UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Problematika bezpečnosti cloud computingu

Bc. Evžen Mynka

Diplomová práce
2013

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2012/2013**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Evžen Mynka**
Osobní číslo:	**I11394**
Studijní program:	**N2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Problematika bezpečnosti cloud computing**
Zadávající katedra:	**Katedra softwarových technologií**

Zásady pro vypracování:

Cílem práce je poukázat na problematiku bezpečnosti v technologiích Cloud computig. Autor představí přístupy a řešení nejvýznamnějších technologií cloud comuping od IBM, VMware a Microsoft a představí různorodost pojetí této problematiky. Na základě tohoto zhodnocení a provedené rešerše, autor navrhne metodiku pro odhalování bezpečnostních rizik spojených s nasazováním technologií cloud. Tuto metodiku ověří v laboratorním prostředí, které bude simulovat prostředí firmy využívající technologie cloud computing a na základě získaných dat provede optimalizaci navržené metodiky.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

HALPERT, B. Auditing Cloud Computing: A Security and Privacy Guide. 1. [s.l.] : John Wiley and Sons Ltd, 2011. 206 s. ISBN 9780470874745. WINKLER,, V. (J. R.) ; SPEAKE, G.; FOXHOVEN, P. Securing the Cloud: Cloud Computer Security Techniques and Tactics. 1. [s.l.] : Syngress Media,U.S., 2011. 314 s. ISBN 9781597495929. KRUTZ, R. L.; VINES, R.D.; BRUNETTE, G. Cloud Security: A Comprehensive Guide to Secure Cloud Computing . 1. [s.l.] : John Wiley & Sons Ltd, 2010. 284 s. ISBN 9780470589878.

Vedoucí diplomové práce: **Mgr. Josef Horálek**
Katedra softwarových technologií

Datum zadání diplomové práce: **31. října 2012**
Termín odevzdání diplomové práce: **17. května 2013**

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

prof. Ing. Antonín Kavička, Ph.D.
vedoucí katedry

V Pardubicích dne 15. listopadu 2012

Prohlášení autora

Prohlašuji, že tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1. autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 12. 2. 2013 Evžen Mynka

Poděkování

Tímto bych chtěl především poděkovat vedoucímu této diplomové práce Mgr. Josefu Janu Horálkovi. Obzvláště za spolupráci, věnovaný volný čas, trpělivost, cenné rady a připomínky při tvorbě této diplomové práce. Také bych rád poděkoval všem, kteří mně během studia podporovali a byli mně oporou. Dále bych chtěl poděkovat Fakultě elektrotechniky a informatiky Univerzity Pardubice za poskytnutí laboratorních prostor umožňujících vytvoření této práce.

Anotace

Tato diplomová práce se zabývá technologií v oboru informační technologie, kterou začíná využívat, respektive již využívá převážná část světových společností. Touto technologií je cloud computing. Tato práce si v první části klade za cíl seznámit čtenáře s danou technologií z historického hlediska, definovat hlavní přístupy a pojmy. Další část práce se zaměřuje zejména na problematiku týkající se jak bezpečnosti, tak i bezpečnostních rizik spojených s danou technologií. Jsou zde představeny jak jednotlivé hrozby, tak i techniky, které tyto hrozby dokáží eliminovat. V další části práce jsou představeny nabízené produkty tří vybraných společností, jimiž jsou Microsoft, IBM a VMware. V závěru je popsán proces nasazení cloud computingu v laboratorním prostředí, jsou zhodnocené dosažené výsledky a navrženy možné metody optimalizace.

Klíčová slova

cloud computing, bezpečnost dat, virtualizace, IaaS, PaaS, SaaS, ISO, IBM, VMware, Microsoft

Title

The Issues of Cloud Computing Security

Annotation

The intent of this thesis is to address the information technology concept known as cloud computing. This technology is being adopted or is already widely used by the majority of the market leaders around the world. Purpose of the first part of the thesis is to describe cloud computing in the historical context and define terms and main approaches. Next part is focused on security and security risks associated with given technology. Individual threats are being discussed as well as techniques on how to mitigate them. Next subject introduces products of the three leading companies – Microsoft, IBM and VMware. Conclusion describes implementation process of cloud computing in the laboratory environment; the results are evaluated and optimization methods are being proposed.

Keywords

cloud computing, data security, virtualization, IaaS, PaaS, SaaS, ISO, IBM, VMware, Microsoft

Obsah

Seznam zkratek

IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
IBM	International Business Machines
ISP	Internet Service Provider
API	Application Programming Interface
SLA	Service Level Agreement
CPU	Central Prosessing Unite
LPP	Least Privilaged Principal
RBAC	Role-Based Access Controls
SSO	Single-Sign-On/Single-Sign-Off
DLP	Data Leakage Provention
IDS	Intrusion Detection Systém
IPS	Intrusion Prevention Systém
PKI	public key infrastructure
MPLS	Multiprotocol Label Switching
VPN	Virtual Private Network
SSH	Secure Shell
TLS	Transport Layer Security
SSL	Secure Sockets Layer
ITIL	Information Technology Infrastructure Library
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ICT	Information and Communication Technology
ISMS	Information Security Management Systems

PDCA	Plan, Do, Check, Act
SAS	Statement of Auditing Standard
FISMA	Federal Information Security Management Act
NSA	National Security Agency
SQL	Structured Query Language
MSDN AA	Microsoft Developer Network Academic Alliance
CCNA	Cisco Certified Network Associate
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
VLAN	Virtual Local Area Network
SDM	Security Device Manager
IIS	Internet Information Server
MAC	Media Access Control
CD	Compact Disk

Seznam obrázků

Seznam tabulek

1 Úvod

Cloud computing spolu s virtualizací tvoří technologie, které ještě v nedávné době byly dostupné pouze pro obrovské nadnárodní společnosti. V dnešní době se tento trend mění a tyto technologie jsou přístupné i pro středně velké a menší podniky. Velmi častou chybou ovšem je vzájemná záměna těchto pojmů a dále strach z použití cloud computingu, který velmi často pramení z neznalosti a z nedůvěry v novou technologii. Cílem této diplomové práce je seznámení veřejnosti s touto technologií a následně poukázat na její silné a slabé stránky z pohledu bezpečnosti.

Tato diplomová práce se skládá ze šesti základních částí. V první z nich definuji termín cloud computing, charakterizuji jeho základní vlastnosti a představím způsob, dle kterého můžeme celý tento koncept členit do patřičných kategorií. Dále budou představeny technologie, které ke cloud computingu neodmyslitelně patří a které tvoří základní pilíře celého cloudu. Nedílnou součástí této kapitoly je snaha poukázat na hlavní společné, respektive rozdílné vlastnosti a způsoby využití jednotlivých technologií. Závěrem je ucelení jednotlivých pojmů.

Druhá část je zaměřena na rizika, která s sebou daná technologie přináší. Tato rizika jsou vybrána s ohledem na různorodost požadavků na cloud computing a na typ služeb, které daná technologie přináší. Hlavní důraz je kladen především na vyčlenění hrozeb spojených s důvěrnosti, dostupností a integritou dat v cloudu.

Třetí část této práce je zaměřená na eliminaci rizik vyčleněných v předchozí kapitole. Jsou zde navrhnutá řešení jak pro jednotlivé model cloudových služeb, tak i pro jednotlivé modely nasazení cloudu. Důležitou součástí je popis funkce bezpečnostních norem a auditů. V neposlední řadě jsou v této kapitole uvedeny povinnosti jednotlivých zúčastněných stran (zákazník a poskytovatel služby).

Ve čtvrté části jsou představeny přístupy a řešení nabízené třemi významnými společnostmi poskytujícími danou technologii. Je zde uveden rozbor jednotlivých nabízených technologií daných společností následovaný jejich hodnocením.

V následující kapitole je popsána tvorba bezpečnostního auditu, který má za účel odhalit co nejvíce chyb a úskalí při nasazování cloud computingu do reálného provozu. Účelem tohoto auditu je usnadnit a především zajistit bezpečný chod dané technologie. V další části této kapitoly je popsán proces nasazení technologie cloud v laboratorním prostředí.

V závěrečné části jsou shromážděny poznatky nabyté během zhotovování této diplomové práce, zhodnoceny výsledky, dosažené úspěchy a naznačený směr, kterým by mohla tato práce dále směřovat.

K práci mě motivoval především můj vztah k informačním technologiím, který se váže hlavně na síťové odvětví a jeho bezpečnost, chuť se v tomto zaměření i nadále

zdokonalovat, popřípadě se tomuto oboru věnovat i v následující kariéře. Dalším důvodem této volby byla chuť zlepšit si přehled týkající se dané problematiky, obzvláště s ohledem na tempo, kterým se v dnešní době tato technologie dostává do popředí.

2 Cloud computing

Cloud computing je technologie jejíž název se stal velice oblíbeným marketingovým spojením v IT. Ovšem jen málo kdo dokáže přesně vysvětlit, co se pod tímto pojmem skrývá. Samotný název vychází ze symbolu mraku (anglicky Cloud). Tento symbol je často používán v různých diagramech pro znázornění internetu a všech zdrojů, které poskytuje. Zjednodušeně lze říci, že se jedná o poskytování služeb, respektive prostředků třetích stran, prostřednictvím internetu. Tyto prostředky mohou být jak softwarové tak i hardwarové.

Jak například uvádí [1] a [2] jedním z hlavních důvodů dnešní popularity cloud computingu je jeho přístupnost a jednoduchost použití. Uživatele nemusí zajímat kde, nebo na čem daná služba běží. Postačí mu pouze zajistit připojení k internetu a bezpečný přístup ke službě, kterou chce využívat. Vzhledem k dostupnosti a rychlosti internetu, jednoduchosti přístupu ke službě a uživatelsky jednoduché správě dat, si stále více firem tyto benefity uvědomuje a začínají cloudové služby využívat. Tento krok firmám výrazným způsobem šetří prostory spolu s náklady, a to jak na infrastrukturu, energie, technickou podporu a údržbu. Dle výše uvedených zdrojů patří mezi další nesporné výhody cloudu i fakt, že uživatel nemusí vlastnit výkon na svém stroji. Sdílením prostředků lze dosáhnout požadovaného výkonu za mnohem nižší cenu.

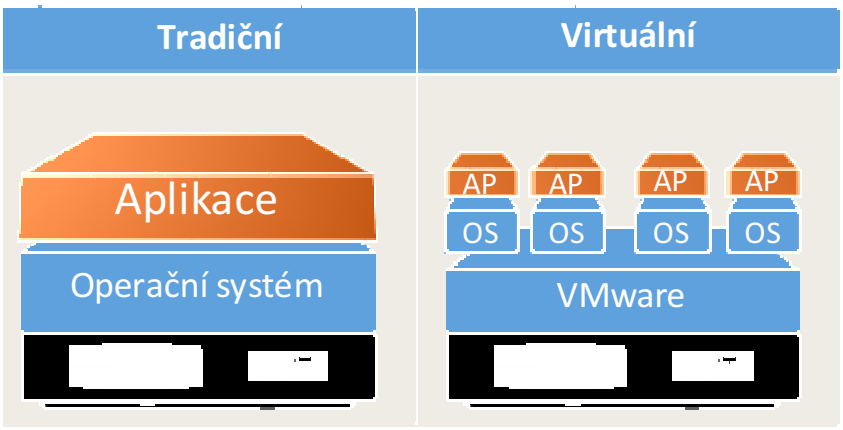
Ovšem dříve, než se dále budeme věnovat cloud computingu je potřeba si definovat podpůrnou technologii, bez které by cloud computing nemohl existovat. Touto technologií je virtualizace. Bez ní by nebylo možné poskytnout služby na bázi cloud computingu. Virtualizace nám zajišťuje realizaci dvou základních vlastností cloud computingu a to „resource pooling“ a „rapid elasticity“ [3]. Těmto vlastnostem se v této diplomové práci budu věnovat podrobněji v kapitole 2.4.

2.1 Virtualizace

Technologie virtualizace je s cloud computingem úzce spjatá. S mírnou nadsázkou by se dokonce dalo tvrdit, že bez virtualizace by cloud computing nebylo možné provozovat. Pojem virtualizace zavedla firma IBM už v 60. letech 20. století. Hlavním důvodem byla snaha rozložit výpočetní výkon mainframů[1] do více virtuálních strojů. Do té doby totiž mainframe mohl současně zpracovávat pouze jeden proces, čímž docházelo k nedostatečnému využití hardwaru a k plýtvání zdroji. Tento trend byl využíván až do 80. let, kdy byl vytvořen model klient-server. Následkem toho virtualizace přestala být potřebná. Ovšem s dalším vývojem technologie v oboru IT se vyskytly nové problémy jako nedostatečně malá ochrana před výpadkem, rostoucí náklady na údržbu, využití zdrojů, atd. Jako vhodné řešení těchto problému se ukázalo opětovné nasazení virtualizace [4].

[1] Mainframe je počítač využívaný ke zpracování velkého objemu dat. Většinou se jedná o sálové počítače s velkou spolehlivostí a bezpečností.

Pod pojmem virtualizace se v dnešním světě rozumí vytváření abstraktní vrstvy mezi hardwarem a softwarem, který nad tímto hardwarem běží. To nám umožňuje na této vrstvě vytvořit skupinu virtuálních strojů, které se na venek chovají jako stroje fyzické. Zjednodušeně lze říct, že si v jednom počítači vytvoříme skupinu počítačů (viz. obrázek 1). Tyto virtuální stroje mohou být navzájem nezávislé na typu operačního systému, architektuře a na připojeném hardwaru [5]. Toto je však jen jeden z mnoha typů virtualizace. Další typ virtualizace, který využívá každý z nás, je reprezentován virtuální pamětí počítače. Jedná se o proces, kdy počítač k alokaci paměti využívá jak paměť RAM, tak i část pevného disku. Nám, jakožto uživatelům, se však tato paměť jeví jako souvislá. Této metodě odkládání části dat z RAM na pevný disk se říká swapping.



Obrázek 1 - Princip virtualizace (Autor – upraveno dle: [4])

Mezi hlavní důvody, které vedly ke znovupoužití virtualizace patřit zejména nárůst výkonu hardwaru a procesní paměti [1]. Znovuzavedení virtualizace se v dnešní době ukazuje jako jeden z klíčových kroků, který zejména velkým firemním infrastrukturám otevírá nové možnosti.

Jak uvádějí zdroje [5] a [6], mezi hlavní přínosy virtualizace může patřit:

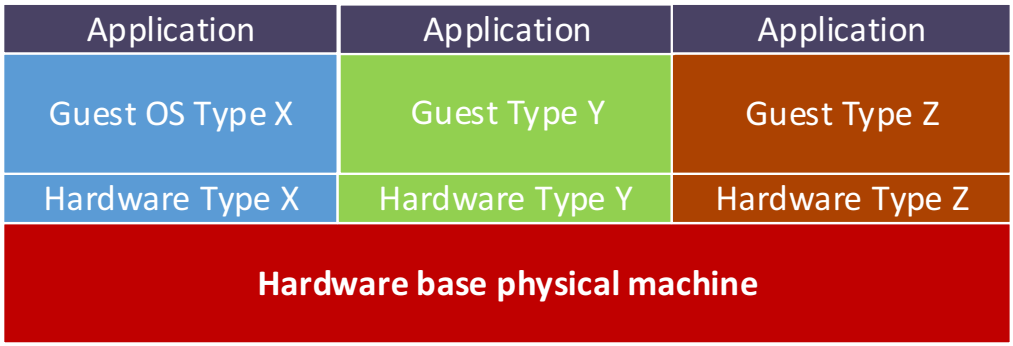
- Lepší využití hardwarových zdrojů
- Lepší bezpečnost a dostupnost
- Škálovatelnost
- Snížení nákladů na řízení a zdroje

Vzhledem k rozsáhlosti a náročnosti tématiky dané technologie, zde budou představeny jen vybrané vlastnosti a jejich základní popis. Dále bych chtěl uvést, že podrobný rozbor virtualizace není účelem této diplomové práce.

2.1.1 Emulace

Obrázek 2 si klade za cíl znázornit princip emulace. Ten, spočívá v překladu strojových instrukcí hostovaného sytému na strojové instrukce hostitelského systémem. Tento proces je ale velice pomalý a neefektivní. I přes svou výkonnostní nevýhodu má toto řešení jedno positivům. Jedná se totiž o jediný způsob, jakým lze na libovolné platformě spustit systém a aplikace libovolné jiné platformy. Dokonce lze emulovat mnoha procesorový stroj na jednoprocesorovém počítači. Emulace je často využívaná například vývojáři, kteří si takto mohou na svých počítačích otestovat aplikace, navržené kupříkladu pro mobilní telefony [7]. Mezi nejznámější emulátory dle [6] patří QEMU a BOCHS.

Na závěr této kapitoly bych ještě rád upozornil na rozdíl mezi termíny emulace a simulace. Simulace je v oblasti IT chápána jako výzkumná technika, u níž je cílem experimentu získání nových informací o simulovaném systému [8]. Naproti tomu cílem emulace je zajištění funkcionality určitého systému za pomocí jiných prostředků.



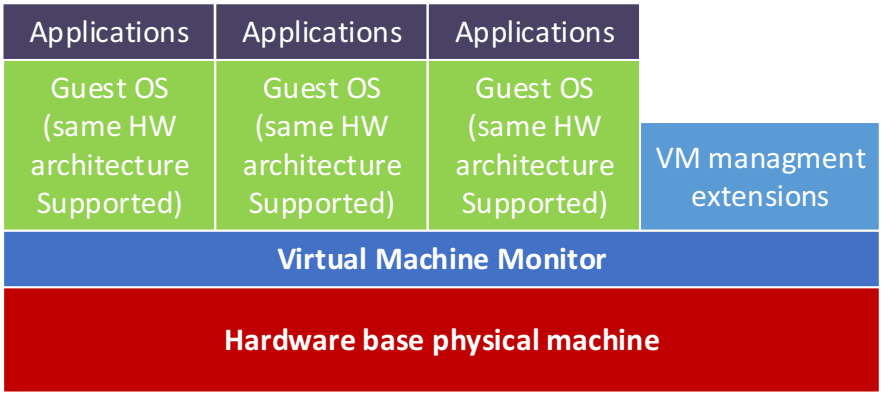
Obrázek 2 - Emulace (Autor - upraveno dle: [7])

2.1.2 Úplná virtualizace

Úplná virtualizace[2] nám zajišťuje stav, kdy operační systém běžící na virtuálním serveru nemůže žádným způsobem poznat, že nemá přístup k fyzickému HW. Samotný operační systém, ani na něm běžící aplikace nevyžadují žádné modifikace. Mezi výhody tohoto řešení patří nezávislost aplikací na hardwaru (jeho výměna nemá na běžící aplikace vliv) a možnost přidělit prostředí tolik prostředků, kolik je v dané situaci potřeba. Nevýhodou této metody je značná režie, která je spojená s přístupem virtuálního systému k hardwaru. Úplná virtualizace se uplatňuje při implementaci privátního cloudu, kdy firma virtualizuje vlastní fyzické servery. Tato virtualizace probíhá za účelem snížení provozních, pořizovacích a administrativních nákladů na server. Tento proces je mnohdy

[2] V angličtině také často označovaná jako „native virtualization“.

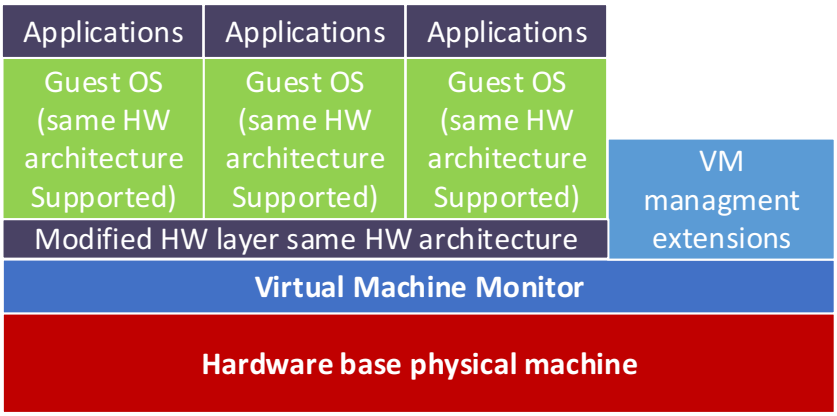
označován jako P2V („Physical to Virtual“). Mezi nejznámější aplikace využívající plnou virtualizaci patří VirtualBox, VMware Player a VirtualPC [5] [6]. Obrázek 3 graficky znázorňuje tento typu virtualizace.



