pokud u jedné z lokací dojde k přerušení komunikace s řídícím serverem, automaticky tyto servery migruje na druhou lokaci. Migraci serverů a další automatické akce lze regulovat na základě pravidel. Tyto pravidla nastavuje administrátor ve vCentru, stejně jako pravidla na řízení a rozdělování zátěže mezi servery.

Varianta B je velmi efektivní a dostačující na základě dnešních potřeb podniku. Autor bakalářské práce podotýká, že se jedná opět o subjektivní typ zapojení. Tato varianta zapojení umožnuje v budoucnosti připojit nové lokality, je chráněna vůči výpadkům, flexibilní co se týče rozšiřování vnitropodnikové infrastruktury a umožnuje regulaci zátěže.

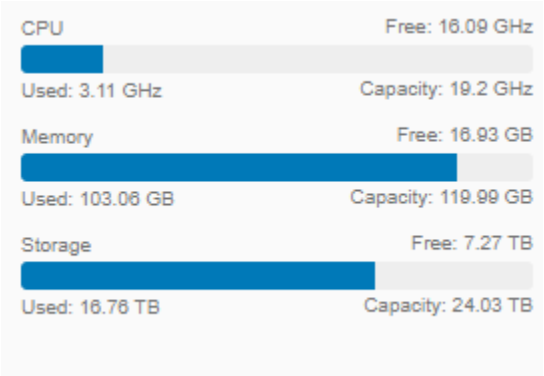


Obrázek 12 - Zapojení virtualizace, varianta B
Zdroj: Autor

4.5. Vytvoření virtuálního stroje

V této praktické části bakalářské práce bude demonstrováno vytvoření virtuálního stroje za pomocí užití hypervizoru VMware vSphere. Demonstrace bude probíhat v testovacím prostředí Ministerstva spravedlnosti ČR. Budou zhodnoceny především nejdůležitější kroky a postupy, které musí být dodrženy při vytváření virtuálního stroje.

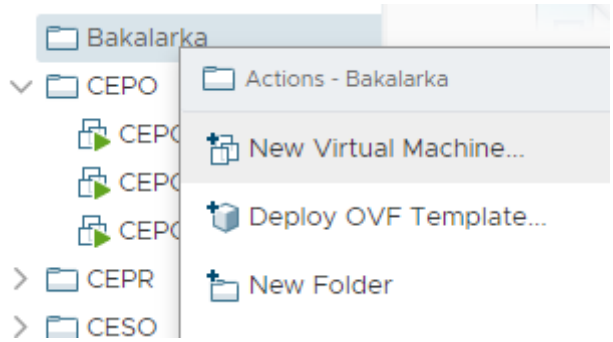
Testovací prostředí ministerstva disponuje těmito parametry:



Obrázek 13 - Parametry testovacího prostředí na MSP
Zdroj: Autor

Opět je nutno podotknout, že testovací prostředí nemusí být stejně výkonné jako prostředí produkční, avšak dostačují pro simulaci reálné zátěže či testování.