Obrázek 3 - Úplná virtualizace (Autor - upraveno dle: [7])

2.1.3 Paravirtualizace

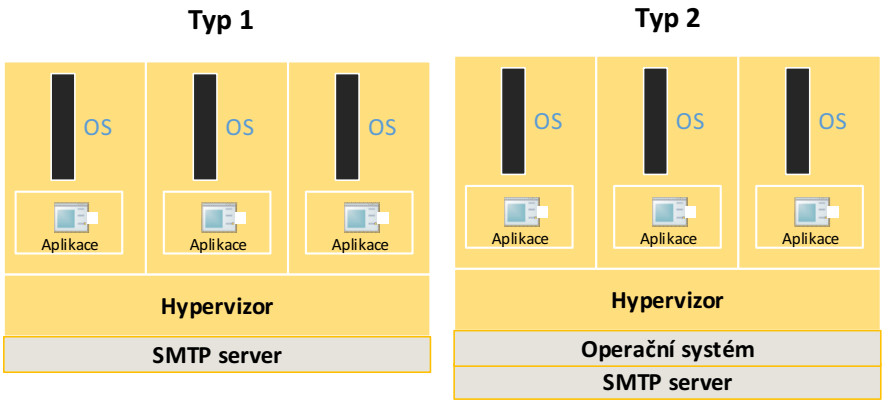
Na rozdíl od úplné virtualizace paravirtualizace nesimuluje kompletní hardware, ale pouze jeho část. Tato volba je vhodná v případě, kdy víme o shodě komponent u fyzického i virtuálního stroje. Díky podobnosti hardwarů obou stran nám paravirtualizace poskytuje lepší výkon než virtualizace úplná [6]. Jinými slovy, nemusíme virtualizovat celý hardware, ale stačí pouze jeho část. Základem tohoto řešení je však upravené jádro hostujícího operačního systému s tzv. hypervizorem. Ten poskytuje hostovaným systémům přístup k hardwaru. Hostované operační systémy jsou také upraveny, protože ví, že nemají přístup k fyzickému hardwaru. Proto svá volání převádí na volání hypervizoru tzv. „hypercall“. Tímto způsobem je odstraněna značná část režie, spojené se vstupně výstupními operacemi. Nevýhodou je ovšem fakt, že tento typ virtualizace nelze použít u systémů, jejichž hardware má různou architekturu. Tento způsob virtualizace nelze uplatnit ani v případě, kdy nám není poskytnutá možnost upravit kód obou stran. Mezi softwary využívající paravirtualizaci patří Microsoft Hyper-V a Xen [5] [9]. Obrázek 4 si klade za cíl ukázka princip paravirtualizace pomocí grafické podoby.



Obrázek 4 - Paravirtualizace (Autor - upraveno dle: [7])

Hypervizor

Dle [10] je tímto pojmem je označována aplikace, která hostovaným operačním systémům poskytuje výpočetní prostředky serveru. Obecně se dá říct, že hypervizor může být dvojího druhu. První typ hypervizoru (levá část obrázku č. 5) se používá při plné virtualizace, kdy je hypervizor instalován přímo na daný server (hardware). Druhým typem je hypervizor, který se používá u paravirtualizace. Jeho grafické znázornění je zobrazeno na v pravé části obrázku č. 5. V tomto případě je mezi hypervizorem a hardwarem serveru další operační systém, který umožňuje běh hypervizoru.



Obrázek 5 - Typy hypervizoru (Autor – upraveno dle: [10])

2.2 Grid computing

Jedná se o další technologií, která je velmi často spojovaná právě s cloud computingem. Mnohdy jsou tyto pojmy vzájemně neprávně zaměňované. Může za to několik společných vlastností obou technologií. Protože se grid computing stále vyvíjí,

neexistuje zatím ustálená definice tohoto pojmu. Proto se zde pokusím spíše popsat hlavní myšlenku dané technologie a poukázat na rozdíly mezi grid a cloud computingem.

Hlavní myšlenou grid computingu je sdílení výpočetních zdrojů nezávislé na geografické lokaci ani typu daného zdroje. Ideologie gridu je taková, že všechna zařízení (PC, notebooky, mobilní telefony, superpočítače) budou sdílet svůj nevyužitý procesorový čas pro řešení jednoho daného, primárně vědeckého problému. Jedním z požadavků je i necentralizované řízení daných zdrojů [11]. V cloud computingu je ovšem providerem centralizované řízení zdrojů žádoucí, ne-li naprosto nezbytné. Další zásadní rozdíl vzniká při ekonomickém pohledu na obě technologie. Zatímco cloud computing je postaven na modelu poskytovatel – zákazník, kde zákazník platí za poskytnuté služby, pak grid computing je rozšířen hlavně v akademické sféře, kde se za poskytnutí prostředků neplatí. Z technologického hlediska je tu ovšem jeden, a to zásadní rozdíl v obou technologiích. Zatímco grid computing se „skládá“ z mnoha na sobě nezávislých výpočetních zařízení, které pracují na dosažení společného cíle. Cílem cloud computingu je poskytnutí výpočetních prostředků pro tyto úkoly, neboli vytvoření požadované infrastruktury [1].

Jako příklad velkých fungujících gridů v dnešní době můžeme uvést program World Community Grig [12] a projekt SETI [13].

2.3 Historie cloud computingu

Začátky cloud computingu sahají až do 60. let 20. století, kdy byly položeny základy virtualizace. Bohužel vzhledem k tehdejší technologii nebylo možné využít výpočetního výkonu mainframu vzdáleně [14]. Tato schopnost nám byla nabídnuta až s příchodem moderních technologií.

První zmínku o cloudu jako takovém vyřkl Joseph Carl Robnett Licklider. V jeho vizi byli všichni propojeni pomocí počítačů, za jejichž pomoci se kdykoli a odkudkoli mohli připojovat k jakýmkoli datům. Tato myšlenka velice přesně vystihuje dnešní pojetí cloud computingu [15].

Další významnou osobností v historii cloudu byl profesor MIT John McCarthy. Jeho publikace z roku 1961 přistupovala ke cloudu jako k obchodnímu modelu. Celý cloud připodobňoval k rozvodu elektrické sítě či rozvodu plynu, kdy velké množství domácností sdílí energii ze vzájemně propojených elektráren. V případě výpadku jedné elektrárny přebírají zátěž ostatní a klient to nikterak nepocítí. Tato myšlenka však byla zapomenuta, protože tehdejší technologické možnosti to nedovolovali. Ovšem na základě této myšlenky vznikl termín „Utility computing“, který se v budoucnosti používal právě pro označení cloud computingu [14].

Samotný termín cloud computing je však daleko mladší. Toto téma začalo být zajímavé až při rozvoji vysokorychlostního internetu. Vznik termínu cloud se připisuje

Ramnathu Chellappovi, který si tento termín zapůjčil od telekomunikačních společností a v roce 1997 ho poprvé použil [16].

Dle zdrojů [1] a [15] byla hlavní průkopnickou společnosti v tomto odvětví firma Amazon, které v roce 2002 poskytla službu Amazon Web Service právě pomocí cloud computingu. Mezi další významné společnosti v současné době patří například IBM, Microsoft, Google a mnoho dalších. A právě těmto společnostem můžeme poděkovat za popularizaci termínu cloud computing.

2.4 Definice

Definovat cloud computing se již pokusilo mnoho odborníků, nikdo však nedošel k jednoznačné definici. Definování cloud computingu je složité kvůli širokému spektru aspektů, které zahrnuje. V poslední době bývá dokonce zvykem spojovat cloud computing s věcmi, se kterými nemá nic společného. Z důvodů nekonzistence pohledů na základní definice a jejich dynamickým vývoji v průběhu psaní této práce, byl zvolen přístup světově uznávané organizace National Institute of Standards and Technology (NIST), která je v této oblasti jedním z hlavních lídrů.

Dle společnosti NIST [3] je cloud computing definován jako model služeb, který „umožňuje okamžitý, snadný a na vyžádání dostupný síťový přístup ke sdílené nabídce konfigurovatelných výpočetních zdrojů (sítě, servery, aplikace a služby), které mohou být v případě potřeby poskytnuty či uvolněny za minimálních administrativních nákladů a potřeby koordinace s poskytovatelem těchto služeb“. Během tvorby této diplomové práce jsem často narážel na odkazy právě na tuto definici a na další materiály spojeny se společností NIST. Z toho usuzuji, že se jedná o obecně platnou a uznávanou definici cloud computingu. Proto z něj v dalších částech své práce budu vycházet i já.

Z této definice je celkem patrný samotný význam cloud computingu, který lze chápat jako nový způsob poskytování počítačových služeb reagující na vyžádání klienta. Jednoduchost přístupu k poskytovaným službám je v dnešní době chápána skrze internetový prohlížeč. Typ služby zde není specifikován. Tudíž se může jednat jak o datové úložiště, jednoduchou aplikaci, ale také o strukturovanou výpočetní síť skupiny počítačů. Bezproblémový chod, monitorování a škálování těchto služeb by měly probíhat bez většího zásahu poskytovatele dané služby.

Dále by mohl být cloud computing chápán jako aplikace či služba, která je dostupná z jakéhokoliv počítače s přístupem k internetu. Typickým zástupcem takové služby je email.

2.5 Obecné vlastnosti

Definice obecných vlastností cloud computingu není jednoduchou záležitostí. Jednou z příčin je složitost, respektive nekompaktnost definice samotného pojmu. To způsobuje odlišný pohled jednotlivých lidí na danou problematiku. O vyčlenění základních vlastností se pokusila společnost NIST, která ve svém dokumentu definuje termín cloud computing, definuje základní vlastnosti a dokonce člení cloud do dvou modelů. Těmito modely jsou model nasazení cloudu a model cloudových služeb, který je také často označován jako distribuční model. Tento dokument se dokonce stal uznávaným širokou odbornou veřejností.

Nyní si představíme základní vlastnosti dle společnosti NIST, které charakterizují podstatu cloud computingu.

- **On-demand self-service** - Volný překlad tohoto výrazu by mohl znít „samoobsluha na vyžádání“ nebo „samoobslužné zadávání požadavků“. Dle zdroje [3] tato vlastnost dovoluje zákazníkovi, aby se sám rozhodl, kdy a které zdroje bude využívat. Typicky se jedná o procesorový čas nebo o využití kapacity na úložišti. To vše bez nutnosti zásahu poskytovatele dané služby. Tento přístup výrazným způsobem zvyšuje flexibilitu dané služby, neboť umožňuje rychle reagovat na měnící se požadavky zákazníků vzhledem k poskytovaným službám.

- **Broad network access** - Broad network access neboli „širokopásmový přistup k síti“. Tím je definován požadavek přístupu ke službám pomocí síťového připojení, a to za použití libovolného klienta a standardního protokolu [3]. Tato vlastnost se úzce dotýká tématu dostupnosti dat v cloudu, která je z pohledu technologie naprosto zásadní.

- **Resource pooling** - Tento termín se dá přeložit buď jako „sdružení prostředků“ nebo jako „sdílení zdrojů“. Tato vlastnost nám říká, že zdroje (jako je výpočetní výkon, atd.) jsou distribuovány mezi jednotlivé zákazníky, kteří sdílí přistup k hardwarovým prostředkům. Ačkoliv jsou tyto prostředky sdíleny, jednotliví uživatelé jsou navzájem izolovaní a jejich data jsou udržována v konzistentním stavu. Uživatel však není schopen zjistit, kde se tyto prostředky nachází. V dokumentu ze společnosti NIST je poukázáno na fakt, že zákazníkům by mělo být umožněno tento fakt ovlivnit. Alespoň na úrovni státu [3]. S tím souvisí geopolitické a právní problémy, kterými se budu zabývat v kapitole 3.2.

Jako příklad sdílení zdrojů můžeme uvést datová úložiště, paměť, procesorový výkon a mnoho dalších.

- **Rapid elasticity** - Tato vlastnost nám z hlediska jak vnitřní, tak i vnější poptávky umožňuje dynamicky měnit přidělené výpočetní zdroje zákazníkům v závislosti na jejich potřebách. Jinak řečeno nám umožňuje přidělovat, odebírat a re-alokovat prostředky pro konkrétní uživatele. Z pohledu zákazníka se zdroje jeví jako nevyčerpatelné. To znamená, že mu mohou být přiděleny kdykoli a v jakémkoli množství. Dále je třeba podotknout, že se od systému očekává provedení požadované změny přidělených prostředků v co nejkratším čase [3].

  Obdobně jako „On-demand self-service“, tak i „rapid elasticity“ zvyšuje celkovou flexibilitu cloudových služeb.

- **Measured service** - Volně přeložena jako „měřitelnost služby“. Protože v cloud computingu je uživateli účtováno pouze za spotřebu daných zdrojů (tento model využití je mnohdy označován jako „Pay as you go“ nebo také „Utility use“[3]), je tato vlastnost zásadní z hlediska ekonomického. Tato vlastnost umožňuje monitoring, kontrolu a report poskytnutých služeb, což umožňuje transparentní pohled na jejich využití. Tento pohled musí být poskytnut jak provideru služby, tak i samotnému zákazníku. Samotná cena se dále odvíjí od typu dané služby a úrovně použité abstrakce [3].

2.6 Uživatelské role v cloud computingu

Dříve, než se začnu věnovat podrobnějšímu popisu dané technologie, je potřeba se seznámit s jednotlivými účastníky, kteří jsou nezbytnou součástí při nasazování a provozování cloud computingu. Tito účastníci se dělí do tří skupin a to na konzumenty, poskytovatele a integrátory [2]. Podrobný popis těchto rolí je uveden v následující části této práce. Jednotliví účastníci mohou v danou chvíli zajímat více těchto rolí, což je znázorněno na obrázku 6, který je přiložen na konci této kapitoly. Samotné členění je důležité především z hlediska rozdělení povinností a odpovědnosti jednotlivých zúčastněných stran.

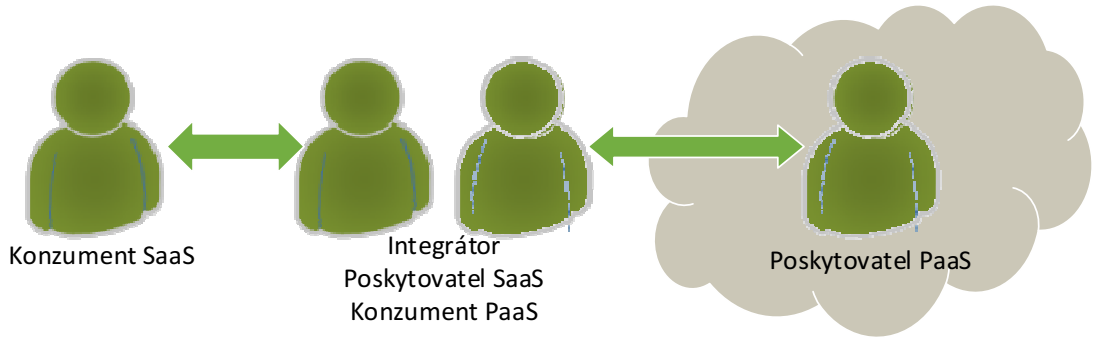
- **Konzument** - Tato role je odvozena z anglického slova „consumer“. Jedná se o stranu, která určitým způsobem poptává a následně využívá cloudové služby od poskytovatele. V této roli se však nemusí vyskytovat pouze koncový zákazník, ale

[3] Neplatí se paušálně, ale pouze za to, co se spotřebuje. Obdobně jako za elektřinu.

může v ní být (a velmi často i bývá) i samotný poskytovatel. Ten určitý typ služeb poptává a jiný (nebo ten samý) distribuuje svým zákazníkům, které můžou tvořit další poskytovatelé.

- **Poskytovatel** - Tento název je odvozeno z anglického „provider“. Dle zdroje [2] se jedná o klasického poskytovatele, jak ho známe například v případě internetu. Poskytovateli je z jeho hlediska jedno, zda danou službu poskytuje koncovým zákazníkům nebo dalšímu poskytovateli cloudových služeb, protože daná technologie v tomto případě nevyžaduje žádnou modifikaci. Dokonce ani sám poskytovatel nemusí vědět (a mnohdy ho to ani nezajímá), zda jeho zákazník je zákazníkem koncovým, anebo jeho služeb využívá jako jakousi platformu pro nabízení svých služeb.

- **Integrátor** - Název je odvozen z anglického „integrator“. Tento typ uživatele integruje dva typy cloudových služeb. Z toho vyplývá, že v této roli se nikdy nemůže vyskytnout koncový zákazník. Jedná se tudíž o poskytovatele-konzumenta, který jeden typ služeb poptává a jiný nabízí svým zákazníkům. V tomto případě je poskytovatel ve velice nevýhodné pozici. V případě výskytu závady na straně jeho poskytovatele, budou jeho koncoví zákazníci kontaktovat svého poskytovatele (integrátora), který s danou závadou ovšem nebude moci nic udělat. Tato rizika ovšem omezují smlouvy nazvaná SLA, kterými se zabývám v další části této práce [2].



Obrázek 6 - Uživatelské role v cloud computingu (Autor - upraveno dle: [2])

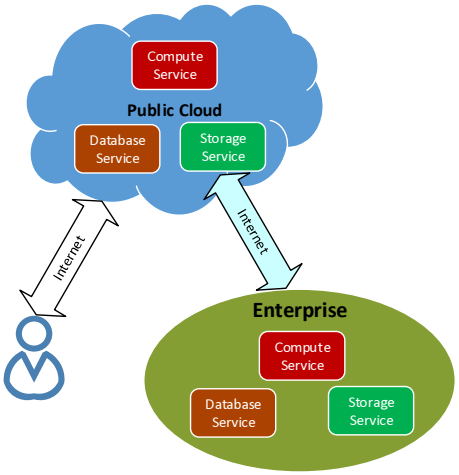
2.7 Modely nasazení cloudu

Protože je s cloud computingem spojeno velké spektrum technologií a lze ho nasadit pro řešení velkého množství problémů, je pro jeho hlubší pochopení této technologie potřeba použít určitý typ abstrakce a simplifikace. To jsou stěžejní důvody

proč se dostupné literatuře (např. [1] [2] [3]) cloud computing dělí do dvou typů modelů, které zjednodušují a zpřehledňují pohled na celou problematiku spojenou s technologií cloud computingu. Těmito modely jsou „model nasazení cloudu“ a „model cloudových služeb“. V této kapitole bude popsán první výše uvedený model. Ten jasně a jednoznačně definuje způsob, kterým může být cloud computing poskytován.

2.7.1 Veřejný cloud

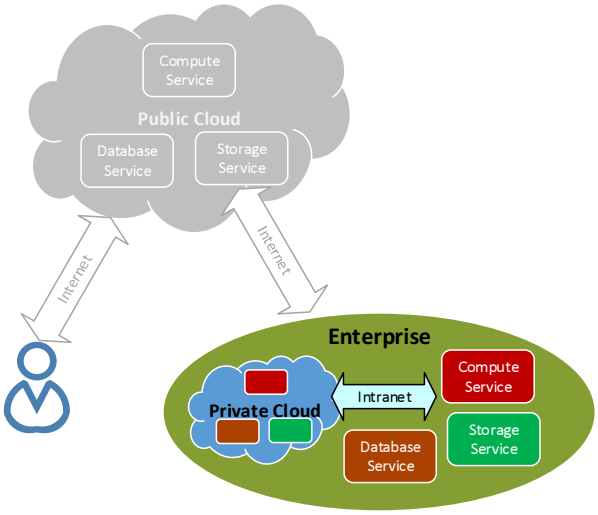
Jak uvádí mou použité zdroje například [1] a [17], veřejný cloud je klasickým a nejstarším modelem nasazení. Označení veřejný dostal na základě cílové skupiny, pro kterou byl určen, čili veřejnosti. Zákazníkům je služba poskytnuta pomocí klientského rozhraní a za samotný běh softwaru a hardwaru ručí poskytovatel. Mezi výhody tohoto řešení patří nízká cena dané služby. Navzdory tomu nevýhodou je značně omezená možnost přizpůsobit danou službu dle potřeb zákazníků. Tato nevýhoda plyne ze základní myšlenky veřejného cloudu a tou je snaha uspokojit společné požadavky co nejvíce uživatelů. S tím jsou však spojeny i určité bezpečnostní problémy a rizika, kterými se budu zabývat v kapitole č. 3. Tento typ poskytování služeb neobsahuje žádné dohody týkající se vlastnictví nebo případů použití cloudu, jako je tomu v případě privátního a komunitního cloudu (viz dále). Jelikož je tento typ služby určen pro velice širokou veřejnost, neumožňuje tento model použít sofistikované metody ověření uživatele, jak tomu bývá v případě veřejného cloudu. Proto je zde kladen důraz na vyšší zabezpečení pro jednotlivé uživatele pomocí mechanizmů pro kontrolu přístupu a práv. Obrázek 7 ilustruje schéma veřejného cloudu.



Obrázek 7 - Veřejný cloud (Autor - upraveno dle: [18])

2.7.2 Privátní cloud

Soukromý neboli privátní cloud se od veřejného liší zejména tím, že se celá služba využívá pro interní účely (například jednou společností) v rámci intranetu (vnitřní podnikové sítě), která je chráněná firemním firewallem [18]. Z toho vyplývá, že firma musí vlastnit celou hardwarovou infrastrukturu, o kterou se může starat oddělení IT nebo poskytovatel prostřednictvím „outsourcingu“. Výhodou tohoto řešení může být znalost o tom kde a v jaké podobě se nachází data, virtuální stroje, ale i samotná fyzická infrastruktura. Mezi další výhody tohoto řešení patří například bezpečnost přístupu, kdy nám odpadá problém s řešením přístupu více různých uživatelů (myšleno společností) ke sdíleným prostředkům. Tato koncepce se stala velice oblíbenou u společností pracujících s citlivými daty, jako jsou například banky. Model privátního cloudu je znázorněn na obrázku č. 8.

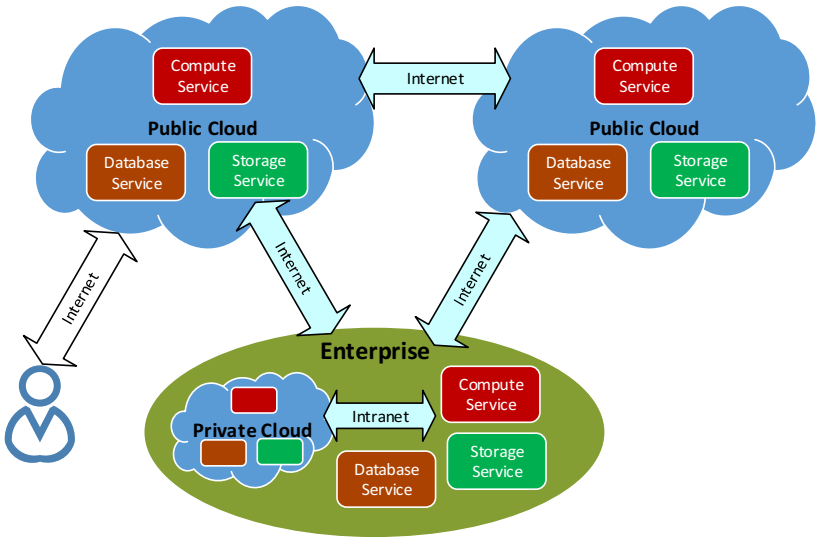


Obrázek 8 - Soukromý cloud Autor - upraveno dle: [18]

2.7.3 Hybridní cloud

Jak už z názvu vyplývá, jedná se o koncept kombinace více typů modelů (typicky privátního a veřejného) [17]. Tato idea umožňuje velkým firmám rozdělit své výpočetní prostředky a především data do několika skupin, respektive cloudů. Důvodů k rozdělení dat může být hned několik. Počínaje omezeními geopolitickými (jimiž se budu zabývat v kapitole č. 3.2), technickými (např. požadavek na šířku datového pásma, latenci, atd.), interními, bezpečnostními (např. ponechání kritických dat z pohledu firmy v privátním cloudu) a dalšími. Tyto jednotlivé cloudy vzájemně spolupracují, a to za pomocí takzvaného poradce („cloud broker“), který má za úkol sjednotit všechna data, aplikace, zabezpečení atd. [18].

Hybridní cloud poskytuje větší stupeň flexibility než je tomu u výše zmiňovaných modelů. Proto se dá očekávat, že se velké korporace budou stále častěji přiklánět k tomuto řešení cloudových služeb. Obrázek 9 znázorňuje model toho, jak by mohlo takovéto řešení vypadat.



Obrázek 9 - Hybridní cloud (Autor - upraveno dle: [18])

2.7.4 Komunitní cloud

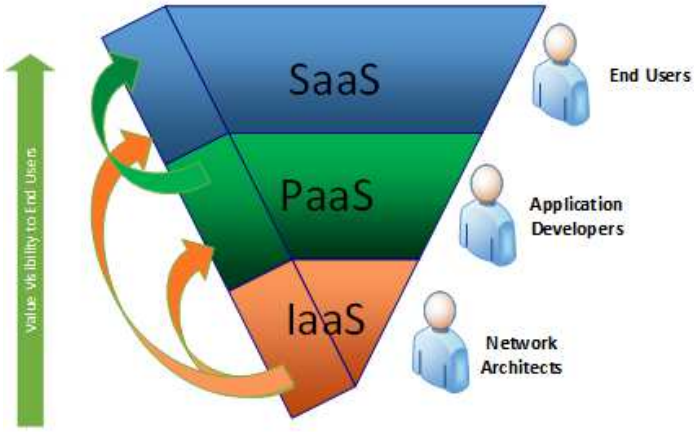
Posledním typem z modelu nasazení cloudu je komunitní cloud. Tento typ se používá v případě, kdy více organizací chce sdílet výpočetní prostředky či data, při čemž mají stejné požadavky na cloudové služby. Mezi tyto požadavky může patřit dostupnost a bezpečnost dat, požadavky na místo uložení, atd. Jedná se tudíž o privátní cloud, který je ovšem sdílený více subjekty. Stále však mezi méně uživatelů, než je tomu u veřejného cloudu. Právě kvůli podobnosti s modelem veřejného cloudu mnohdy toto řešení nebývá veřejností uznáváno [18]. Tento model lze velice dobře použít například ve státním sektoru.

2.8 Modely cloudových služeb

Někdy je tento model také nazýván jako distribuční. Model cloudových služeb poskytuje pohled na cloud computing z hlediska typu poskytovaných služeb. Dle definice NIST jsou zavedené úrovně IaaS („Infrastructure as a Service“), PaaS („Platform as a Service“) a SaaS („Software as a Service“). Podle těchto úrovní se vytvořil model, kde IaaS je vrstvou základní a každá vyšší vrstva v sobě obsahuje všechny nižší vrstvy. To je patrné z obrázku č. 10. Tento způsob pohledu na daný model je použit např. ve zdroji [1]

a nazývá Buttom-UP. Samozřejmostí je existence inverzního pohledu na danou problematiku. Tento inverzní přístup k danému modelu je označována jako Top-Down a je použit např. ve zdroji [17].

Mnoho dodavatelů se snaží toto členění ještě více rozštěpit a vytvářejí nové podkategorie. Vznikla tak koncepce „aaS“ (as a Service) kdy je všechno dodáváno jako služba. To naznačuje i vznik termínu „Everything as a Service“ (XaaS), který v překladu znamená „vše jako služba“. Jako příklad zde uvedu Security-aaS, který je dodáván firmou McAfee a Monitoring-aaS. Ve skutečnosti je však těchto služeb daleko větší množství [1].



Obrázek 10 - Model cloudových služeb (Autor - upraveno dle: [19])

2.8.1 IaaS

První vrstvou modelu je IaaS, nebo-li „Infrastructure as a Service“. Tato část modelu nám dává k dispozici samotný hardware. Konkrétně si pod tím můžeme představit disková úložiště, síťovou infrastrukturu, servery, atd. Typicky je infrastruktura zákazníkovi poskytnuta v podobě virtualizace, kterou jsem se zabýval v kapitole 2.1. Tento model je vhodný pro zákazníky, kteří si nechtějí pořizovat vlastní hardware, který je velice nákladný. Samotný hardware si spravuje poskytovatel služby, respektive je za tuto správu zodpovědný. Tímto uživateli odpadá spousta starostí, které jsou s tím spojeny, jako například správa hardwaru, jeho zabezpečení atd. Jak se shodují např. zdroje [1], [2] a [17], základní vlastností, kterou tento model poskytuje, je možnost nasazení vlastního softwaru nad danou infrastrukturou. Typicky se jedná o operační systém či aplikace. Mnohdy je tento typ služby společnostmi využívají z důvodů zálohování, kdy i v případě živelné pohromy jsou jejich data pořádku ve vzdáleném datovém centru.

Mezi největší a nejvýznamnější poskytovatele této služby patří v současnosti např. firma Amazon.

2.8.2 PaaS

Druhou vrstvou ve výše zmiňovaném modelu je PaaS – „Platform as a Service“. Pod pojmem platforma jsou myšleny hardwarové prostředky, aplikační frameworky a další prostředky, které nám podporují celý životní cyklus tvorby a poskytování webových aplikací a služeb. Konkrétně zde mluvíme o databázích, vývojových rozhraních, aplikačních serverech atd. Nedílnou součástí této služby je operační systém, na kterém tyto služby běží. Hlavními cíli této vrstvy jsou tedy: usnadnění nasazení daných prostředků bez vedlejších nákladů a problémů s tím spojených a následné umožnění běhu sofistikovanějších aplikací na této vrstvě. Výše uvedené problémy se nyní přesouvají na poskytovatele. To znamená, že se zákazník nestará o nákup licencí, verzování systému a samotnou přípravou pro běh dané služby. Dále se zákazník nestará ani o infrastrukturu, na které daná služba běží [2] [17]. Danou infrastrukturu buď vlastní daný poskytovatel, nebo si ji propůjčuje formou IaaS od dalšího poskytovatele. Při výskytu jakéhokoliv problému však zákazník komunikuje pouze se svým poskytovatelem nehledě na to, zda nastala porucha v PaaS nebo IaaS. Z toho vyplývá, že poskytovatel dané služby (integrátor) zodpovídá i za služby, které mu jsou jako integrátoru poskytovány.

Tato vrstva je teda primárně určená pro vývojáře či deployment administrátory, jejichž hlavní pracovní náplní je návrh, vývoj a provoz aplikací. Mezi nejznámější služby typu PaaS v době psaní této práce patří např. Windows Azure od společnosti Microsoft [1] nebo Google App Engine [17] od společnosti Google.

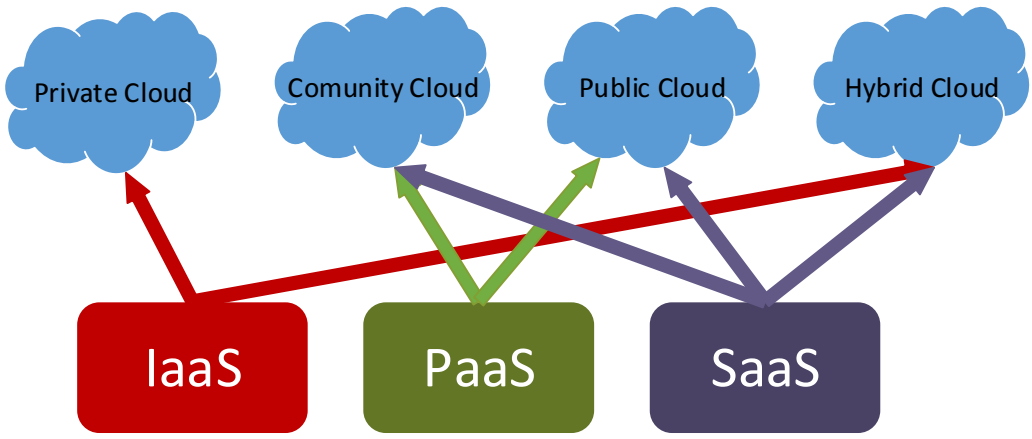
2.8.3 SaaS

Poslední vrstvou modelu je SaaS – „Software as a Service“. Jedná se o nejvýše postavenou vrstvu, která využívá obě své „podvrstvy“. Již z názvu je patrný hlavní účel SaaS. Tím, je poskytnou uživateli hotový software. Ten je poskytnut přes webové rozhraní, takže si uživatel do svého stroje nemusí nic instalovat. Navíc je tak dostupný velkému množství uživatelů. Jedním z nejjednodušších a zároveň nejpopulárnějším příkladem SaaS jsou emailové služby [1].

Z pohledu uživatele se jedná o nejjednodušší typ služby, protože zde z jeho strany odpadají veškeré starosti a problémy. Ty jsou však přesunuty na providera dané služby, a proto se z pohledu poskytovatele jedná o nejkomplikovaněji poskytovanou službu. Důvodem je povinnost providera starat se o celkovou správu systému, správu operačního systému, správu aplikací a v neposlední řadě i o správu hardwaru, a to buď přímo[4] nebo nepřímo[5].

[4] Myšleno ve chvíli, kdy poskytovatel tyto prostředky vlastní.
[5] Myšleno prostřednictvím Service Level Agreement (SLA) se svým poskytovatelem daných služeb.

Grafické znázornění rozdělení cloudových služeb dle výše uvedených typů a znázornění, pro jaké účely se konkrétní modely využívají dle společnosti NIST [3] je patrné na obrázku níže (viz obr. č. 11).



Obrázek 11 - Rozdělení cloudových služeb a typy jejích využití (Autor - upraveno dle: [20])

2.9 Výhody cloud computingu

Cloud computing je v dnešní době velice oblíbený zejména proto, že svým zákazníkům přináší množství nesporných výhod. Zde se však nebudu zabývat veškerými výhodami dané technologie, ale pouze těmi, které jsou z mého pohledu zásadní a na kterých se shodli mou použité zdroje [1], [2] a [17].

První z nich může být snížení nákladů na infrastrukturu. Respektive zákazníkům odpadá nutnost budování vlastního, mnohdy velice drahého, datového centra. Sem musíme počítat nejen cenu serverů a dalšího potřebného hardwaru, ale i cenu za napájení. Dále se musí zahrnout cena správy hardwaru a mzdových nákladů pracovníku IT. V neposlední řadě musíme počítat i s prostorem potřebným pro vybudování dané infrastruktury. Po porovnání těchto nákladů s náklady spojenými za nákup poskytované služby, se mnoho společností přikloní k řešení s využitím cloud computingu. Dokonce i v situaci kdy se tyto náklady rovnají, se musí zvážit, která varianta je pro firmu vhodnější.

Další výhodou této technologie je rychlost. Zde však rychlost bude brána z lehce odlišného pohledu, především z pohledu vývoje. Tato výhoda vyplývá ze situace, kdy zaměstnanci IT nemusí kupovat a konfigurovat nová zařízení a mohou se tak soustředit na koncepční záležitosti a na vývoj aplikací. Tím je docíleno stavu, kdy jsou rychle dostupné požadované aplikace, a to vše za zlomek ceny, kterou by si vyžádalo vnitropodnikové řešení.

Mezi naprosto klíčovou vlastnost cloud computingu patří škálovatelnost. Tu využijeme ve chvíli, kdy předpokládáme vysoký nárůst výpočetních požadavků (nebo

dokonce už zde tyto požadavky jsou). Ve vnitropodnikovém řešení bychom museli kupovat, instalovat a nastavovat dodatečný hardware. Cloud computing nám ovšem umožňuje ovlivnit množství využití dané služby. To nám například umožňuje objednat dodatečný procesorový výkon, dodatečnou kapacitu úložiště, atd. Vzhledem k faktu, že náklady takového řešení závisí na spotřebě zdrojů, nás tento způsob řešení pravděpodobně vyjde levněji, než nákup nového vybavení. Jakmile totiž nárůst požadavků pomine, lze využívané zdroje jednoduše snížit a nemusíme řešit co s novým zařízením. Jednoduše tak lze zvyšovat a snižovat spotřebu zdrojů s ohledem na firemní potřeby.

Mezi nesporné výhody cloud computingu patří dostupnost. Tato technologie nám totiž umožňuje mít přístup ke svým datům či aplikacím odkudkoli na světě. Jediným požadavkem je internetové připojení. V případě SaaS dokonce není potřeba si na svojí pracovní stanici instalovat jakýkoliv software.

Jako další výhodu lze uvést zkušenost dodavatelů. Velmi často se stane, že s příchodem nové technologie na trh s ní přijde i velký počet menších a mnohdy nevěrohodných společností, které tuto technologii nabízí. Ti pak mnohdy poskytují nekvalitní služby vzhledem k dané technologii. V případě cloud computingu je ovšem situace jiná. Zde jsou poskytovateli renomované a celosvětově známé společnosti jako Microsoft, Amazon, IBM a další. Tento fakt nám de facto zaručuje i 24 hodinovou podporu a poskytování služeb. Z toho vyplývá další výhoda a tou je řešení výpadků služby. V tomto případě se starost přesouvá na poskytovatele a zákazník tak má opět o starost méně. Zde je důležité upozornit na fakt, že se poskytovatel snaží udržet své služby v chodu pokud možno bez výpadků. Pokud by totiž některý poskytovatel začal mít dlouhodobější problém s dostupností svých služeb, velmi rychle by přišel o své zákazníky. Proto každý poskytovatel cloudových služeb zaměstnává celou řadů odborníků, kteří po dobu 24 hodin dohlížejí na bezproblémový chod serverů, na nichž tyto služby běží.

Cloud computing nám dále umožňuje přesunout na třetí stranu požadavky na zpracování dat, které nejsou pro naši firmu kritické. Tudíž se pracovníci IT mohou zaměřit na důležité úkony spojené s činností organizace.

V neposlední řadě je zde i jistá výhoda zabezpečení. Tento bod je však spekulativní. Proto se více touto problematikou zabývám v kapitole č. 3.

2.10 Situace při nichž použití cloud computingu nemusí být vhodné

Jako všechny technologie, tak i tato není dokonalá, všemocná a není ji vhodné nasazovat za každou cenu a v každé situaci.

Prvním z mnoha problémů může být hardwarová závislost. Ta nastává ve chvíli, kdy vlastníme aplikaci, která vyžaduje specifický hardware nebo ovladač. V takovém případě řešení cloudu nemusí být nikterak vhodné. Poskytovatelé totiž velice často nemají vámi požadovaný specifický hardware, ale i v případě kdy ano, není zcela po problémech.

Pokud totiž poskytovatel časem tuto požadovanou součást hardwaru vymění za jinou, můžete se ocitnout před nepříjemným problémem [1].

Do problému s cloud computingem se dostaneme i ve chvíli kdy chceme mít úplnou kontrolu nad serverem. Vyžaduje-li naše aplikace vládu nad všemi spuštěnými procesy nebo potřebujete-li informace o dostupné paměti, využití procesoru a obdobné další informace, nebudu pro vás cloudové řešení vhodné. Všechny tyto informace má totiž poskytovatel. Nesmíme však zapomenout na stav, kdy v některých cloudech nedostanete ani přístup uživatele root [1].

Dalším aspektem, který je zmíněn ve zdroji [1] a ovlivňuje rozhodování, zda přejít na cloudové řešení, je integrace se stávajícími aplikacemi. Mějme modelovou situaci, kdy podnik využívá dvě databáze. Jedna obsahuje citlivá data a je hostovaná lokálně. Druhá je v cloudu a obsahuje pouze data veřejná. Při práci s těmito databázemi je velice pravděpodobné, že se nakonec citlivá data objeví i v cloudu. Výkon celého systému bude dále limitován tím, co nám dovolí cloud a připojení k internetu.

Pokud mezi kritické požadavky na systém patří rychlost dostupnosti dat, i zde pak nemusí být použití cloudu vhodné. Důvodem je umístění dat na vzdálených serverech, které mohou být rozmístěny po celém světě. Na data sice nebudeme muset čekat hodiny nebo minuty, ale i tak vzniklá prodleva může být nepřijatelná [1].

Nesmíme zapomínat i na požadavky právní, geopolitické a bezpečnostní. Touto problematikou se ovšem věnuji v dalších částech své diplomové práce.