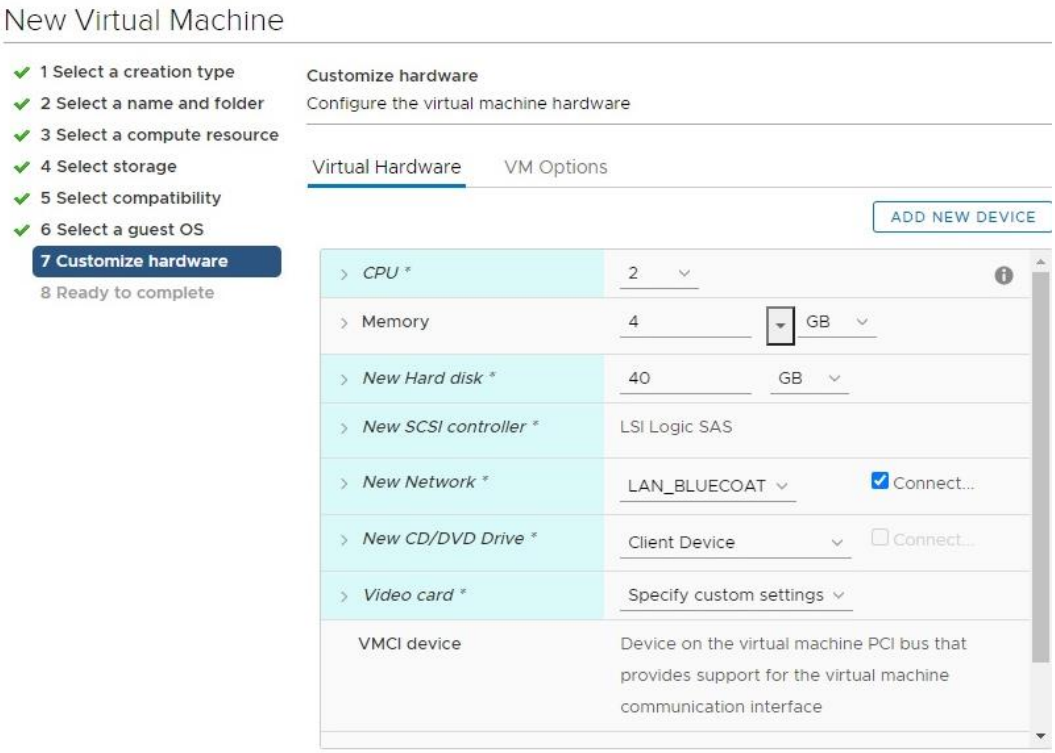
Po úspěšné instalaci hypervizora na fyzický či virtuální server, přistupujeme k jeho rozhraní pomocí IP adresy. K přihlášení je zapotřebí administrátorský účet. Pokud podnik disponuje přídavným úložným prostorem jako například diskové pole nebo má již vytvořenou strukturu serverů v podobě clusteru, je zapotřebí tyto komponenty přidat do administrace ve vSphere. Při vytváření nového virtuální stroje si uživatel určí, kam bude umístěn. Pro naší demonstraci budeme vkládat nový virtuální server již do existujícího serverového clusteru.



Obrázek 14 - Struktura virtuálních serverů
Zdroj: Autor

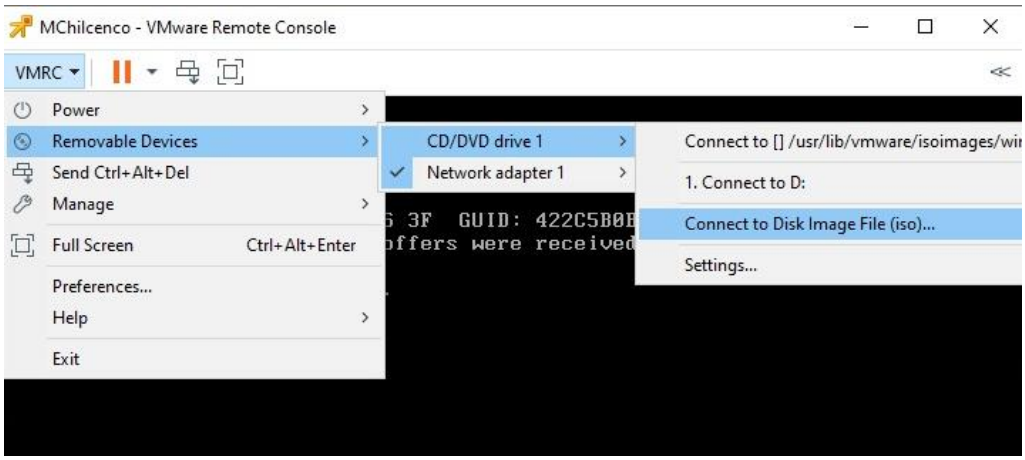
Uživatel bude mít na vybranou hned z několika možností. Zdali se bude jednat o stroj nový, zkopírovaný již z existujícího serveru, či vložený v podobě předkonfigurovaného vzoru. Po upřesnění umístění a přidělení úložného prostoru z lokálního, či přídavného uložiště, bude uživatel vyzván k selekci operačního systému. Pro naší demonstraci bude použita verze OS Microsoft Windows Server 2019 (64-bit).