3 Možné hrozby související s cloud computingem

Bezpečnost dat je jednou z klíčových vlastností, která je v oboru informační technologie požadovaná a na kterou je kladen obrovský důraz. Některé studie dokonce uvádějí, že pro takřka 75 % firem je bezpečnost nejčastějším zdrojem obav a tudíž je tento problém naprosto zásadní [21]. Bezpečnost dat je o to více potřeba řešit v případě, kdy uživatel komunikuje přes internet nebo v rámci intranetu. V takovém případě nevíme, kudy daná data putují a kdo všechno k nim může mít přístup. V oblasti cloud computingu se o odpovědnost za bezpečnost dat spolu dělí dvě skupiny. Do té první patří poskytovatel služby, kdežto na druhé straně je samotný uživatel, který danou službu využívá. Míra odpovědnosti a povinností jednotlivých skupin v nemalé míře záleží jak na distribučním modelu, tak i na modelu nasazení cloudu. Jako příklad zde uvedu situaci, kdy uživatel přistupuje k veřejnému cloudu a je mu poskytován software jako služba (SaaS). V tomto případě je uživatel povinen se starat pouze o dvě věci. Tou první je bezpečný přístup ke svému pracovnímu stroji, respektive o přístup ke službě z bezpečného stroje, a tím minimalizování šance na zcizení přihlašovacích údajů. Druhou věcí je zajištění, aby všichni jeho uživatelé byli seznámeni se zásadami bezpečného používání služby v rámci podnikové politiky a provádění kontroly dodržování těchto zásad. Veškera další odpovědnost spojená se zabezpečením (fyzické zabezpečení serverů, šifrování atd.) je přesunuta na stranu poskytovatele dané služby.

Aby se předešlo situacím, kdy poskytovatel musí nastínit svou bezpečnostní konfiguraci zákazníkovi jako důkaz, že jsou jeho data v bezpečí, byly vytvořeny bezpečnostní normy. Tím, že poskytovatel splňuje určitou normu, je zákazník jednoznačně informován o tom, jaký stupeň bezpečnosti mu daný poskytovatel dokáže nabídnout. Nejznámější sérií norem, týkajících se cloud computingu je série ISO 27000 [2], kterou se budu zabývat v další části této práce.

Dále je potřeba dodat, že cloud computing může pokrývat velmi široké spektrum požadavků, a to jak ze strany zákazníka, tak i ze strany poskytovatele. Proto neexistuje jednotná doporučená bezpečná konfigurace dle typu poskytovaných služeb a modelu nasazení cloud computingu. Všechny bezpečnostní hrozby a typy možných bezpečnostních opatření tak závisí na konkrétních službách, požadavcích, použitém hardwaru, softwaru a mnoho dalších faktorech. Z toho vyplývá, že v této kapitole nebudou a ani nemohou být popsány všechny bezpečnostní hrozby, které se mohou vyskytnout. V této kapitole tak najdete pouze ty nejznámější a nejvýznamnější hrozby z pohledu bezpečnosti.

3.1 Dodavatel cloudových služeb

Ač se to na první pohled nemusí zdát patrné, je výběr poskytovatele cloudových služeb jedním ze zásadních kroků pro zákazníka. Důvodem je obrovský rozdíl přístupu jednotlivých poskytovatelů, a to nejen z hlediska bezpečnosti, ale i dostupnosti, kvalitě poskytovaných služeb, ceny, atd.

Průzkum s názvem „Security of Cloud Computing Providers Study“ provedený v dubnu roku 2011 společností Ponemon Institute, dostupné na [21], poukazuje na až alarmující zjištění. Z výzkumu vyplývá, že poskytovatelé cloudových služeb, se zaměřují primárně na poskytnutí levného a lehce implementovaného řešení, které zlepší zákazníkovy služby. Bezpečnost služeb je pro ně až druhotným problémem, který v mnoha případech vůbec neřeší. Z výzkumu je dokonce patrné, že poskytovatelé se v mnohých případech nezajímají o bezpečnost dat a tento problém přesouvají na zákazníka. V neposlední řadě nejsou tyto rychlé a levné služby mnohdy zkoumány z pohledu bezpečnosti, a tak by se daly označit za potencionálně nebezpečné. O této skutečnosti hovoří fakt, že 63 % poskytovatelů se sídlem v Evropě a 62 % se sídlem v USA si není jistých, zda jsou jejich služby bezpečné.

Výsledky studie jako je tato, ale i výsledky mnoha dalších, které jsou obdobně zaměřené, nám dávají varovný signál o tom, že výběr poskytovatelé služeb je krok, na kterém opravdu záleží.

Protože oblast cloud computingu je velice mladá[6] (obzvláště z hlediska marketingového), nejsou zde žádná obecná doporučení, týkající se obecného postupu výběru vhodného poskytovatele [1]. Jednou z možných variant je braní v potaz velikosti, renomé a historie společnosti, poskytující cloudové služby. Toto hledisko vychází z faktu, že velké nadnárodní firmy dodávající služby cloud computingu, jsou v dané oblasti zkušenější a mnohdy nabízí kvalitnější a rozsáhlejší podporu. Nad tím vším by samozřejmě mělo být ověření poskytování dané služby v požadované kvalitě a s potřebným zabezpečením. Mezi takové firmy může například patřit VMware, Microsoft, IBM, Google, Amazon a mnoho dalších.

Dle zdrojů [2] a [17] je výběr kvalitního poskytovatele důležitý i proto, že v oblasti cloud computingu obecně platí, že se mezi poskytovatelem služby a jeho zákazníkem vytváří mnohem důvěryhodnější a intenzivnější vztah, než v případě například poskytovatele internetu. Tento vztah může být budován v několika krocích. Jedním z prvních je proces dojednávání požadovaných služeb a seznamování se s novým prostředím, které cloud computing přináší. Samozřejmostí je seznámení se s technologiemi a postupy, které daný poskytovatel nabízí a používá. Tento krok je potřeba brát s mírnou rezervou. Nedá se totiž očekávat, že by vám poskytovatel detailně popsal svou bezpečnostní politiku spolu s konfigurací všech svých zařízení. Tím by se sám vystavoval jistému bezpečnostnímu riziku. Tento vztah je pro obě strany důležitý jak z hlediska důvěry, tak i z hlediska budoucí spolupráce. Musíme si uvědomit, že společnost využívající služby třetí strany této třetí straně mnohdy poskytuje data, která mohou být z pohledu fungování naprosto zásadní. Nedokážu si představit situaci, kdy by firma poskytla tak cenná data někomu, ke komu nemá absolutní důvěru. Tato důvěra se týká jak bezpečnosti dat před ztrátou, tak i před jejich zneužitím. Důvěra je důležitá i ve chvíli, kdy vám poskytovatel nastíní jeho přístup k řízení havarijních událostí. Tuto vlastnost si lze

[6] Toto tvrzení vyplývá už jen ze samotné historie cloud computingu (viz kapitola 2.3 této diplomové práce).

mnohdy ověřit až ve chvíli, kdy k havárii skutečně dojde (porucha úložného média). Pokud se následně zjistí, že poskytovatel neprovedl ty aktivity, které sliboval (záloha dat na jiné médium), důsledky mohou být pro zákazníka fatální. Aby se podobným situacím a následným sporům o dopadu odpovědnosti předešlo, musejí se všechny podobné vlastnosti uvést do smlouvy o poskytování služeb (SLA). Dále v závislosti na povaze businessu firmy a typu využívaných služeb, může být komunikace mezi oběma stranami velmi intenzivní. A to jak ze začátku, tak i v průběhu této spolupráce. Důvody mohou být různé. Počínaje neustále se měnícími požadavky zákazníků, až po změny nabídky daného poskytovatele. V závislosti na těchto požadavcích musí poskytovatel nabídnout servis svých služeb na patřičné úrovni, v požadované kvalitě a hlavně v požadovanou dobu. Nutno ovšem podotknout, že všichni výše zmiňovaní poskytovatelé jsou natolik velcí, že jim tento požadavek nečiní problémy. To proto, že zaměstnávají spoustu odborníků, kteří jsou k dispozici 24 hodin denně a kteří obsluhují velké množství datových center rozmístěných po celém světě.

Mezi další klíčové vlastnosti cloud computingu, které s důvěryhodností až tak nesouvisí, patří i dostupnost služeb. Tato vlastnost je z pohledu zákazníka naprosto klíčová a měla by být uvedena ve smlouvě o poskytování služby (SLA). Obecně lze ale říci, že se všichni poskytovatelé snaží, nebo by se alespoň měli snažit, o maximalizování této vlastnosti, stejně tak jako o bezpečnost dat svých zákazníků. Nikdo totiž nebude využívat službu, která je neustále nedostupná, nebo o které se ví, že má problémy s bezpečností. Problémy s dostupností měla v minulosti například společnost Rackspace, která v roce 2007 měla 36 hodinový výpadek svých služeb. Na vině byla porucha trafostanice umístěné mimo jimi spravované datové centrum [2].

Jak je uvedeno v [1], dá se obecně říci, že ač s sebou technologie cloud computingu přináší spoustu potenciálních rizik, žádná z nich nejsou z pohledu bezpečnosti nová. Úkolem důvěryhodného poskytovatele by tedy měla být snaha těmto rizikům předejít nebo je alespoň minimalizovat.

3.2 Právní a geopolitická rizika

Ačkoliv by se na první pohled tento bod mohl zdát až zábavný, není tomu tak. Musíme si uvědomit, že výběr umístění uložení vašich dat nemá vliv pouze na jejich dostupnost, ale i na to kdo k nim bude mít přístup a jakým způsobem se s daty bude nakládat. Různé země a oblasti totiž mají odlišné přístupy ke způsobu zacházení a ukládání soukromých dat. Počínaje Spojenými státy americkými a konče Evropskou unií. Konkrétně ve státech Evropské unie platí zákon o ochraně osobních dat [22]. Ve Spojených státech amerických existuje obdoba výše uvedeného zákonu, který se ovšem týká zdravotních záznamů občanů Spojených států amerických [2]. Z toho je možné vypozorovat, že se jednotlivé státy chovají jinak k datům svých obyvatel a jinak k těm, co patří cizincům nebo lidem ze zahraničí. Legislativa Spojených státu amerických dokonce nařizuje předání veškerých dat, o které si bezpečnostní úřad zažádá, a to bez svolení majitele. Tento zákon

neuvádí, o jaký druh informací se může jednat, a tudíž si bezpečnostní úřad může vyžádat jak osobní, tak i finanční záznamy kterékoliv společnosti nebo jednotlivce. Pro podání této žádosti ovšem musí existovat podezření ze spáchání nebo připravování trestné činnosti. Z tohoto důvodů si Kanada upravila svou legislativu. V současné době nesmí žádný Kanadský státní orgán používat k ukládání dat server ležící na území Spojených státu amerických, a to z důvodu možného nežádoucího přístupu ze strany amerických bezpečnostních úřadů [1]. Jako příklad zde uvedu přístup Číny, který je trochu odlišný. Dle [17] zákony Číny umožňují vládě neomezený přístup k jakýmkoliv datům, bez ohledu na jejich citlivost (obsah). V tomto případě se sice nabízí využít možnosti šifrování, ale existuje tu stále riziko, že tato data budou dešifrována.

S touto, a výše uvedenou problematikou (viz kapitola 3.1), mohou souviset i další možné nepříjemnosti. Může totiž nastat situace kdy vy jako firma (uživatel cloudu) budete vládní agenturou požádáni o předání určitých dat. Ale i proto, že daná data vlastní váš poskytovatel cloudových služeb nikoliv vy, jste zodpovědní za dodržení požadovaných podmínek, které vládní organizace přednesla. Tyto podmínky se mohou týkat jak rozsahu dat, tak i času, do kdy musíte daná data předložit. Proto musíte vědět, jak rychle je váš poskytovatel schopen reagovat v situacích které vyžadují rychlou reakci [17].

Při volbě umístění námi využívaného datového centra bychom se měli vyhnout místům se zvýšeným rizikem ničivých přírodních živlů. Tímto mám na mysli hlavně zemětřesení, povodně, hurikány a tornáda. Samotná datová centra v takových oblastech sice bývají proti těmto přírodním živlům chráněná, ne vždy však tato ochrana může být dostatečná. I zde platí pravidlo, které říká, že je lepší problémům předejít, než se s nimi následně vypořádávat.

3.3 Riziko zneužití citlivých dat - Data breaches

Tato hrozba je noční můrou každé společnosti. Situace, kdy se citlivá data dostanou do rukou konkurence, může ohrozit chod společnosti a dovést ji i ke krachu. Dle [23] byla v listopadu roku 2012 za pomocí vědců z University of Wisconsin a korporace s názvem RSA odhalená metoda, pomocí které lze získat privátní šifrovací klíč jiného virtuálního stroje běžícího na stejném fyzickém serveru. Naneštěstí útočník tuto komplikovanou metodu v mnohých případech ani nemusí použít. Naprosto mu postačí mít špatně navrženou databázi, jež využívá cloudových služeb. Pomocí využití této chyby je útočníkovi umožněn přístup nejen k datům dané společnosti v dané databázi, ale i k datům všech ostatních zákazníků, kteří tuto databázi využívají.

Východiskem z této situace zdá se být použití složitého šifrovacího klíče pro zabezpečení dat. To nám ovšem nezajistí jistou ochranu před odcizením a následnou ztrátou dat. Jako další možnost zabezpečení se nabízí uchovávání citlivých dat v offline záložním systému. To však značně zvyšuje náklady a nároky na režii.

3.4 Riziko ztráty dat – Data loss

Ztráta dat zde není chápána ve smyslu odcizení, jako tomu bylo v minulém případě. Zde je chápána ve smyslu smazání čí odstranění. Tento problém nejčastěji postihuje jak firmu využívající cloudových služeb, tak následně i samotné koncové zákazníky dané společnosti. Příčin ztráty dat může být hned několik, počínaje útokem krackera[7], přes chybu personálu poskytovatele, chybu hardwaru nebo jako důsledek přírodní katastrofy. Musíme si také uvědomit, že za ztrátu svých dat může být zodpovědný i samotný zákazník (uživatel). Postačí, aby si daný uživatel svá data chránil pomocí klíče a ten následně ztratil nebo zapomněl. I v tomto případě jsou data považována za ztracená, protože k nim nemá nikdo přístup. Musíme si však také uvědomit, že pouze používání silných a doporučených hesel nám také nemusí vždy pomoci. Jako příklad zde může sloužit případ jednoho novináře, jemuž se hackeři dostali na účet Googlu, Tweetru, Applu a Amazonu. To vše bez znalosti jediného hesla nebo použití brutal force[8] útoku [24]. Tito útočníci následně využili jeho účtu na Apple ICloud k úplnému odstranění všech jeho dat z IPhonu, IPadu a MacBooku [25].

Řešením z této situace je opět offline zálohování a dodržování vnitropodnikových doporučení a nařízení týkající se ochrany dat. Samozřejmostí je používání silných hesel a šifrování dat.

Vážnost této hrozby a nejednotnosti v zákonech a povinnostech si uvědomili i zákonodárci EU a v lednu 2012 renovovali zákon z roku 1995. Tento zákon zpřísňuje metody ochrany, způsobů mazání a zacházení s osobními daty uživatelů [22].

3.5 Riziko odcizení účtu nebo přenášených dat - Accoutn or service trafick hijacking

Z pohledu zabezpečení se nejedná o nikterak nový způsob hrozby. Tato metoda útoku je podobná phishingu[9]. Útočník se snaží získat citlivé údaje od uživatele a následně pomocí nich získat přístup k jejich účtu, nebo ke kontrole nad službou. Ve chvíli kdy se to útočníku povede, stává se účet útočníkovy oběti jeho novým útočištěm. Dalším důsledkem může být neoprávněný přístup nepovolené osoby ke kritickým datům či částem systému společnosti [23].

[7] Tímto termínem je označována osoba, která má dobré znalosti v oboru počítačové bezpečnosti a tyto znalosti zneužívá ke svému prospěchu při průnicích do softwaru.
[8] Neboli útok hrubou silou. Jedná se o metodu, kdy se útočník pomocí zkoušení různých kombinací znaků snaží přijít na hodnotu klíče.
[9] Podvodná technika, kdy se útočník snaží od uživatele získat jeho osobní údaje.

V dubnu 2010 Amazon opravil bug (chybu), který do té doby pomocí Cross-Site skriptu[10] útočníkům umožňoval přístup k přihlašovacím údajům. V roce 2009 tatáž společnost byla zneužita pro běh mnoha Zeus botnetů[11] [26].

Společnosti si jsou této hrozby dobře vědomy, a proto se snaží o zamezení sdílení účtu mezi více uživateli, znemožnění posílání osobních a citlivých údajů. V neposlední řadě zavádějí dvouúrovňovou autentizaci, pokud to daná situace dovoluje [23].

3.6 Riziko zneužití účtu - Malicious insider

Volný překlad definice dle společnosti CERT zní:

„*Pod pojmem narušitel rozumíme zaměstnance, jednatele či obchodního partnera, který má nebo měl autorizovaný přístup k podnikové síti, sytému nebo datům, jenž tento přístup zneužil za účelem negativního ovlivnění integrity, dostupnosti nebo důvěrnosti dat nebo informačního systému*“ [27].

Tento typ hrozby je společný jak pro IaaS[12], PaaS[13], tak i SaaS[14]. Více informací týkajících se těchto pojmů naleznete v kapitole 2.8. Snad největší riziko hrozí, pokud touto osobou je administrátor poskytovatele služby. V tomto případě pak nemusí zákazníku stačit ani používání šifrování dat spolu se správným způsobem uchování šifrovacího klíče [28]. V případě veřejného cloudu je zákazník v této chvíli bezmocný a musí spoléhat pouze na korektnost svého poskytovatele. V případě cloudu privátního lze této hrozbě předejít dodržováním správných politik v oblasti lidských zdrojů, definování adekvátních uživatelských rolí a odpovědností. K následné ochraně lze dodatečně využít i monitoring poskytovaných služeb a aktivity jejích uživatelů. Dále musí být stanovená a dodržována pravidla týkající se typu, způsobů a míst přístupu k daným službám. Nesmíme však zapomenout ani na proškolení personálu a s jeho seznámením s bezpečnostními politikami a zásadami, které se musí dodržovat [23].

3.7 Rizika spojená se zneužitím služeb cloud computingu - Abbuse of Cloud Services

Cloud computing umožňuje i malým společnostem mít přístup k výkonu desítek až stovek serverů, kterého by jinak tyto společnosti nikdy nemohly dosáhnout. Ne všichni však tento výkon používají pro dobrou věc. Tento výkon se může zneužívat například

[10] Je metoda kdy útočník využívá bezpečnostních chyb ve skriptech webových stránek (hlavně neošetřené vstupy) pro podstrčení vlastního skriptu nebo škodlivého kódu.
[11] Softwarový agent, internetový robot či počítač napadený malwarem (škodlivým softwarem), který slouží pro rozesílání spamu (nevyžádaná pošta), DDoS útoku atd.
[12] Infrastruktura jako služba
[13] Platforma jako služba
[14] Software jako služba

k prolamování hesel. Na běžném stroji toto prolomení může trvat velice dlouhou dobu. S využitím cloud computingu však tento čas může být zkrácen i na řády minut. Další využití této technologie může být k vytvoření DoS útoku, šíření malwaru atd. [23]

Tento problém není tak snadné vyřešit, jak by se na první pohled mohlo zdát. Na druhou stranu je toto spíše problematika poskytovatelů služeb než samotných zákazníků, proto se této hrozbě nebudu věnovat do detailů.

3.8 Odepření služby nebo přístupu k ní - Denial of Service (DoS)

Jedná se o relativně jednoduchý útok, který se špatně brání a může mít fatální důsledky. Primárním účelem tohoto útoku je znemožnit přístup uživatelům k dané službě. Neboli zpomalit chod dané sužby na neúnosnou úroveň nebo v ideálním případě způsobit její pád (odepření služby). To se nejčastěji provádí pomocí konzumace všech dostupných zdrojů, které daná služba nabízí. Toho se dá dosáhnout mnoha způsoby. Například pomocí vytížení procesoru, pamětí, místa na disku, propustnosti linky, apod. Tento útok má i svou distribuovanou podobu kdy se na „oběť“ v jeden okamžik útočí z více míst, zejména pomocí takzvaných zombee[15]. Tento typ útoku zpravidla má větší sílu a nazývá se DDoS (Distributed DoS) [29]. Zajímavou alternativou k tomuto útoku je metoda, kdy útočník předem informuje veřejnost o cíli a čase plánovaného útoku. V důsledku toho se část uživatelů snaží otestovat, zda je na danou službu opravdu veden útok a zda je tato služba dostupná. Tímto jednáním však sami přispívají k vytížení a tím i k DoS, respektive k DDoS útoku.

Útočníkům však nemusí vždy jít pouze o znepřístupnění služby. Z povahy cloud computingu, kdy platíte za to, co spotřebujete, může být cílem útočníka způsobit vám jako zákazníkům znatelné finanční ztráty. V tomto případě vám služba nejspíše nebude znepřístupněná, avšak poskytovatel může za využití svých služeb (i když nelegální a ne vámi) účtovat značnou částku. Tato varianta útoku však vyžaduje, aby útok byl veden přes daného zákazníka.