Virtuálnímu stroji lze přidělit parametry jako například počet procesorů, RAM paměť či úložný prostor na základě dostupných zdrojů serveru, na kterém virtualizace právě probíhá.



Obrázek 15 - Přidělování parametrů virtuálnímu stroji
Zdroj: Autor

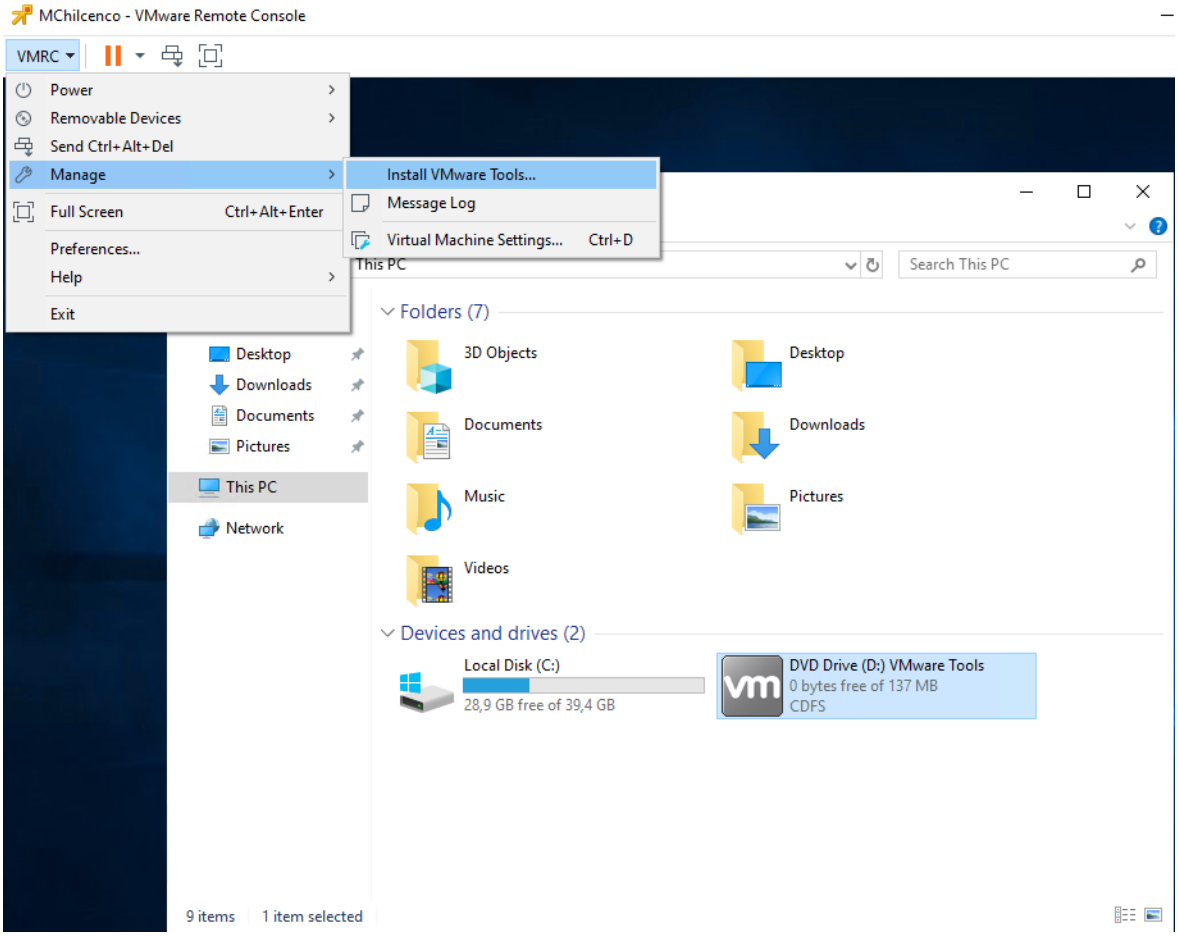
Po úspěšném vytvoření virtuálního serveru lze stroj spustit. Ovládaní serveru se nachází v administraci vShpere. K virtuálnímu stroji přistupujeme skrz remote konzoli. Při instalaci operačního sytému bude uživatel potřebovat ISO soubor operačního sytému. Pomocí zvolené cesty z lokálního či virtuálního uložiště uživatel zvolí ISO soubor a relaci restartuje za pomocí kláves CTRL + ALT + DELETE.