Jak již bylo zmíněno výše, proti tomuto typu útoku není moc způsobů ochrany. Nabízí se zde několik variant jako možnost propouštět jen část přijímaných požadavků. Ovšem je tu riziko, že mezi nepřijatými požadavky bude požadavek legální (myšleno ne ten, který posílá útočník) a tím se docílí znepřístupnění služby „legálnímu“ uživateli, což bývá hlavním cílem tohoto útoku. Dalšími možnostmi ochrany se stává firewall a IPS, ale efektivita těchto metod není vždy dostatečná. Navíc metoda IPS nemůže být použitá vždy [30].

V době psaní této diplomové práce došlo na území České republiky k masivním DDoS útokům na tuzemské zpravodajské weby. Během těchto útoků byla řada napadených

[15] Napadený počítač, který se bez vědomí svého uživatele účastní útoku.

webů nepřístupná. Weby, které tento útok „ustály“ se v době útoků potýkali s vysokou odezvou a částečnými výpadky svých služeb [31].

3.9 Rizika plynoucí z neznalosti či nepochopení prostředí computingu - Insufficient Due Diligence

Jak je patrné např. z [1] a [2], s příchodem cloud computingu se mnoho společností snažilo tuto technologii co nejdříve implementovat a to beze snahy plně pochopit problematiku, kterou s sebou přináší. Hlavními důvody byly nesporné benefity. Jako ušetření počátečních investic týkajících se infrastruktury, škálovatelnost, dostupnost, menší režie ze strany zákazníka, atd. Bez plného pochopení problematiky prostředí cloudu, přístupu k aplikacím a službám a operací zodpovědných za bezpečnost, šifrování, monitoring a organizaci dat, se uživatel vystavuje riziku na pro něj neznámé úrovni. Tato rizika však mohou mít fatální důsledky na fungování společnosti.

Předejití těmto hrozbám není až tak technologický náročný proces jako spíše proces náročný časově. Každá společnost by se měla před začátkem využívání cloudových služeb plně seznámit s riziky, odpovědnostmi a povinnostmi, které s sebou tento nový model přináší. Společnost by se měla seznámit s prostředím svého poskytovatele a s technologiemi které využívá a detailně projít všechny požadavky na funkcionalitu a bezpečnost. Hlavně v případě využívání veřejného cloud může nastat situace, kdy organizace požaduju určitou úroveň ochrany, kterou jí poskytovatel nemůže zaručit. Poskytovatel však s ohledem na různorodost a množství svých zákazníků nemusí být ani do budoucna schopen požadovanou funkcionalitu zaručit. Z tohoto důvodů je plné seznámení velice důležitým faktorem a to ještě před začleněním cloud computingu do svého portfolia. Naopak v případě privátního cloudu tento problém nenastává, protože zde jsou ze strany poskytovatele služby poskytovány přesně dle požadavků zákazníka. Pokud se společnost seznámí se všemi faktory a rozhodne se pro řešení v podobě cloud computingu, nemělo by se zapomínat na proškolení uživatelů, kteří budou danou službu využívat. A nebo je s touto změnou alespoň seznámit. Během tohoto procesu by se nemělo zapomínat na zaškolení personálu a jeho seznámení se všemi jejich novými povinnostmi a odpovědnostmi [2].

3.10 Problematika nezabezpečených rozhraní a API - Insecure interfaces and APIs

Jak uvádí [32], poskytovatelé cloudových služeb v minulosti upozornili na skutečnost, kdy mnoho typů softwarových rozhraní nebo API používaného jejich zákazníky, obsahovalo bezpečnostní vady. Tato rozhraní jsou v programech sloužících pro komunikaci s poskytovatelem, monitoring služby, její orchestraci a řízení. Ve své podstatě bezpečnost a dostupnost všech cloudových služeb závisí na bezpečnosti základních API.

Tato rozhraní a API musí zajistit bezpečný chod pro autorizaci, autentizaci, šifrování, monitoring a ostatní klíčové funkce. Pokud nebude zajištěna bezpečná funkce těchto prvků, nemůžeme následně zajistit správné a bezpečné chování těchto procesů. A co víc. Mnoho společností přidává těmto „nebezpečným“ API svou přidanou hodnotu a tento produkt dále distribuují svým zákazníkům, což v důsledku může vést k dalšímu zvyšování bezpečnostních rizik [33].

Pro snížení těchto bezpečnostních rizik by měl poskytovatel služby sledovat aktuální dění na „poli“ bezpečnosti, dostatečně často aktualizovat svůj software a používat bezpečnostní záplaty. V případě nalezení problému musí poskytovatel neprodleně kontaktovat svého zákazníka a seznámit ho s potenciálními riziky. V ideálním případě pak poskytovatel prodiskutuje dostupné možnosti, jak by se dal daný problém řešit.

3.11 Rizika spojená se sdílením technologické slabiny (chyby) - Shared technology vulnerabilities

Poskytovatelé cloudových služeb nabízejí své služby klientům v podobě sdílení infrastruktury, platforem a aplikací. Jak je patrné z [23], tyto prostředky, ať už hardwarové či softwarové, nemusí být navrženy pro zajištění isolace přístupu jednotlivých uživatelů ve sdíleném prostředí cloud computingu. V důsledku této slabiny se stává celý systém zranitelný. Tento typ zranitelnosti je nadále sdílen skrz všechny své modely. Pokud se taková slabina vyskytne a nebude odstraněna, dochází k ohrožení celého cloudu daného poskytovatele, respektive všech jeho systémů a uživatelů. Dle [34] je tento typ útoků často využíván krackery např. k získání administrátorských oprávnění k danému systému nebo pro spuštění svých aplikací v kernel módu[16].

Proti této hrozbě se doporučuje použít obranná strategie, ve které bude do detailů popsán způsob zabezpečení sítě, aplikací, výpočetních jednotek, ukládacích médií, uživatelů a jejích přístupu. Nadále se bude striktně monitorovat veškerá aktivita spojená se službami IaaS, PaaS a SaaS. Nedílnou součásti jsou pravidelné aktualizace firmwaru a požívání bezpečnostních patchu (záplat) [23].

3.12 Zálohování a způsob odstraňování dat

Problematikou, spojenou se zálohováním se zabývá spousta odborné literatury. Já se v této části práce nebudu zabývat problematikou zálohování jako takového, jako spíše rozdíly v pohledu na zálohování v závislosti na modelu nasazení cloudu jako tomu je v [2]. Navzdory rozdílnostem v jednotlivých modelech existuje doporučení (pravidlo), které usnadní spánek lidem zodpovědným za firemní data. Jedná se pouze o uvedení způsobu

[16] Privilegovaný režim pro běh procesů v CPU.

a frekvenci zálohování požadovaných dat do smlouvy mezi poskytovatelem cloudových služeb a zákazníkem (SLA).

V případě veřejného cloudu kdy má uživatel všechna data u svého poskytovatele služby, je dobré daného providera donutit zálohovat právě pomocí výše uvedené SLA. Seriózní poskytovatel si však důležitosti zálohování musí být vědom, a tak by tuto „nadstavbu“ měl zaručit v rámci nabídky svých služby.

V případě privátního cloudu se může situace lišit dle toho, zda daná společnost má vlastní IT oddělení poskytující privátní cloud, nebo se o jeho zajištění stará externí firma. V případě provozování vlastního cloudu je pouze na dané společnosti, jakou strategii k zálohování příjme. Pokud je tento cloud poskytován externí firmou, objevuje se stejný problém jako u cloudu veřejného. Rozdíl však spočívá v lepších možnostech přizpůsobit strategii, týkající se zálohování podnikové politice.

Při využívání hybridního cloudu si zákazník rozděluje svá data na dvě skupiny. Tou první jsou „běžná“ uživatelská data, která nejsou pro chod firmy klíčová, a tak mohou být uložená ve veřejném cloudu. Těmi druhými jsou data, jejichž ztráta by mohla mít pro firmu existenční význam. Ta jsou uložena v cloudu privátním [1]. Záloha dat tak musí probíhat pro obě skupiny dat, avšak v privátním cloudu musí být daleko častější.

Dalším rizikem, které je mnohdy opomíjeno, je metoda odstraňování dat. Běžně se data na úložištích pouze zneplatní, ale ve skutečnosti na daném médiu stále existují. To pro běžné prostředí informační technologie, jak jí známe, teď nepředstavuje žádné bezpečnostní riziko. V prostředí cloud computingu však k takovýmto úložným médiím typicky přistupuje více uživatelů. Tito uživatelé sice mají omezený přístup pouze k vlastním datům, tato omezení však platí pouze pro platná data. Z toho vyplývá, že po „smazání“ dat, respektive uvolnění paměťového prostoru na úložném médiu, uživatelem X, může v budoucnu na tento prostor dostat práva uživatel Y. Pokud tato situace nastane, jeví se tento prostor uživateli Y jako prázdný, obsahuje však data uživatele X. Uživateli Y tudíž pro přístup k těmto datům stačí změnit bit platnosti dat. Z pohledu X je proto tento typ mazání dat naprosto nepřijatelný. Toto riziko může být odstraněno za pomocí nasazení sofistikovanějších metodik pro odstraňování dat. Jednou z možností použít uznávané metody, splňující normy amerického ministerstva obrany. Tato norma nese označení DOD 5220.22-M. Celé znění daného standardu je dostupné na [35].

3.13 Další rizika

- **Vzdálený přístup** - Vzdálený přístup ke službě je de facto jedním z hlavních rysů cloud computingu a může být realizován dvěma způsoby. Tím prvním, který je typický hlavně pro veřejný cloud, je prostřednictvím internetu. Druhým způsobem,

jenž se běžně využívá v případě privátního cloudu, je prostřednictvím intranetu[17]. Ačkoliv je v obou případech přístup ke službám lehce odlišný, požadavky na bezpečnou komunikaci jsou shodné. Těmito požadavky jsou důvěrnost a zachování integrity dat. Z hlediska zákazníka se tudíž jedná o klíčové vlastnosti, a proto se na eliminaci tohoto typu rizik musí klást velký důraz. Samotnou metodikou a technologiemi eliminujícími tento typ rizik se budu věnovat v další části této práce [1].

- **Omezený způsob kontroly** - Toto riziko vychází ze samotné povahy cloud computingu a týká se především veřejného cloudu. V podstatě se dá říci, že veřejný cloud je z velké části „nebezpečný“ právě kvůli omezené možnosti kontroly dodržování bezpečnostních politik a nutnosti důvěřovat svému poskytovateli [2]. Existují sice monitorovací nástroje, které zákazníkovi poskytují přehled o využívání služby, neřeknou však nic o porušování bezpečnostních politik nebo špatném typu zálohování, které jsou uvedeny v SLA. V porovnání s vlastním IT oddělením si zákazník nemůže kontrolovat fyzický přístup k zařízení, množství a kvalifikaci oprávněných osob s přístupem k používanému hardwaru či softwaru a mnoho dalších aspektů, které je nutné dodržet pro zachování správného a bezpečného fungování IT oddělení.

[17] Vnitřní podniková síť

4 Přístupy a metody pro odstranění a minimalizaci rizik spojených s cloud computingem

Ač si třeba mnozí po přečtení předchozí kapitoly řeknou, že využívání cloud computingu je nebezpečný, nemusí tomu tak být. Všechny výše uvedené hrozby byly známy ještě před rozmachem cloud computingu a tudíž existují techniky a metodiky, které tyto hrozby dokáží minimalizovat či úplně eliminovat nebo alespoň snížit jejích dopad na uživatele. Právě těmito metodikami se budu nyní zabývat v této kapitole. Dříve než tomu tak bude si musíme uvědomit několik skutečností.

Tou první je centrální správa bezpečnosti cloud computingu ze strany poskytovatele. Tato vlastnost nám oproti klasickým řešením může výrazným způsobem zvýšit bezpečnost našich dat a námi využívaných služeb. Duhou záležitostí, kterou musíme mít na paměti je fakt, že poskytovatel cloudových služeb, a to jak privátního, veřejného nebo hybridního, nám nemůže poskytnout 100% ochranu proti všem typům hrozeb. Tento fakt však není vždy zcela zřejmý. Pro jeho lepší uvědomění si zde budu parafrázovat Steva Rileyho, který je spoluautorem [2]. Steve Raley v kapitole 4 ve svém příkladu přirovnává bezpečnost v cloud computingu k bezpečností v běžném životě. Ve svém přirovnání říká: *„Ač má neprůstřelná vesta velmi dobré bezpečnostní vlastnosti proti střelnému zranění, neznamená to, že si ji budeme nasazovat před každým odchodem z domu. Důvodem, proč si jí nevezmeme je, že pravděpodobnost, že na nás bude někdo střílet je de facto nulová. Tudíž nemá smysl se snažit tuto hrozbu nadále snižovat. Navíc je tato vesta těžká, nepohodlná a mnohdy „společensky“ nevhodná a tak je svému nositeli v danou situaci pouze na obtíž“*. Stejné pravidlo platí i v prostředí cloud computingu. Ani zde není důvod aplikovat všechny bezpečnostní opatření. Jednak je to mnohdy zbytečné, nepohodlné a v neposlední řadě drahé. Nesmíme však zapomenout na to, že ne všechny bezpečnostní požadavky ze strany zákazníka se musí shodovat s bezpečnostní politikou poskytovatele. V takovém případě musí zákazník zvolit jiného poskytovatele nebo ze svých požadavků upustit. Nedá se totiž předpokládat, že by poskytovatel kvůli jednou zákazníku měnil svou bezpečnostní politiku a s tím i bezpečnostní politiku všech svých zákazníků. Nezapomínejme však ani na to, že bezpečnostní požadavky zvedají režii síťového provozu. V důsledku „přehnanosti“ těchto požadavků může být ovlivněn požadavek například na rychlost dostupnosti dat.

4.1 Okruhy zájmu pro minimalizaci bezpečnostních rizik

V této kapitole se podrobněji zaměřím na jednotlivé bezpečnostní okruhy, pomocí nichž lze výrazným způsobem zvýšit jak bezpečnost dat v cloudu, tak i námi využívaných cloudových služeb. Tato kapitola nebude obsahovat žádná přesná nastavení firewallu a podobně nýbrž obecná pravidla a metodiky, při jejichž dodržování se může výrazným způsobem snížit riziko zneužití nebo napadení cloudových služeb.

4.1.1 Stanovení bezpečnostní politiky a správa lidských zdrojů

Pokud se chceme efektivně bránit hrozbám plynoucím z využívání moderních technologií (v našem případě cloud computingu), musíme si nejdříve určit, co pomocí daných technologií chceme získat. Tento krok nebývá tak jednoduchý jak by se ve skutečnosti mohlo zdát. Mnoho lidí má v skutečnosti jen povrchní představu o tom co vlastně chce a čeho chce dosáhnout. Dalším krokem by mělo být vytvoření bezpečnostního protokolu, v němž by se měly nacházet informace týkající se zabezpečení v rámci IT.

Ač to na první pohled nemusí být patrné, lidský faktor je i v prostředí cloud computingu velice významný a tudíž se z pohledu bezpečnosti nemůže vynechat. V následujícím kroku by se s danými bezpečnostními politikami měli seznámit uživatelé tohoto systému, obvykle pracovníci firmy. Toto proškolení jednak snižuje riziko chyb personálu a jednak přesouvá část odpovědnosti na samotné zaměstnance. V rámci tohoto školení by se měl být personál seznámit s hlavními zásadami bezpečnosti v informační technologii [1]. Velká část bezpečnostních incidentů totiž vznikne v důsledku neznalosti uživatelů systému. Další část bezpečnostních úniků je tvořeno v důsledku využití této neznalosti pracovníku třetí stranou například pomocí phishingu[18].

Výše zmiňované kroky by měly být jakousi nultou fází při postupu odstraňování rizik spojených nejen s cloud computingem, ale se všemi problémy souvisejícími s bezpečností v rámci IT. Tato doporučení a mnoho dalších jsou používaná autory jak v [2], tak i v [17].

4.1.2 Správa identit, rolí a práv

Ve světě bezpečnosti IT mnohdy platí jedno paradoxní pravidlo a to, že největší hrozbou pro systém jsou uživatelé tohoto systému. Proto je naprosto nezbytné mít kontrolu nad právy přístupu jednotlivých uživatelů. Tento problém se dá vyřešit zavedením odlišných uživatelských rolí dle typů uživatelů přistupujících k dané službě a nadále těmto uživatelům umožnit přístup pouze k datům potřebným k jejich práci. V případě využívání softwaru jako služby (SaaS) jsou veškeré odpovědnosti týkající se dané problematiky přesunuty na stranu poskytovatele cloudových služeb. Poskytovatel by měl zákazníkovi zaručit, že používá procesy, zaručující monitoring a správu jednotlivých uživatelských rolí a práv přístupu k daným datům v závislosti na výše uvedených rolích. Přidělení jednotlivých rolí uživatelům je mnohdy označován jako Least Privilaged Principal (LPP) [17] a závisí na autorizačním procesu, který musí probíhat v souladu s dodržením vnitropodnikových bezpečnostních politik o který se i v tomto případě stará poskytovatel služeb. Tento přístup není důležitý pouze pro omezení práv „oprávněným“ uživatelů

[18] Podvodná technika, kdy se útočník snaží od uživatele získat jeho osobní údaje.

systému, ale i pro omezení přístupu uživatelům, kteří do systému nesmějí mít přístup [36]. Omezení přístupu jednotlivých uživatelů je označováno jako Role-Based Access Controls (RBAC) [17]. U cloudových služeb se často užívá zdvojený bezpečnostní mechanismus. Nejprve kontrolují přístup ke cloudu samotnému, potom ke cloudové službě. Příjemnou vlastností, kterou poskytovatelé mohou nabízet je tzv. SSO (Single-Sign-On, respektive Single-Sign-Off). Jedná se o metodu, která při využívání různých služeb od jednoho poskytovatele vyžaduje pouze jedno přihlášení, respektive odhlášení od všech služeb.

Pokud se připojujeme k veřejnému cloudu nebo privátnímu v rámci internetu, je zapotřebí další stupeň ochrany. Tato ochrana může být zajištěná na úrovní zařízení, kdy ke službě můžeme dovolit přístup pouze z daného pracovního stroje. Dalším způsobem ochrany je použití vhodného DLP (Data Leakage Provention) softwaru, který zaznamenává jakékoliv kopírování a určuje odpovědnost v případě ztráty dat [37].

Nezbytnou součástí tohoto bezpečnostního opatření je seznámit samotné uživatelé systému s jeho rolí v systému a tím i s jeho právy a povinnostmi, které z toho vyplývají.

4.1.3 Infrastruktura firmy a bezpečná komunikace v cloudu

Ačkoliv se při využití cloud computingu může celé IT oddělení přesunout do cloudu a tím výrazným způsobem ulehčit společnosti starosti ohledně správy, zabezpečení a podobně, je infrastruktura firmy (firemní sítě) stále důležitou součástí bezpečnostní politiky. Tato vnitřní síťová infrastruktura nám totiž určuje, jakým způsobem se připojujeme k poskytovateli cloudu. Pokud si tuto vnitřní síť dobře nezabezpečíme, nemusí nám být zbylé bezpečnostní politiky a pravidla uplatněná na straně poskytovatelé nic platná. K těmto účelům může posloužit firemní firewall a systémy IDS a IPS (Intrusion Detection Systém a Intrision Prevention System). Poslední dva výše zmiňované systému slouží jako prevence proti průniku do sítě a v případě průniku pro jeho detekci [37].

Na druhé straně zabezpečení infrastruktury na straně poskytovatelé vyžaduje daleko více práce. Poskytovatel musí brát v potaz mnoho faktorů, které tuto bezpečnost ovlivňují. Tyto faktory jsou podrobněji popsány v normě ISO 27002, kterou se budu zabývat v kapitole 0 této diplomové práce.

Jak z povahy cloud computingu vyplývá, tak jedním požadavků je, aby data v době přenosu mezi poskytovatel a uživatelem nebyla v ohrožení. Posílají-li se data v rámci firemního intranetu, není riziko příliš vysoké. Komunikujeme-li prostřednictvím internetu, musíme zasílaná data zašifrovat. Ben Halpert ve své knize [2] upozorňuje na jistá bezpečnostní úskalí, která souvisí s uchováním šifrovacího, respektive dešifrovacího klíče. Hlavní důraz pak klade především na požadavek aby klíč nebyl uložen v cloudu, ale v prostředí uživatelského informačního systému. Dle [37], ale řada profesionálních poskytovatelů nabízí například standardizované nebo speciální zákaznické služby jako je

PKI (public key infrastructure), jenž umožňují bezpečný, ověřený a šifrovaný přenos dat. Pokud poskytovatel cloudových služeb dodává i síťové komunikační služby, integrované služby jako MPLS (Multiprotocol Label Switching) mohou zajišťovat přísné oddělení datových toků jednotlivých uživatelů. K přenosu dat v rámci jednotlivých MPLS sítí se využívá VPN (Virtual Private Network) sítí, jenž zajišťují vytvoření bezpečného „tunelu" pro komunikaci. Sítě typu MPLS-VPN sice poskytují základní ochranu, mohou však být vylepšeny například o šifrované tunely SSH (Secure Shell), IPSec či TLS/SSL[19][20]. Nejlepšího způsobu ochrany lze dosáhnout vytvořením dedikovaného spoje přímo mezi uživatelskou organizací a poskytovanými službami v datovém centru poskytovatele. Toto řešení však nemusí být vhodné pro společnosti s velkým množstvím působišť [37].

4.1.4 Fyzické zabezpečení datového centra

Tento okruh zabezpečení může zákazník ovlivnit pouze pokud provozuje vlastní cloudové řešení, v opačném případě se všechny starosti přesouvají na poskytovatele služeb. Obecně by se dalo říci, že pro cloud computing platí stejná pravidla fyzického zabezpečení pro datové centrum jako pro ostatní datová centra nezávisle na typu služeb, která poskytuje. Tyto pravidla se dají dohledat takřka ve všech literaturách a jsou obecně známá. Počínaje správným výběrem umístění datového centra, přes přístup pouze autorizovaných osob, ochraně proti požáru a konče zajištěním subdodavatele elektrické energie a plánem pro extrémní situace jakými jsou požáry, povodně, zemětřesení a další. Přehled těchto požadavků na fyzické zabezpečení datového centra lze najít např. ve [36].

Problematiky týkající se tohoto typu zabezpečení si však jsou v dnešní době vědomy snad všechny společnosti, nebo by alespoň měly být. Proto se dá předpokládat, že renomovaní poskytovatelé cloudových služeb budou mít tuto problematiku precizně řešenou. V důsledku toho budou moci poskytnout vyšší stupeň ochrany, než jaký je dostupný v klasickém datovém centru průměrné společnosti s vlastním IT oddělením.

4.1.5 Správa služby a proces obnovy dat

Správa poskytované služby sice neleží v rukou zákazníka, avšak existují způsoby, pomocí kterých lze dosáhnout vyšší bezpečnosti poptávaných služeb. Pro zvýšení bezpečnosti poskytovaných služeb je potřeba se ujistit, že poskytovatel do svých služeb a systémů implementuje nejnovější bezpečnostní záplaty, čímž je udržuje stále bezpečné vůči známým způsobům útoku. Dle [37] mohou být součástí těchto služeb i spolehlivé

[19] Jedná se o privátní komunikační transportní protokol založený na symetrické kryptografii.
[20] Více informací o daných technologiích najdete např. na http://technet.microsoft.com/en-us/library/cc737154(v=WS.10).aspx a http://technet.microsoft.com/en-us/library/cc784149(v=ws.10).aspx

procesy ITIL[21] (Information Technology Infrastructure Library) [38], jako řízení změn a problémů. Dosáhnout těchto vlastností lze například pomocí uvedením těchto požadavků v SLA[22] (Service Level Agreement).

Při snaze minimalizovat bezpečnostní rizika bychom neměli zapomínat ani na situace, kdy nám žádná bezpečnostní opatření nepomohla a je potřeba vrátit vše do stavu před útokem. Právě toto by měla být jedna z klíčových oblastí zájmu firmy přecházející na technologii cloud computingu. Spolehliví poskytovatelé tento katastrofický scénář mají vyřešený například zálohováním všech zákazníkových dat na jiné fyzické úložiště. Dle [17] však existují zcela zásadní rozdíly ze stran poskytovatelů v době a „pohodlnosti" obnovy požadovaných dat do původního stavu před útokem.

4.1.6 Monitorování služeb a ověření bezpečnosti

Při sepisování SLA a stanovování všech bezpečnostních požadavků je mnohdy zákazník ujišťován, že vše co si žádá je pro daného poskytovatele samozřejmostí. Zákazníkovi může být ze strany poskytovatele dodáno několik nástrojů umožňujících monitorování aktivit. Jak uvádí [17] se toto monitorování dá rozdělit do dvou skupina to fyzických a kybernetických událostí. Do první skupiny lze zařadit události jako je natáčení videa, sledování do zabezpečených prostor, sledování poplašných senzorů, napájení atd. Do druhé kategorie patří metody nazývané Housekeeping, Treath Monitoring a Incident response. Podrobný popis těchto tří metod naleznete např. v kapitole č. 10 zdroje [17].

Pokud však na straně zákazníka vznikne sebemenší podezření, že ne vše co poskytovatel slibuje bude splněno, doporučuje se provést například penetrační testování[23] s pomocí nezávislé třetí strany [17]. V případě odhalení nedodržování některého z bodu uvedeného v SLA ze strany poskytovatele lze doporučit buď změnit poskytovatele, nebo s ním vyjednat změnu bezpečnostních politik na jeho straně.

4.2 Bezpečnostní audit

Volný překlad definice pojmu audit dle [39] zní: "*Audit je systematický, nezávislý a dokumentovaný proces, jehož cílem je získání záznamů, tvrzení nebo jiných relevantních informací o zkoumané problematice. Tyto informace následně objektivně hodnotí splněnost všech kritérií daného auditu.*"

[21] Jedná se o celosvětově nejuznávanější sbírku doporučení pro řízení a správu IT systémů.
[22] Smlouva o poskytování cloudových služeb
[23] Penetrační testování patří mezi techniky etického hackingu. Jde o testování za účelem nalezení co nejvíce chyb a následného vniknutí do systému. Získané výsledky se následně použijí pro opravu nalezených slabin v systému.

Jinými slovy je bezpečnostní audit (v oblasti IT) proces nebo sada postupů, jejichž cílem je ověřit bezpečnost síťové infrastruktury firmy a všech „entit“ s ní spojených. Výsledkem auditu je protokol, který obsahuje vyhodnocení všech testů. Tyto audity se provádí kvalifikovanými společnostmi v oboru počítačové bezpečnosti. Jednou z nevětších a neznámějších auditorských společností je například Ernst & Young, která dle [40] patří mezi čtyři největší auditorské společnosti na světě. Dle [41] tato společnost provedla v roce 2012 bezpečnostní audit normy ISO 27001 pro služby společnosti Google. Mezi další celosvětové společnosti zabývající se audity patří například PricewaterhouseCoopers (PwC). Aby vypovídající hodnota výsledků těchto testů byla průkazná, všechny se řídí dle normy ISO 19011. Samotná norma ISO 19011 přitom vychází z normy ISO 9000 [39].

Bezpečnostní audity jsou záležitostí středně velkých až velkých společností (cca nad 50 zaměstnanců), to ovšem neznamená, že se menších firem netýká. V malých podnicích s několika málo zaměstnanci se v mnoha případech bezpečnost příliš neřeší a zabezpečení mnohdy bývá založeno spíše na důvěře. Ovšem pokud v podniku chybí určité směrnice ohledně bezpečnosti a společnost se začne rozrůstat, bezpečnostní riziko prudce vzroste [42]. Tímto důvodem jsou samotní zaměstnanci. Pro více informací ohledně této problematiky si přečtěte kapitoly 4.1.1 a 4.1.2. Nemluvě o problematice s úschovou osobních dat zaměstnanců, kterou nařizuje tuzemská legislativa. Dalším problémem zabezpečení firem bývá nedostatečná kvalifikace pracovníků, odpovídajících za bezpečnost. Začne-li společnost řešit problém týkající se zabezpečení ICT (informační a komunikační technologie) až při výskytu problému, mohou se náklady na jeho odstranění vyšplhat mnohonásobně výše, než jak by tomu bylo v případě zavedení „preventivních opatření“.

V tak rozsáhlém prostředí jaké tvoří cloud computing, je provádění bezpečnostních auditů nutností. Tyto audity mohou plnit funkci například kontroly bezpečnostních požadavků, pomoc při řízení bezpečnosti datového centra, dokonce mohou zvyšovat jak transparentnost bezpečnostních opatření, tak i konkurenceschopnost poskytovatele na trhu. Poslední dvě výše zmiňované vlastnosti jsou poskytovány pomocí norem, jako jsou ISO 27001, které jsou na poli bezpečnosti informační technologie celosvětově uznávané [43].

Samotný proces provádění bezpečnostního auditu z velké části záleží na velikosti společnosti, v níž je prováděn. Rovněž metodika samotného procesu se liší v závislosti na společnosti provádějící audit. Vezmeme-li tuzemskou společnost zabývající se bezpečnostními audity jakou je např. IBAcz, která je dle [44] v rámci IBA Group jedním z největších dodavatelů ICT ve střední a východní Evropě. Tato firma rozděluje proces provádění auditu do tří skupin (pilířů). První pilíř se zabývá technickým zabezpečením zákazníka. K testování slouží penetrační testy, jež využívají metodiky blackbox[24] a whitebox[25] testování. Více informací o penetračním testování se dozvíte z [45]. Druhý pilíř představuje kontrolu bezpečnosti interních procesů zákazníkovy společnosti a jejích

[24] Kontrola bezpečnosti vůči veřejně známým chybám v použitých nástrojích.
[25] Kontrola bezpečnosti interních struktur řešení IT.

souladu s nařízenou bezpečnostní politikou. To v sobě mimo jiné zahrnuje kontrolu aktivit, bezpečnostní politiky a managementu rizik (disaster recovery, obnova dat a zálohování). Posledním pilířem je personální audit, jenž se zaměřuje na rizika, vznikající při napadení společnosti zevnitř. Tento krok obsahuje kontrolu přístupu zaměstnanců k citlivým dokumentům, způsob práce s nimi a v neposlední řadě kontroluje, zda byla zachována integrita dat.

4.3 Normy

Pokud chceme přistoupit k otázce zabezpečení informačního systému zodpovědně, musíme dodržovat určitý postup, pravidla a omezení. Naštěstí je otázka bezpečnosti na poli IT už dlouhou dobu, a tak si nemusíme tyto postupy vymýšlet. Pro tyto účely nám poslouží mezinárodní standardy (normy), které mohou být v rámci jednotlivých států či firem modifikovány. Všechny nicméně mají stejný základ.

Díky spolupráci Mezinárodních standardizačních organizací ISO a IEC (International Electrotechnical Commission) mohla vzniknout celá řada norem. Tyto standardy velmi často vznikají jako výběr „toho dobrého“ buď z jiných standardů, nebo věcí prověřených praxi. V případě norem ISO/IEC týkajících se bezpečnosti, byly jako podklad použity britské normy. Protože výčet všech norem týkajících se bezpečnosti by byl nad rámec této diplomové práce, budu se v následujících částech zabývat pouze některými z nich [46].

Použití těchto standardů nám zaručí mnoho výhod. Pomocí norem například můžeme dosáhnout určité úrovně zabezpečení, zaručit konzistenci a kvalitu naších bezpečnostních pravidel, můžeme zvýšit důvěryhodnost své organizace, zvýšit spokojenost zákazníků atd. [47] V tak rozsáhlém prostředí jako je cloud computing je využívání norem naprostou nezbytností. Tyto standardy poskytovatelům slouží jako důkazní materiál pro jeho stálé a potencionální zákazníky, že jsou jejich služby zabezpečeny. A také zvedají renomé poskytovatele a cenu na trhu cloud computingu. Další výhodou, plynoucí z využívání těchto standardů je jaké si „know-how“, kdy poskytovatel svému zákazníků sdělí, že plní normu XY a zákazník automaticky ví (nebo si může dohledat), které bezpečnostní prvky a mechanizmy může od daného poskytovatele poptávat. Navíc má poskytovatel toto tvrzení podloženo certifikátem od standardizační společnosti, která mu daný certifikát vydala. Cílem těchto norem je tak zjednodušit postup zabezpečení a jednoznačně definovat okruhy, které jsou zabezpečeny dle požadovaných kritérií. Nesmíme však zapomenout na skutečnost, že tyto standardy nám říkají pouze to, jakého stavu musíme dosáhnout. Neříkají ovšem, pomocí jakých postupů toho máme docílit.

Dále bych chtěl dodat, že tato část práce je zaměřená na stručný popis vybraných bezpečnostních norem. Hlavním účelem není plné seznámení čtenářů s těmito standardy, ale pouze předání základních informací, které s nimi souvisí.

4.3.1 Normy rodiny ISO/IEC 27000

Norma ISO/IEC 27000

Jedná se o první normu řady ISO 27000, jenž je součástí ISO/IEC ISMS (Information Security Management Systems). V rámci rodiny ISO 27000 je tento standard označován jako Overview and Vocabulary. Plná dokumentace je k dispozici na [46], proto nadále budu z této dokumentace vycházet. Jak je z názvu patrné, obsah této normy tvoří převážně slovníček pojmů, přehled a popis ISMS.

Obsah ISMS se skládá ze systematických doporučení pro návrh, implementaci, realizaci, řízení, monitoring, správu a především vylepšení bezpečnosti podnikových informačních systémů. Princip zabezpečení je založen na systému odhadu rizik pro danou společnost. Tyto rizika se následné posuzují na základě požadavků dané firmy. Princip úspěšnosti této metodiky závisí na několika bodech počínaje porozumění jednotlivým potřebám bezpečnosti v informatice a konče přezkoumáváním vhodnosti daného zabezpečení a vytvářením vhodných modifikací.

Norma ISO/IEC 27001

Tato norma je v rámci rodiny ISO 27000 někdy také označována jako Requirements [46]. Dle [48] byla tato norma publikována v říjnu 2005 a nahradila starší britský standard BS7799-2. Jedná se o specifikace ISMS. Tato specifikace jednak rozšiřuje původní BS7799-2 a jednak tento standard harmonizuje s ostatními normami řady 27000. Cílem tohoto standardu je poskytnout model pro návrh, implementaci, řízení, monitoring a správu ISMS. Tato norma zavádí model PDCA[26] (Plan, Do, Check, Act), který je využíván i v dalších normách řady 27000. To ve skutečnosti znamená, že fáze plánování, implementace, kontrola (sledování) a vylepšení jsou 4 kroky, které postupně a cyklicky aplikujeme při zavádění a provozu ISMS, a to v organizaci jakékoliv velikosti. Ač se tato metodika z pohledu velikosti společnosti nemění, implementace se může výrazným způsobem lišit, a to dle charakteru dat, počtu uživatelů nebo rozsahu systému.

Kromě výše uvedeného obsahuje tato norma také:

- Požadavky na implementaci ISMS
- Požadavky na implementaci opatření dle ISO/IEC 17799
- Popis požadavků, které je nutné splnit pro certifikaci dle ISO/IEC 27001

[26] Plánování, Implementace, Kontrola, Vylepšení

Norma ISO/IEC 27002

Jak uvádějí zdroje [46] a [48], jedná se o přejmenovanou normu IS0 17799, jenž obsahuje stovky potenciálních bezpečnostních kontrolních mechanizmů, které napomáhají zabezpečit a udržet požadavky kladené normou ISO/IEC 27001. Tyto okruhy se týkají všech úrovní zabezpečení počínaje kontrolou bezpečnostní politiky, přes fyzické zabezpečení až po kontrolu řízení bezpečnostních incidentů.

4.3.2 Další normy

Z hlediska bezpečnosti nejsou důležité pouze standardy zajišťující bezpečný informační systém. Stejně důležitou roli mají i standardy dokazující, že daný informační systém bezpečným ve skutečnosti je. Mnohým, byť i třeba zákazníkům cloud computingu stačí, že jejích poskytovatel plní např. normu ISO 27001. Mohou se však vyskytnout i jedinci, kteří mohou požadovat další důkaz, že tomu tak je. K tomu může posloužit norma ISO/IEC 15408-1 (až 3), jejímž hodnotícím kritériem je seznam podmínek, které má systém plnit. S pomocí této normy lze také definovat základní bezpečnostní parametry, které má síť splňovat [49].

Další normou, které pomáhá zlepšit zabezpečení je např. ISO/IEC IS 13335-2. Tento standard kompletně popisuje řízení bezpečnostních rizik v informatice. Doplňky této normy obsahují příklady přístupů při odhadu bezpečnostních rizik a seznam možných hrozeb, zranitelných míst bezpečnostních kontrol. Tato norma se dle [50] často uplatňuje při nastavování frameworky pro definici bezpečnostních rizik na interní úrovni společnosti.

5 Přístupy a řešení vybraných významných firem poskytujících cloud computing

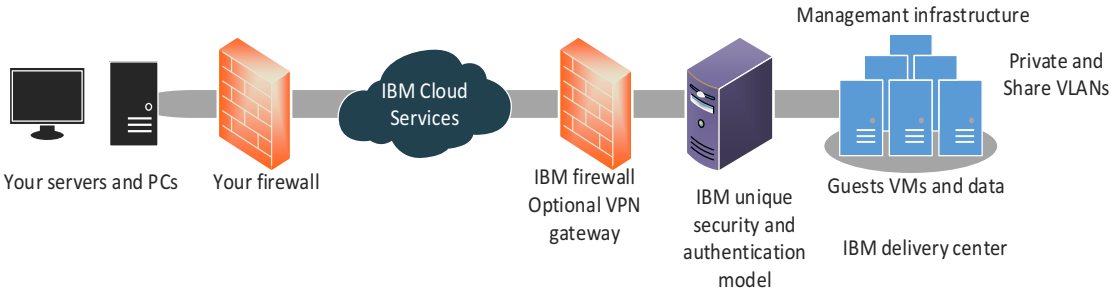
V této kapitole si představíme tři významné hráče na poli poskytování cloud computingu. Výběr těchto poskytovatelů neprobíhal pouze na základě velikosti či renomé dané společnosti, ale byl brán ohled i na jistou působnost daných firem na tuzemském trhu. Cílem tohoto výběru bylo dosáhnout přijatelnějšího uživatelského postoje čtenářů této diplomové práce vůči výše zmiňovaným společnostem.

Dále bych chtěl dodat, že cílem této kapitoly není kompletní výčet a popis všech nabízených cloudových produktů daných firem, ale pouze seznámení čtenářů se současnými možnostmi na tuzemském trhu.

5.1 IBM

První vybranou společností, která zde bude popsána, je společnost IBM. Jedná se o americkou společnost s více než stoletou historií. Za tuto dlouhou historii si firma vydobyla značné renomé na trhu a nasbírala řadu cenných zkušeností. V České republice je tato firma v povědomí veřejnosti známá především díky prodeji výpočetní techniky, převážně notebooků. Odborná veřejnost však tuto společnost zná i jako významného hráče v nabídce zboží na poli superpočítačů (Watson), serverů a datových center. IBM se o cloud computing začala poprvé zajímat v roce 2007, kdy si vytvořila svůj první vlastní privátní cloud a následně po dohodě s Googlem začala na amerických univerzitách poskytovat cloudové služby [51]. 4. června 2013 provedla IBM akvizici společnosti SoftLayer, jenž zaujímá významný postoj (21000 zákazníků ve 140 zemích světa) na poli v poskytování IaaS (Infrastructure as a Service) [52].

IBM je v poskytování cloudových služeb velice různorodé, protože poskytuje IaaS, PaaS i SaaS (více informací o modelech cloudových služeb najdete v kapitole 2.8), a to v podobě veřejného, privátního i hybridního cloudu (více informací o modelech nasazování cloudu v kapitole 2.7). Obrázek 12 ilustruje IBM SmartCloud. Jedná se o koncepci, do které v IBM spadají všechna výše uvedená řešení.