Obrázek 16 - Připojení ISO souboru k virtuálnímu stroji
Zdroj: Autor

Po úspěšné obnově relace dojde k instalaci OS serveru. Instalace probíhá v základním postupu jako při instalaci běžného systému Windows. Při instalaci je zapotřebí zvolit, zdali se bude jednat o desktop či datacentrum variantu. Pro zajištění plynulého chodu a komptability dalších funkcí musí uživatel nainstalovat na virtuální stroj

doplněk nazývaný VMware Tools. Tento krok zajistí plynulý chod virtuálního stroje a doinstalování potřebných ovladačů.

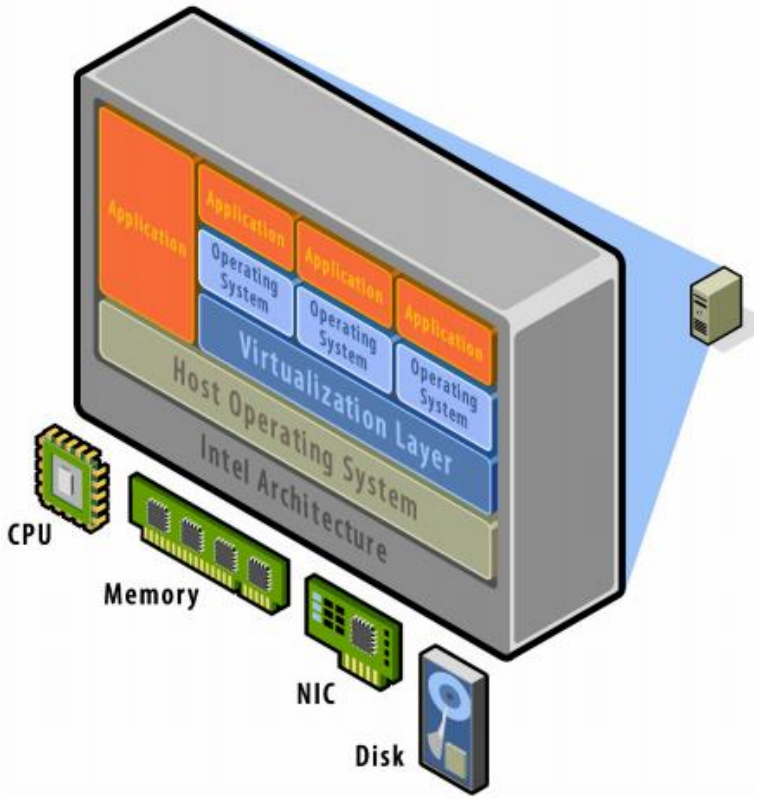


Obrázek 17 - Instalace VMware Tools
Zdroj: Autor

Nyní má uživatel připravený virtuální stroj k používání. Další kroky při konfiguraci virtuálního stroje jsou již subjektivní. Hlavní roli hraje účel virtuální stroje, k čemu se bude využívat a jaké služby podporovat. Uživatel ovšem nesmí zapomenout na zabezpečení virtuální stroje hned po jeho instalaci. To znamená přidání do domény, nastavení proxy serveru či stáhnutí a nainstalování příslušného antivirového programu.

4.6. Postupy a metody při zabezpečení virtuálního stroje

Důležitým aspektem při zabezpečování virtuálních strojů či samotné virtualizace je schéma zapojení a provozování této technologie. Pokud je hypervizor nainstalován přímo na hardwaru fyzického stroje, bez jakéhokoliv operačního systému, je zranitelnější, než pokud by fungoval v operačním systému. Firma VMware doporučuje toto schéma zapojení, viz obrázek č. Obrázek 18 - Schéma zapojení virtualizace doporučována firmou VMware., abychom preventivně odvrátili základní typy útoku a zároveň zajistili plynulý chod virtualizace.



Obrázek 18 - Schéma zapojení virtualizace doporučována firmou VMware
Zdroj: http://www.cpd.iit.edu/netsecure08/ROBERT_RANDELL.pdf

Mezi základní kroky k zabezpečení virtuálního stroje a celé virtualizace patří oddělení řídicí jednotky, tzn. servis konzole nebo vSphere od prostředí, kde je provozována virtualizace. Útočník by se musel dostat k samotnému virtuálnímu stroji a až pak k řídící jednotce.

Pokud máme oddělenou řídcí jednotku, můžeme přistoupit k samotné segmentaci. To znamená rozdělit síť na menší části a každou z nich jedinečně zabezpečit. U tohoto kroku lze použít virtuální segmentaci, kterou hypervizor VMware nabízí, nebo lze použít jiné komerční nástroje například Blue Lane atd.

Nyní můžeme přistoupit k zabezpečení virtuálního stroje. Po vytvoření virtuálního stroje je nezbytné, aby administrátor přidal virtuální jednotku do příslušné domény. Dále na základě vnitřních pravidel infrastruktury nastavil proxy server, DNS server a nainstaloval antivir či nakonfiguroval firewall. Nesmíme zapomínat, že virtuální stroj musíme taktéž chránit, jako by to byl stroj fyzický. Útočníkovi je jedno o jaký stroj se bude jednat, zdali fyzický či virtuální. Zajímají ho především data obsažené na stanici.

Opět zde nesmí chybět delegování oprávnění. Udělujeme taková oprávnění, která jsou nutná. To znamená, není zapotřebí dávat obyčejnému uživateli, který bude přistupovat na virtuální stroj za účelem každodenní správy, vyšší oprávnění než potřebuje. S vyššími oprávněními opět stoupá zodpovědnost, protože tyto účty jsou častým cílem při napadení.

Veškerá komunikace a data, která putují skrz tuto jednotku, by měla být zašifrována. Máme na mysli komunikaci s ostatními servery a data uložená na serveru.

5. Výsledky a diskuse

Pokud budou shrnuta veškerá data, která bakalářská práce obsahuje, lze docílit odpovědi, zdali se vyplatí zavádět či provozovat virtualizační technologií. Bylo docíleno všech stanovených cílů, jak hlavních, tak i dílčích, které si bakalářská práce stanovila. Při provádění finančního porovnávání v našem modelovém příkladu jsme zjistili, že provozování fyzické varianty vyjde o 58 % nákladnější než při variantě virtuální. Tento aspekt je klíčový při rozhodování, zdali se vyplatí zavádět a používat tuto technologii. Nebereme v potaz samotné zvýšené náklady na provoz, chlazení, údržbu a nutnost dokupování dalšího hardwaru při rozšiřování infrastruktury.