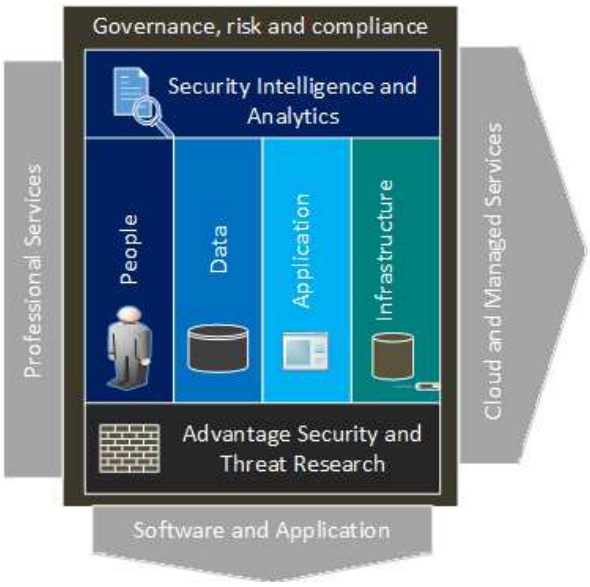
Obrázek 12 - IBM SmartCloudu (Autor – upraveno dle: [53])

Na stránkách této společnosti lze zdarma stáhnout nástroje IBM SmartCloud a IBM SmartCloud Analytic. Tyto nástroje slouží pro sestavení vlastního cloudového řešení typu IaaS a seznámení se se základní analytickou sadou nástrojů. Oba výše zmiňované balíčky jsou poskytnuty zdarma po dobu 60 dnů. Veškeré další nástroje jsou poskytovány jak nadstavba a vyžadují telefonickou nebo emailovou objednávku.

Problematiku zabezpečení uložených a posílaných dat v cloudu řeší IBM pomocí vlastního bezpečnostního frameworku. Tento bezpečnostní framework pomáhá chránit uživatele, software i hardware. Dle IBM viz [54] na zlepšování tohoto frameworku pracuje přes 6000 odborníků ve 14 laboratořích, zabývajících se bezpečností v oboru IT. Dále dle IBM tento framework denně zaznamená přes 13 miliard bezpečnostních událostí. Tento framework splňuje normu ISO 27001. Podrobný popis tohoto frameworku lze najít na odkazu, který je umístěn ve spodní části této stránky[27]. Obrázek 13 znázorňuje schematický nákres tohoto frameworku. Jak uvádí Nick Coleman v [55], z hlediska bezpečnosti IBM splňuje normy jako ISO 9000, ISO 20000, ISO 27001 a ISAE3402.

Dále IBM nabízí širokou škálu pomocných bezpečnostních prvků. Pomocí těchto prvků lze de facto nastavit bezpečnost ve své organizaci doslova na míru. Za vše následně hovoří získání ceny za nejlepší řešení zabezpečení cloud computingu za rok 2012 od SC Magazine, který se zabývá bezpečností na poli IT [56].

[27] http://www.ibm.com/ibm/files/X869751J69908G27/1securityandCloudIBM_382KB.PDF



Obrázek 13 - IBM Security Framework (Autor - upraveno dle: [54])

V neposlední řadě zaslouží IBM pochvalu i za zpracování svých webových stránek. Ty jsou přehledné, intuitivní a ke každé nabízené službě je dodán základní popis, plná dokumentace a krátké seznamovací video.

5.2 VMware

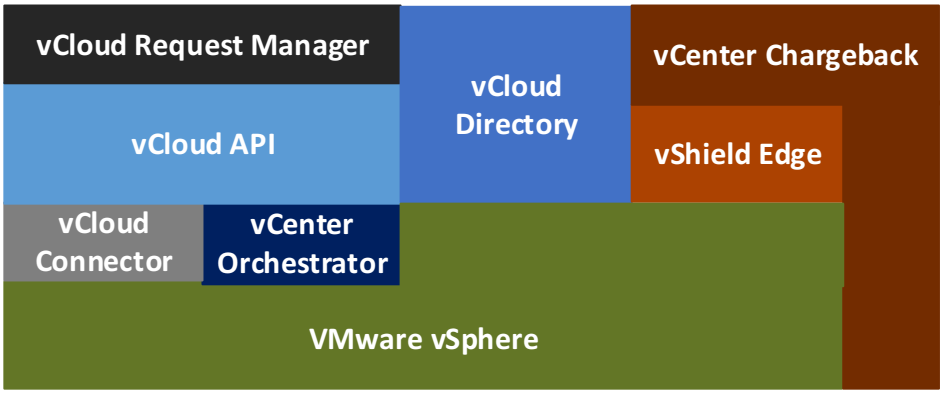
VMware je americká společnost, která je na trhu relativně krátkou dobu, a to od roku 1998. Navzdory tomu je právě tato společnost mnohými považována za průkopníka v oblasti virtualizace a možnosti rozvoje cloud computingu. Dle [57] na virtualizační technologii této společnosti pracovalo v roce 2009 okolo 80 % serverů. Dle [58] byl tento podíl na konci roku 2012 okolo 65 %. V rámci České republiky se podíl pohyboval dokonce okolo 90%. Tento propad (v rámci celosvětového využívání služeb) je způsoben zvýšenou konkurencí na trhu oproti minulosti. Přesto takovýto podíl vypovídá o kvalitách služeb nabízených danou společností. Dle výše uvedeného zdroje a [59] má tato firma vizi pokročit od virtualizace jednotlivých serverů až po virtuální datová centra. Vzniklo by tak softwarově definované datové centrum, které by naplňovalo určitá cloudová řešení.

Díky vysokému podílu na trhu v oblasti virtualizace a výtečným technologickým vlastnostem měla tato společnost předpřipravenou cestu pro vstup na trh v oblasti cloud computingu. VMware poskytuje služby napříč všemi modely nasazení cloudu. V oblasti privátního cloudu VMware praktikuje přístup založený na bezpečnostních zónách[28]. K těmto službám mohou být poskytovány jak nástroje pro správu zabezpečení, monitoring,

[28] Více na http://www.arm.com/products/processors/technologies/trustzone.php

tak i analýzu možných bezpečnostních událostí. Tyto nástroje poskytuje rovněž pro všechny modely nasazení cloudu [60].

Dále je touto společností nabízeno řešení s označením vCloud. Dle použitého zdroje [60] se jedná o řešení, při kterém se mohou požadavky zákazníka přenést z vnitřního privátního cloudu na cloud provozovaný právě společností VMware. Toto řešení významným způsobem zvyšuje flexibilitu služeb. Schéma jednotlivých částí, z nichž se vCloud skládá, je znázorněno na obrázku č. 14.



Obrázek 14 - Přehled komponent obsažených ve vCloud (Autor - upraveno dle: [60])

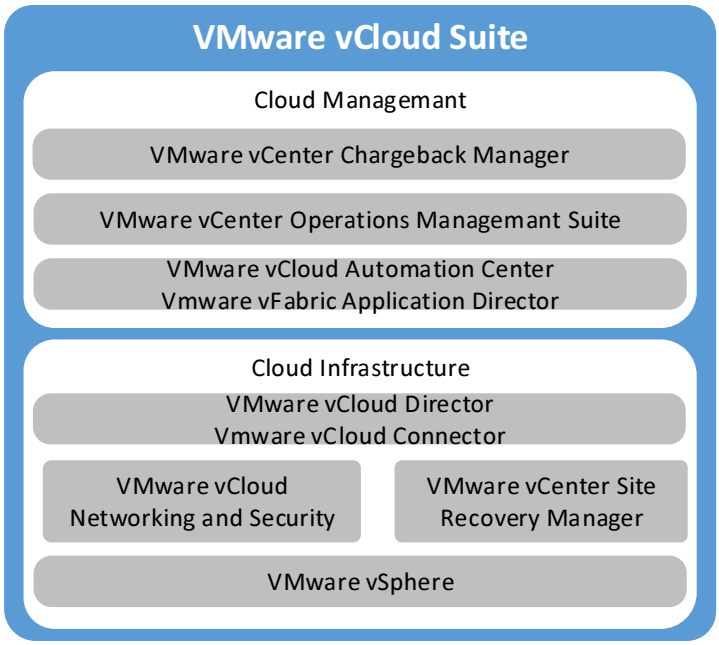
V oblasti zabezpečení cloud computingu čerpá VMware zkušeností především z oblasti virtualizace, jenž cloud computing významným způsobem využívá. Kromě výše uvedených technologických nástrojů se VMware zaměřuje v oblasti bezpečnosti i na největší zdroj bezpečnostních rizik. Touto oblastí jsou samotní uživatelé služeb. V tomto ohledu VMware poskytuje vlastní tréninkové, školící a certifikační programy umožňující rozšíření znalostí a zkušeností souvisejících s bezpečnosti nejen na poli cloud computingu. Tyto programy jsou primárně určeny administrátorům a lidem zodpovědným za bezpečnost služeb[29].

Jak už v dnešní době bývá u renomovaných poskytovatelů cloudových služeb zvykem, tak i VMware nabízí základní prostředí pro nasazení cloudu na omezenou dobu zdarma. Tímto prostředím je VMware vSphere with Operation Managemant. Tento nástroj poskytuje základní prvky pro správu a zabezpečení cloudových služeb. K tomu přidává možnost vyzkoušet si některé přídavné balíčky jako VMware vCloud Director nebo VMware vSphere Data Protection Advanced. Tyto služby lze zdarma využívat po dobu 60 dnů.

Portfolio služeb této společnosti je však daleko rozsáhlejší. Patří tam služby jako VMware vCloud Suite, jenž umožňuje kompletní integraci IaaS do prostředí cloudu. Navíc

[29] Víc informací na http://mylearn.vmware.com/mgrReg/plan.cfm?plan=32565&ui=www_cert

tento balík poskytuje nástroje pro kompletní správu, řízení a zabezpečení těchto služeb. Kompletní popis služeb obsažených v tomto balíčku je znázorněn na obrázku č. 15.



Obrázek 15 - VMware vCloud Suite (Autor - upraveno dle: [60])

Tato společnost, ač je ze všech tří popisovaných nejmladší, dokáže nabídnout nejefektivněji využitelný systém služeb, a to jak v oblasti virtualizace, tak i cloud computingu. Tato efektivita pramení převážně ze skutečnosti, že VMware dokáže velmi přesně, a pro zákazníka šetrně, přizpůsobit svou technologii dle jeho požadavků. Cílem je, pokud možno, co nejmenší zásah do stávajícího datového centra zákazníka, což u ostatních společností nebývá vždy zvykem [58].

5.3 Microsoft

Poslední a na tuzemském trhu nejznámější společností je Microsoft, která je na tuzemském trhu známá především díky operačnímu systému Windows a kancelářskému balíčku Office. Stejně jako předchozí dvě (IBM a VMware) je i Microsoft společností, která vznikla ve Spojených státech amerických, a to v roce 1975. Přestože Microsoft byl původně zaměřen pouze na vývoj operačních systémů, dnes je jeho působení daleko rozsáhlejší. V současné době tato společnost nabízí například herní konzoli Xbox, výše zmiňovaný kancelářský balíček Office, řadu operačních systémů, služby cloud computingu atd. Technologie cloud computingu vážněji upoutala pozornost Microsoftu již v roce 2008

a v dnešní době nabízí řadu cloudových služeb napříč všemi modely nasazení cloudu (IaaS, PaaS a SaaS) [61].

Nejznámějším produktem dané společnosti typu PaaS je bezesporu Windows Azure. Dle slov Microsoftu je Azure: *„Flexibilním operačním systémem, který je doručován jako služba. Jeho hlavní funkcí je vývoj, testování, hosting a správa aplikací."* Azure podporuje řadu jazyku jako .NET, PHP, Java, Ruby a Python [62]. Tento nástroj umožňuje běh vývojového prostředí na straně Microsoftu. V důsledku toho umožňuje vývojářům pokračovat v rozpracované práci na jakémkoliv zařízení bez nutnosti instalací potřebných vývojových nástrojů. Microsoft umožňuje uživatelům si tuto službu vyzkoušet zcela zdarma, a to po dobu 30 dnů. Nutností je projít registrací, která je prováděná pomocí telefonního čísla a čísla kreditní karty. Tím si Microsoft ověří existenci daného uživatele a zamezí opětovné nové registraci stejného uživatele za účelem využívat tuto službu i nadále zdarma. Další službou, kterou v oblasti PaaS Microsoft nabízí je například databáze SQL Azure [61].

Na poli SaaS nabízí Microsoft celou řadu produktů. Jako první se zmíním o emailové službě. Microsoft dříve nabízel dvě emailové služby, tudíž by se dalo říci, že si sám sobě konkuroval. V průběhu tohoto roku však došlo ke sjednocení těchto služeb pod službu s názvem Outlook. Další službou v této kategorii, kterou Microsoft nabízí je kancelářský balík Office 365. Jedná se o balík se stejnými funkcemi jako klasický Office, který je ovšem uložený v cloudu a přináší tak s sebou všechny výhody plynoucí z použití cloud computingu. V poslední době se Microsoft snaží zapůsobit i na poli cloud gamingu, a to za pomoci výše uvedené konzole Xbox. Celkově Microsoft ve svém obchodu nabízí přes 400 cloudových služeb, tudíž je nelze, a v tomto případě to ani není účelem, všechny popsat.

V oblasti privátních cloudových služeb používá Microsoft technologie jako Windows Server 2012 a s vlastním Hyper-V[30] v kombinaci se System Center 2012. Jak uvádí Microsoft v [63], tato kombinace poskytne společnosti potřebnou virtualizaci, možnost řídit koncové služby a soustředit zájem podnikání na přidanou hodnotu. Tabulka 1 obsahuje hrubé srovnání produktů Windows Server 2012 s produktem od vSphere v5.1 od společnosti VMware. Tato komparace je brána z pohledu Microsoftu. Podrobnější informace lze nalézt ve výše uvedeném dokumentu. Microsoft nabízí jak Windows Server 2012, tak i System Center 2012 i ve zkušební verzi a to na 180 dnů.

[30] Podrobnější informace o činnosti hypervizoru najdete na koci kapitoly 2.1 této diplomové práce.

Tabulka 1 - Srovnání produktů Windows Server 2012 Hyper-V s VMware vSphere 5.1 Ent Plus dle Microsoftu (Autor – upraveno dle: [64])

Capability	Resource	Windows Server 2012 Hyper-V	VMware vSphere 5.1 Ent Plus
Scalability, Performance, Density	Active Virtual Machines Per Host	1,024	512
	Memory Per Virtual Machine	1 TB	1 TB
	Virtual Processors Per Virtual Machine	64	64
	Maximum Nodes Per Cluster	64	32
	Maximum Virtual Machines Per Cluster	8	3
	SR-IOV with Live Migration support	Yes	No
Storage	Native 4KB disk support	Yes	No
	Maximum Virtual Disk Size	64 TB	2 TB
	Encrypted Cluster Storage	Yes	No
Secure Multitenancy	Open Extensible Switch	Yes	Closed
	Resource Meeting	Yes	Chargeback Req.
Flexible Infrastructure	1GB simultaneous Live Migrations	Unlimited	4
	10GB Simultaneous Live Migrations	Unlimited	8
	Live Storage Migration	Yes	Yes
	Shared-Nothing Live Migration	Yes	Yes
	Network Virtualization	Yes	VXLAN Req.
High Availability	Virtual machine replication	Yes	Yes
	Guest OS Application Monitoring	Yes	API Only
	Guest Clustering With Live Migration & Dynamic Memory	Yes	No

Jak se shodují [65] a [66], zaujímá Microsoft z hlediska bezpečnosti svých služeb obdobnou strategii, jaká je aplikována v normě ISO 27000. Tato strategie vyplývá z analýzy rizik a jejich následné eliminace. Využívá k tomu model PDCA (viz kapitola 4.3.1). V problému fyzického zabezpečení jsou plněny normy ISO/IEC TR 18044 a NIST SP800-61[31]. Dále Microsoft plní nomu ISO 27001 a atesty SAS (Statement of Auditing Standard) 70 typu I a II[32]. V roce 2011 Microsoft podstoupil certifikaci FISMA (Federal Information Security Management Act) [33] [61].

[31] Více informací o daných normách můžete získat na http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35396 a http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

[32] Více informací naleznete na http://sas70.com/

[33] Více na http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Navzdory odlišnostem napříč všemi výše uvedenými poskytovateli jak k nabízeným službám, tak i k jejich zabezpečení, mají tyto společnosti některé vlastnosti společné. První z nich je snaha poskytnout svým zákazníkům služby v nejlepší možné kvalitě. Druhou je zajištění bezpečnosti svých služeb na stejné, nebo lepší úrovni než jaká by byla dosažená v datových centrech jejich zákazníků. Přidanou hodnotou jsou zde navíc všechny výhody, plynoucí z využití technologie cloud computingu.

6 Popis praktické části

V této části bude autorem navrhnuta metodika pro odhalování bezpečnostních rizik při nasazení technologie cloud computing. Dále zde bude popsán postup nasazení privátního cloudu pomocí nástrojů, které poskytuje společnost Microsoft. U každého z těchto nástrojů bude nastíněná použitá konfigurace a především popsány bezpečnostní mechanizmy, které jsou těmito nástroji poskytovány. Dále bude provedeno zhodnocení zabezpečení daného řešení a jeho testování. V poslední části budou autorem navrhnuty úpravy výše použité metodiky testování za účelem dosažení transparentnějších výsledků z hlediska bezpečnosti.

6.1 Návrh metodiky pro odhalování bezpečnostních rizik v prostředí cloud computingu

Metodika navržená v této diplomové práci vychází z předpokladu nasazení privátního cloudu. Tím se eliminují rizika spojená například s poskytovatelem cloudových služeb, jak tomu je v případě cloudu veřejného. Tato metodika dělí proces analýzy a kontroly bezpečnosti do čtyř základních kategorií, které jsou dále členěny do dílčích částí. Povaha této metodologie by se vzhledem k ISO/OSI modelu dala nazvat jako Buttom-Up, kdy danou analýzu začínám na fyzické úrovni a postupně systematicky postupuji k úrovni nejvyšší (aplikační). Výjimku tvoří pouze skupina rizik, jež nejsou spojená s technologickým řešením při nasazování a provozování cloud computingu. Dodržením postupu při kontrole bezpečnostních politik a nastavení, by se měla odhalit převážná část rizik spjatých cloud computingem.

6.1.1 Metodika pro odhalování rizik spojených s netechnologickou části cloud computingu

V této části se budeme zabývat postupem odhalování rizik, která nemají spojitost s technologickým řešením. Jedná se především o problematiku pochopení problémů spojených s danou technologií. Dále odhalení znalosti jednotlivých administrátorů, existence bezpečnostní politiky, organizace bezpečnosti, atd. Mnou navrhovaná metodika se snaží zahrnout všechny aspekty spojené s touto problematikou do čtyř bodů, které jsou podrobněji rozepsány v následující části práce.

- **Rizika plynoucí z neporozumění prostředí cloud computingu** – Dříve, než se začneme zabývat metodikou odhalováním konkrétních rizik, se musíme ujistit, zda strana nasazující cloud computing rozumí dané problematice. Z výsledků této analýzy následně můžeme vyvodit závěry, jenž nám můžou poodhalit body zájmu našeho dalšího zkoumání.

- **Zajištění dostatečné úrovně znalostí u administrátorů** – Jak již z dříve uvedených částí této práce vyplývá, nejčastějším zdrojem chyb je lidský faktor. Důsledky chyb způsobených uživateli se liší v závislosti na možnostech (právech) daného uživatele. V případě chyby administrátora mohou mít tyto chyby naprosto fatální důsledky. Proto je vhodné si ověřit znalosti a zkušenosti jednotlivých administrativních pracovníků, popřípadě je zdokonalit v rámci některého ze školících programů. Problematika nedostatečných znalostí se netýká pouze administrátorů, ale všech uživatelů systémů. Z těchto důvodů je nutné se během zkoumání rizik zaměřit i na existenci školícího programu, nebo jakéhokoliv jiného materiálu, který by uživatelům dodal požadované znalosti.

- **Organizace bezpečnosti a bezpečná administrace** – V prostředí cloud computingu se mnohdy jedná o velice rozsáhlá datová centra. V takových případech je naprosto nutná existence dokumentu popisujícího bezpečnostní politiku dané společnosti. Tento dokument by měl na různých přístupových úrovních detailně popisovat práva a odpovědnosti jednotlivých uživatelů, nastavení systémů a jeho požadavky. Součástí tohoto dokumentu by měl být i tzv. krizový plán. Tím by měla být zajištěna organizace bezpečnosti. V tomto dokumentu by neměla chybět pasáž popisující jakým způsobem a ze kterých míst a za pomocí jakého softwaru by měl mít uživatel přistupovat ke službám. Ověření existence a kvality zpracování takového dokumentu by se tedy mělo stát nezbytnou součástí při odhalování bezpečnostních rizik. V dalších fázích odhalování rizik by se rovněž mohla, ne-li měla, kontrolovat konfigurace obsažená ve výše uvedeném dokumentu s konfigurací skutečnou.