V teoretické části byly shrnuty veškeré poznatky o této technologii a o jejích hypervizorech. Byla shrnuta témata jako hypervizor, konsolidace a typy virtualizací. Dále byla dopodrobna rozebrána tématika, proč se vyplatí virtualizovat, jaké k tomu máme důvody a nakonec hmotné či nehmotné přínosy této technologie. V teoretické části je taktéž obsaženo, proč je virtualizace tak důležitá z pohledu kybernetické bezpečnosti, jakou má v tomto IT sektoru roli, úvod k tomuto odvětví, zásady kybernetické ochrany a využití VMwaru v kybernetické bezpečnosti. Kybernetická bezpečnost je s virtualizací úzce spjatá již od počátku. Tato technologie umožnuje zabezpečení celkové vnitřní infrastruktury podniku a zároveň dodává další stupeň bezpečnosti jako takové. Pokud budou dodrženy všechny zásady a postupy, které bakalářská práce uvádí, lze docílit kvalitně zabezpečené informační infrastruktury a zároveň ochrany před možnými útoky. Dobře zabezpečená infrastruktura je klíčovým aspektem k docílení stabilního chodu podniku. Je nepřípustné jen reagovat na vzniklé bezpečnostní incidenty, je důležité se preventivně chránit a brát v potaz veškeré bezpečnostní rizika k docílení maximální bezpečnosti. Na otázku, který hypervizor je nejlepší a jaký si má uživatel vybrat, neexistuje jednoznačná odpověď. Z historie víme, že firma VMware s jejím hypervizorem značně dominovala po velmi dlouho dobu. Ovšem nesmíme zapomínat na dnes již prosperující hypervizor Hyper-V od firmy Microsoft a také Citrix, kteří dnes rovněž konkurují. Každý hypervizor má něco, co druhý nemá a zároveň má své nedostatky. Proto je tato otázka velmi subjektivní a závisí čistě na uživateli či podniku, pro který produkt se rozhodne.

V praktické části bakalářské práce byly shrnuty veškeré metody a postupy spojeny s touto technologií. Máme na mysli vytvoření virtuálního stroje, jeho správa na denní bázi, konfigurace, možnosti zapojení a rovněž seznámení s testovacím prostředím. Po vytvoření virtuálního stroje je nezbytnou součástí ho zabezpečit a tím zamezit možnosti vzniku bezpečnostního incidentu. Zavedení virtualizační technologie do vnitropodnikové infrastruktury není vůbec jednoduchý krok, jak se na první pohled může zdát. Toto rozhodnutí musí být řádně promyšleno. Pokud se ovšem se rozhodném pro tuto této technologie je důležité provést analýzu stávající infrastruktury, rozvržení a naplánování budoucích virtuálních strojů a strojů, které mají zůstat ve fyzické formě. Díky kalkulaci podnik dostane korektní odpověď, zdali se mu vyplatí zavádět a provozovat tuto technologii.

5.1. Klady a zápory virtualizace

Virtualizace přináší možnost dynamického rozvoje a způsobu spravování vnitropodnikové infrastruktury. Možnost migrace serverů v reálném čase či správného rozvržení podnikové zátěže umožnuje stabilní chod, vysokou dostupnost či rychlý rozvoj

podniku. Výměnu hardwaru nebo vnitropodnikové změny lze provádět za chodu, bez nutnosti vypínání strojů. Díky testovacímu prostředí, které virtualizace nabízí, lze vkládat již otestované produkty či služby. Například administrátor v podniku si může založit nový virtuální stroj, nakonfigurovat bez časové tísně dle potřeb a v reálném čase migrovat a následně nasadit do plného chodu bez nutnosti jakýchkoliv omezení provozu.

Další výhodou virtualizace je i její finanční přínos. Nejedná se o žádný zisk, ale o ušetřené náklady na provozu, která tato technologie přináší. Virtualizace umožnuje konsolidace serverů, lépe využívat podnikové zdroje a vylučuje nutnost nákupu zbytečného hardwaru. Díky konsolidaci lze vynaložit menší náklady za správu a chod hardwaru, chlazení, prostory, personál, licence a mnoho dalších.

Virtualizace umožnuje centralizovaně spravovat všechny části IT infrastruktury. Za pomocí správného rozvržení virtuálních strojů lze regulovat zátěž, tím zajistit prevenci vůči výpadkům, vysokou dostupnost služeb a možnost zabezpečení. Virtualizace aplikací přináší i centralizovanou správu pro podniky. Všechny aplikace mohou být nainstalovaný na jednom místě, odkud jsou pak spuštěny. Tímto lze zajistit menší zátěž provozu či nutnost obsluhy každé stanice jednotlivě. Aplikace se aktualizují v jednom centrálním adresáři.

Nevýhodou této technologie je nutnost velké počáteční investice při zavádění. Na začátku je zapotřebí vynaložit velké částky za nákup licencí, podpory a dalších nákladů spojených s touto technologií. Rovněž je zapotřebí reorganizace infrastruktury při zavádění virtualizačních technologií. Tento krok může být taktéž finančně náročný.

6. Závěr

Hlavním cílem bakalářské práce bylo představit a následně demonstrovat užití virtualizační technologie z pohledu kybernetické bezpečnosti. Uvést a zhodnotit klady této technologie, představit kybernetickou bezpečnost a následně demonstrovat realizaci za pomocí hypervizoru VMware.

Teoretické poznatky a problematika spojena s touto technologií jsou shrnuty v jednotlivých kapitolách bakalářské práce. Postupně byly rozebrány veškeré aspekty a přínosy této technologie a zároveň uvedená doporučení a postupy, jak s touto technologií zacházet. Autor si pro tuto bakalářskou práci zvolil jako hlavní nástroj pro demonstraci této technologie hypervizor VMware. Autor je si plně vědom, že se najde značný počet čtenářů, kteří budou s tímto hypervizorem nesouhlasit a budou preferovat raději užití konkurenčního produktu. Volba hypervizora je velmi subjektivní téma, uživatelé mají rozdílné preference. Teoretická část bakalářské práce obsahuje poznatky spojené s touto technologií, dále přestavuje IT sektor pod názvem kybernetická bezpečnost a v závěru demonstruje samotné užití a přínosy této technologie z pohledu kybernetické bezpečnosti. Čtenáři bakalářské práce mohou taktéž narazit na metody a postupy, které jsou zde obsaženy. Tyto nástroje slouží k zabezpečení vnitřní infastruktury a měly by být každodenně dodržovány, v důsledku docílení maximální efektivnosti. Pokud budou absolvovány všechny bezpečnostní kroky, lze docílit maximálně zabezpečeného celku. Bezpečnost je v dnešní době velmi důležitá. Spousta uživatelů si neuvědomuje, jak jednoduché je přijít o svá data. Podniky by měly brát větší ohled, nepodceňovat tyto typy hrozeb a preventivně se chránit proti všem možným typům útoků. Reagovat na již vzniklé bezpečnostní incidenty nestačí!

V praktické části je realizován vlastní návrh řešení, který danou problematiku demonstruje. Byl uveden postup, kterým by se měl podnik řídit pří zavádění této technologie do vnitropodnikové infrastruktury a kroky spojené s tímto úkonem. Bakalářská práce obsahuje analýzu infrastruktury, taktéž finanční porovnání fyzické a virtuální varianty řešení, možnosti zapojení, představení testovacího prostředí a samotné vytvoření a zabezpečení virtuálního stroje pomocí technik a postupů používané v kybernetické bezpečnosti.

7. Seznam použitých zdrojů

Knižní zdroje

1. RUEST Danielle, RUEST Nehlson, *Virtualizace – podrobný průvodce*, 1. vydání, Computer Press a.s. 2010, ISBN 978-80-251-2676-9

Internetové zdroje

2. Virtualnipc.cz [online], *Úvod do virtualizace na desktopu* [cit. 2020-08-04] Dostupné z: https://www.virtualnipc.cz/vmware-workstation-uvod-do-virtualizace-na-desktopu-1875

3. Businessworld.cz [online], *Co je to virtualizace* [cit. 2020-08-15] Dostupné z: https://businessworld.cz/ostatni/co-je-to-virtualizace-7158

4. Azure.microsoft.com [online], *Virtual Machines* [cit. 2020-08-15] Dostupné z: https://azure.microsoft.com/cs-cz/services/virtual-machines/

5. Interval.cz [online], *Virtualizace – mýtus, kouzlo, hype nebo realita?* [cit. 2020-08-15] Dostupné z: https://www.interval.cz/clanky/virtualizace-mytus-kouzlo-hype-nebo-realita/

6. Beranr.webzdarma.cz [online], *Virtualizace operačních systémů* [cit. 2020-08-23] Dostupné z: http://beranr.webzdarma.cz/virtualizace.html#litVirtualizaceServeru

7. Fi.muni.cz [online], *Virtualizace* [cit. 2020-08-24] Dostupné z: https://www.fi.muni.cz/~kas/pv090/referaty/2016-podzim/virt.html#cast1, https://www.fi.muni.cz/~kas/pv090/referaty/2016-podzim/virt.html#cast2

8. Ibm.com [online], *IBM and HP virtualization* [cit. 2020-09-02] Dostupné z: https://www.ibm.com/developerworks/aix/library/au-aixhpvirtualization/index.html

9. Systemonline.cz [online], *Virtualizace IT* [cit. 2020-09-06] Dostupné z: https://www.systemonline.cz/virtualizace/virtualizace-it.htm

10. Kvalitninavody.cz [online], *10 Důvodů proč virtualizovat* [cit. 2020-09-06] Dostupné z: https://www.kvalitninavody.cz/10-duvodu-proc-virtualizovat/

11. Alliancetechpartners.com [online], *How Virtualization Helps Save Money and Increase Efficiency* [cit. 2021-09-24] Dostupné z: https://www.alliancetechpartners.com/virtualization-can-help-save-money-increase-efficiency/

12. Eukhost.com [online], *VMware ESX vs. VMware ESXi Functionalities* [cit. 2021-10-11] Dostupné z: https://www.eukhost.com/kb/vmware-esx-vs-vmware-esxi-functionalities/

13. Vmware.com [online], *VMware vSphere with Operations Management and VMware vSphere* [cit. 2021-10-21] Dostupné z: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/vmware-vsphere_pricing-white-paper.pdf

14. Microsoft.com [online], *Hyper-V overview* [cit. 2021-10-24] Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831531(v=ws.11)?redirectedfrom=MSDN

15. Xenproject.org [online], *Xenproject - history* [cit. 2020-10-24] Dostupné z: http://www.xenproject.org/about/history.html

16. Vmware.com [online], *Zásady kybernetické hygieny* [cit. 2020-10-26] Dostupné z: https://blogs.vmware.com/emea/cs/2019/04/zasady-kyberneticke-hygieny/

17. Nukib.cz [online], *Kybernetická bezpečnost* [cit. 2020-10-26] Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/

18. Kybez.cz [online], *Kybernetická bezpečnost* [cit. 2020-11-09] Dostupné z: https://www.kybez.cz/o-nas1

19. Iso.cz [online], *ISO 27001* [cit. 2020-11-09] Dostupné z: http://www.iso.cz/iso-27001

20. Egovernment.cz [online], *Datové centrum není bezpečnostní výprodej* [cit. 2020-11-11] Dostupné z: https://www.egovernment.cz/soubor/datove-centrum-neni-bezpecnostni-vyprodej-o-ciz-vmware/

21. Vmware.com [online], *VMware vSphere Compute Virtualization -Licensing, pricing and packaging* [cit. 2021-01-29] Dostupné z: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vsphere/vmware-vsphere-pricing-whitepaper.pdf

22. Vmware.com [online], *VMware Infrastructure 3 - Pricing, Packaging and Licensing Overview* [cit. 2021-01-29] Dostupné z: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vi_pricing4.pdf

Ostatní zdroje

23. Interní materiály MSP