- **Politika akceptovatelných hesel** – Ačkoliv by se z logického hlediska mohl tento bod sloučit s předchozím, z důvodu závažnosti možných důsledků a velmi časté absenci dané politiky tomu tak nebude. Problém spočívá ve skutečnosti, že zřejmě každý si uvědomuje, že by si svá data měl chránit. Už ale ne každý si uvědomuje, že špatné heslo může znamenat nulovou ochranu. Proto by se při odhalování rizik souvisejících s cloud computingem, a se zabezpečením obecně, měla pozornost věnovat existenci politiky akceptovatelných hesel.

6.1.2 Metodika pro odhalování rizik spojených s fyzickou bezpečností

Tato rizika nesouvisí pouze s oblastí cloud computingu, ale všeobecně se zabezpečením datových center či jednotlivých serverových středisek. Rizika se v tomto případě dají rozdělit do tří kategorií.

- **Rizika spojená s fyzickým zabezpečením serverů** – tato část kontroly je zaměřená na fyzické umístění serverů v budově a na zabezpečení přístupu pouze oprávněným osobám. Obecně platí zásada, že se nedoporučuje mít datové centrum

v nízko položené oblasti (údolí, sklep atd.). Obzvláště pokud se jedná o oblast s reálnou možností záplav. Samotná místnost musí být dobře zabezpečená z důvodů minimalizování šance na vniknutí neoprávněné osoby. To vše by mělo být doprovázeno monitorováním výše uvedených prostor a vedením záznamů o vstupu do objektu.

- **Rizika spojená s kontrolou přístupu oprávněných osob** – V této části se autor zaměří primárně na pracovníky, který disponuje právy pro přístup do datového centra. Tento personál by tedy měl projít určitou bezpečnostní prověrkou a jeho množství by mělo být stanoveno na minimální akceptovatelný počet. Dále by před vstupem do datového centra měla proběhnout kontrola identity dané osoby, a to pokud možno na dvojí úrovni. Například pomocí přístupového hesla a biometrických údajů.

- **Rizika spojená s existencí krizového plánu** – Dále by pro minimalizaci rizik selhání datového centra měl existovat krizový plán a mechanizmy umožňující jeho realizaci. Mezi tyto mechanizmy může patřit umístění protipožárních vstupních dveří, zajištění hasícího mechanizmu, existence sekundárního nezávislého dodavatele elektrické energie, UPS systémů či záložních serverů umístěných v dostatečné vzdálenosti od daného datového centra. Tato vzdálenost je relativní vzhledem k povaze datového centra a typu služeb, které poskytuje.

Pro odhalení těchto rizik je zapotřebí mít fyzický přístup do datového centra, popřípadě k bezpečnostní dokumentaci, která obsahuje popis výše zmiňovaných bezpečnostních mechanizmů.

6.1.3 Metodika pro odhalování rizik spojených se síťovou bezpečností

Tato rizika jsou spojená především s topologií podnikové sítě, prvků, které používá a jejich následné konfiguraci. Stejně jako v minulém, tak i v tomto případě se dají rizika rozdělit do tří kategorií.

- **Rizika spojená s typem síťové topologie** - Tento bod je důležití zejména z pohledu zajištění spolehlivého a bezporuchového chodu sítě. Dle doporučení společností CISCO v kurzu CCNA Explorotion je vhodné využívat některou ze „standardních“ topologií jakými jsou kruh, hvězda, strom a další. V rámci těchto topologií je vhodné přijmout opatření, která minimalizují rizika selhání sítě. Jako příklad zde uvedu implementaci druhého kruhu v případě vybudování kruhové topologie.

- **Rizika spojená s použitými typy síťových prvků a jejích firmwaru** – Dalším bodem zájmu metodiky jsou samotné aktivní síťové prvky jako například routery a switche (směrovače a přepínače) a firmware, který obsahují. V dnešní době nabízí trh řadu inteligentních aktivních síťových prvků, které jsou schopny provádět inspekci provozu na L2 vrstvě. Na základě této inspekce se pak rozhoduje, zda se jedná o korektní data nebo o právě probíhající útok, který je třeba zastavit. Konkrétně se jedná o switche s funkcí dynamic ARP inspection, broadcast-storm control a DHCP snooping. Nasazením těchto síťových prvků se eliminuje nutnost mít tuto ochranu implementovanou v operačních systémech připojených počítačů. V případě takového typu napadení, bude tento útok zastaven dříve, než stačí dosáhnout na připojená zařízení. Jedná se zejména o útoky zaměřené na manipulaci síťového provozu.

  Dále je potřeba zkontrolovat verzi používaných firmwarů u daných zařízení, update verze daného firmwaru a zjistit jejich bezpečnostní slabiny (pokud jsou známy). Následně vůči těmto slabinám implementovat požadovaná bezpečnostní opatření. Pokud nemáme přímý přístup k daným zařízením, můžeme danou síť monitorovat. K těmto účelům slouží například nástroj NMAP. Tento nástroj slouží ke zjištění, zda je zařízení zapnuté, verzi použitého firmwaru, určení dostupných portů, služeb a mnoha dalších informací potřebných pro určení konfigurace síťových prvků a následnou identifikaci jejich zranitelnosti.

- **Rizika spojená s chybnou či nedostatečnou konfiguraci síťových prvků** – Rizika obsažená v tomto bodu se týkají především správné konfigurace síťových prvků. Pro minimalizaci těchto rizik se musíme zaměřit na nastavení týkající se zabezpečení vzdáleného přístupu k těmto prvkům, rozdělení rolí oprávnění dle typu přistupujících uživatelů, správné nastavení směrování a směrovacích protokolů, šifrování komunikace mezi jednotlivými prvky sítě, šifrování nastavení jednotlivých prvků, vypnutí nepoužívaných portů a služeb, nastavení VLAN, access listů, konfigurace firewallu, popřípadě využití DMZ atd. Pro usnadnění, zpřehlednění a minimalizaci chyb při této konfiguraci lze u výrobků společnosti CISCO využít speciální software SDM (Security Device Manager), který svým uživatelům umožní nastavit požadované vlastnosti v grafickém prostředí. Dále tento nástroj zajistí zakázání všech nepotřebných portů a služeb na daném zařízení. V případě absence přímého přístupu k síti lze jako v předchozím případě použít monitorovací nástroj NMAP, který nám může zobrazit požadované informace o konfiguraci daných síťových prvků. Na základě této konfigurace lze následně určit slabiny daného systémů.

Pro komplexní odhad rizik systému obsažených v posledních dvou bodech lze použít některou z metodik zabývající se penetračním testováním. Pro dosažení požadované úrovně testu je však zapotřebí mít kvalitního testera, který daný test provede

v požadovaném rozsahu (v rámci celé infrastruktury) a do požadované hloubky (využití všech dostupných nástrojů pro otestování všech typů zranitelnosti).

6.1.4 Metodika pro odhalování rizik spojených se zabezpečením použitého softwaru, poskytovanými službami a organizací uživatelských rolí

Tato část metodiky pro odhalování bezpečnostních rizik je zaměřená na kontrolu zabezpečení na softwarové úrovni. Spadá sem zabezpečení použité virtualizační technologie, operačních systémů, jejich služeb, požitých aplikací, nástrojů pro správu uživatelů a jejich účtů, ale i použití antivirů, anti spywarů[34], anti malwarů[35], atd.

- **Typ operačního systému a virtualizační technologie** - S každým typem operačního systému (OS) jsou spojená určitá rizika a technologické slabiny. Proto je velice důležité kontrolovat dostupnost nejnovějších aktualizací a bezpečnostních záplat. Dále je vhodné zvolit nejnovější verzi OS. Tyto nové verze s sebou sice mohou přinést nová bezpečnostní rizika, ta se však záhy odstraní právě pomocí výše zmiňovaných aktualizací. Přidanou hodnotou novějších OS však bývá ponaučení z chyb (nejen bezpečnostních), které obsahovaly systémy starší.

  Následující bod kontroly by měl připadnout kontrole technologie použité virtualizace. Virtualizační technika se pro různé typy virtualizace napříč různými společnostmi nepatrně liší a každá obsahuje svá bezpečnostní rizika. Zvažme situaci, kdy máme například virtuální server od společnosti VMware. Tatáž společnost pro zlepšení zabezpečení daného serveru nabízí balíček s názvem VMware ESXi 3.5. IBM pro ochranu virtuálních strojů běžících na technologii od VMware nabízí službu s názvem Security Virtual Server Protection for VMware. Z důvodu nízké úrovně zabezpečení základních virtualizačních technik [52] se doporučuje využít nadstavbových služeb pro zajištění lepší bezpečnosti těchto strojů.

- **Konfigurace OS** – V této části by se měla kontrola zaměřit na role a funkce nastavené v OS. Pro zajištění bezpečné konfigurace se musí dodržovat určité zásady. Mezi ty hlavní patří přidělení danému serveru pouze potřebných rolí, které má server vykonávat. Nastavení využití bezpečnějších protokolů, pokud to situace dovoluje (např. využívat protokol HTTPS namísto HTTP). Povolení přístupu přes šifrovaný VPN tunel, nastavení typu a frekvence zálohování dat, povolení šifrování ukládaných dat, zapnutí sofistikovanějších metod autentizace (povolení využití

[34] Nástroj pro odhalování škodlivého softwarů, jehož účelem je špionáž dané oběti a získávání jejich zpravidla citlivých dat.
[35] Z anglického **mal**icious soft**ware** což lze přeložit jako škodlivý kód. Jedná se o škodlivý software, jehož primárním účelem je zpravidla získání citlivých dat nebo privilegovaného přístupu.

čtečky otisků prstů pro přihlášení do systému), nastavení politiky hesel, nastavení logování provedených změn a aktivit na serveru, atd.

- **Typy používaných aplikací a frekvence jejich aktualizací** – Tato část metodiky pro odhalování bezpečnostních rizik je věnována samotným nainstalovaným aplikacím na serveru. Striktně se doporučuje používat pouze softwary „prověřených“ společností, které je nutné nadále udržovat v aktuálním stavu pomocí pravidelných aktualizací. Dodržením tohoto pravidla se redukuje riziko použití škodlivého softwaru nebo riziko využití některé ze slabin softwaru stávajícího. Stejně jako v předchozím bodě i zde platí pravidlo instalovat pouze nezbytný software. Minimalizuje se tak riziko zneužití chyby, zefektivní administrace a zredukuje vytížení zdrojů daného serveru.

- **Antivir, anti spyware, anti malware** – Tento bod obsahuje kontrolu přítomnosti ochranných programů, jakými jsou například antivirus, anti-malware, atd. Samozřejmostí je nasazení prémium verzí těchto softwaru a nikoliv takzvaných free licencí, které neposkytují dostatečnou ochranu. V neposlední řadě musí proběhnout kontrola aktuálnosti databáze hrozeb daných programů. Samozřejmostí by rovněž měl být software detekující bezpečnostní incidenty. Jako alternativa k výše zmiňovaným programům se může v prostředí cloud computingu využít sofistikovanějších softwarů, jakým je například Microsoft Systém Center 2012 Endpoint Protection, který zajišťuje nejen plnohodnotnou ochranu celého systému.

- **Izolace uživatelů, jejich dat, procesu a služeb, restrikce uživatelských přístupových práv** – Při odhalování bezpečnostních rizik musíme věnovat pozornost také uživatelům systému. Musíme zajistit izolaci jednotlivých uživatelů, respektive jejich skupin, správné rozdělení práv a povinností a přístupu k jednotlivým datům, službám a procesům. K těmto účelům slouží řada nástrojů, které disponují grafickým rozhraním. Toto grafické rozhraní následně administrátoru ulehčí jak samotné vytváření uživatelských skupin a přiřazování patřičných práv, tak i následnou kontrolu tohoto nastavení. Jako příklad zde uvedu produkt Virtual Machine Manager společnosti Microsoft patřící do rodiny Systém Center 2012.

- **Kvalita a rozsah monitorovacích prostředků** - Naprosto nezbytnou součástí každého většího IT oddělení musí být monitorování provozu. Pole působnosti a kvalita daného monitoringu je závislá jak na bezpečnostních požadavcích společnosti, tak na její rozsáhlosti. Protože navržená metodika má ambice nejen problémy odhalovat, ale i zajistit aby k nim v budoucnu nedocházelo, je funkce kontrola monitorovacích funkcí naprosto nezbytná.

Pro správné odhalení rizik spadajících do této skupiny je zapotřebí mít buď patřičný monitorovací software, který nám poskytne patřičné informace o typu OS, jeho nastavení,

použitých aplikacích a rozdělení rolí a práv jednotlivých uživatelů, nebo mít přístup k prvkům (serverům atd.) a nástrojům pro správu konkrétního datového centra.

6.2 Použité technologie

Pro praktickou část této diplomové práce byly autorem použity zejména technologie společnosti Microsoft. Důvodů k této volbě bylo hned několik. Prvním z nich je rozsáhlost nasazení tohoto operačního systémů na serverových platformách. Druhým důvodem je 180 denní zkušební doba, jež uživatelů poskytuje dostatečnou dobu na vyzkoušení produktu. V neposlední řadě při rozhodování pomohl i partnerský program MSDN AA[36], který platí mezi Fakultou elektrotechniky a informatiky Univerzity Pardubice a Microsoftem. Tento program umožňuje studentům využívat produkty dané společnosti pro domácí použití.

První důležitou komponentou pro poskytování cloudových služeb je Microsoft Windows Server 2012, jenž tvoří základní prostředí pro běh všech dalších potřebných komponent. Detailnější nastavení tohoto serveru bude popsáno v další části této diplomové práce. Další nezbytnou komponentou je Microsoft Systém Center 2012 Configuration Manager. Před instalací tohoto softwaru je však potřeba u Windows Serveru doinstalovat funkci pro podporu .NET frameworku 3.5, který se v základní konfiguraci neinstaluje. Dále je potřeba nainstalovat Microsoft SQL Server 2012, který Microsoft nabízí také zdarma. Při instalaci tohoto serveru je potřeba nainstalovat vlastnost umožňující full-textové vyhledávání[37], která bude vyžadována dalšími balíčky v rámci Systém Center 2012. Součástí výše zmiňovaného balíčku Systém Center 2012 je i software pro zvýšení možností zabezpečení a usnadnění jeho řízení. Tím je Systém Center 2012 Endpoint Protection SP1.

Dalším nezbytným softwarem pro nasazení a správu cloudu, který byl použit, je Microsoft Systém Center 2012 Service Manager. Tento produkt není běžně dostupný zdarma. Avšak díky programu MSDN AA jsem mohl tento produkt zdarma získat, což mě výrazným způsobem ulehčilo vybudování a následnou správu potřebných služeb. Výše zmiňovaný nástroj však pro svůj chod potřebuje mít nainstalovaný Microsoft Report Viewer, který je dostupný na stránkách Microsoftu. Dále pro správu rolí jednotlivých uživatelů a správu diskového úložiště byl použit software Systém Center 2012 Virtual Machine Manager. Dalším použitým balíčkem v rámci Systém Center 2012 je Operation Manager. Tento nástroj slouží pro monitorování heterogenního a cloudového IT prostředí. Kromě toho nám nabízí možnost vytvářet reporty o nashromážděných údajích. Před dokončením instalace tohoto softwaru však bylo potřeba do systému nainstalovat Server Virtualization Management Pack.

[36] Microsoft Developer Network Academic Alliance
[37] Jedná se o techniku hledání řetězců v dokumentech a databázích, které jsou předem indexované.

Dále na straně přistupujícího klienta byl použit operační systém Windows 7 Professional. Pro usnadnění přístupu k použitému serveru byla využitá technologie pro vzdálený přístup. K tomuto účelů posloužil software třetí strany TeamViewer 8, který je pro nekomerční účely dostupný zdarma. Pro práci se získanými instalačními balíčky byl použit nástroj Deamon Tools Light. Dále pro virtualizaci klientských stanic byl použit VMware Player 5.0.2.

6.3 Nasazeni privátního cloudu a testování jeho zabezpečení

V této kapitole se autor věnuje procesu nasazování výše zmiňovaných technologií spolu s detailnějším popisem jejich nakonfigurovaných parametrů. Dále bude provedeno testování zabezpečení a to na základě výše uvedené metodiky. Právě dle výše uvedené metodiky bude tato kapitola rozdělená na čtyři části, a to z důvodů lepšího mapování metodiky na proces nasazování privátního cloudu.

6.3.1 Proces nasazování cloud computingu související s netechnologickou částí

V této části metodiky pro odhalování rizik uvádím čtyři body, na které by se měla osoba provádějící kontrolu zaměřit. První z nich hovoří o rizicích plynoucích z nepochopení prostředí cloud computingu. Troufám si tvrdit, že tato rizika v tomto případě nehrozí. Druhý bod hovoří o kontrole úrovně znalostí jednotlivých administrátorů a možných rizicích, která vyplývají z nedostatku vědomostí. Zde už narážíme na možný problém, který vyplývá z mých de facto nulových zkušeností v tomto oboru. Ve třetím případě se metodika zaměřuje na existenci dokumentu, popisující bezpečnostní politiku. Tento požadavek však vyplývá z předpokladu rozsáhlého datového centra, které v tomto případě nemáme. Proto bude tento krok ignorován. Posledním bodem zájmu metodiky je politika akceptovatelných hesel. Tato politika zprvu nebyla zavedena, avšak služby rodiny Windows Systém Center 2012 její nasazení pro svůj chod vyžadovaly. Konkrétně se jednalo o balík Configuration Manager, který následně vyžadoval i změnu hesla ve Windows Server 2012.

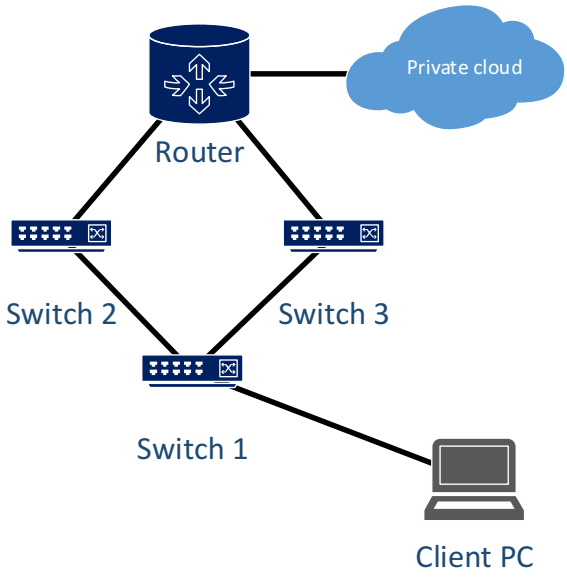
6.3.2 Proces nasazování cloud computingu související s fyzickou bezpečností

Této části nechci věnovat velkou pozornost, a to hned z několika důvodů. Jednak se v mém případě jednalo o laboratorní prostředí, které se s prostředím datového centra nedá srovnávat, navíc bych se nerad dopouštěl spekulací. Tyto spekulace by se týkaly hlavně prvního (rizika spojená s fyzickým zabezpečením serverů) a třetího (rizika spojená s existencí krizového) bodu, jimiž se daná metodika zajímá. Věnujme se tedy zbývajícímu (druhému) bodu dané problematiky. Tím je kontrola přístupu oprávněných osob. Ačkoli v laboratoři normálně probíhá výuka, v době mého působení byl již semestr ukončen. V důsledku toho byl přístup do daných prostor značně omezen. Pro získání přístupu do výše uvedené místnosti jsem musel na recepci předložit průkaz studenta, pomocí něhož byla ověřena jak moje identita, tak i to, že jsem pořád studentem univerzity. Dále patřičnou osobou na recepci bylo u mnou uvedené osoby ověřeno, zda jsem s ní domluven na přístupu do dané učebny. Tento postup proto považuji za dostatečný. Nutno dodat, že ne vždy byl tento postup striktně dodržen, což se z bezpečnostního hlediska může považovat za nepřípustné. Je také zapotřebí dodat, že v případě skutečného datového centra by tato metodika byla nedostatečná.

6.3.3 Proces nasazování cloud computingu související se síťovou bezpečností

Protože cílem této diplomové práce je nasazení cloudového řešení, vytvoření metodiky na ověřování bezpečnosti v prostředí cloudu a následné použití této metodiky pro odhalení bezpečnostních rizik, nebyl zde důvod budovat rozsáhlou vnitropodnikovou síťovou topologii. Proto byla autorem v této práci použita pouze provizorní síťová topologie, která obsahuje tři switche a jeden router. Model obsahující tři switche byl zvolen z důvodu dosažení lepší dostupnosti v případě výpadku buď switche dva, nebo tři. Obrázek 16 znázorňuje schéma vybudované síťové infrastruktury. Již ze znázorněného schématu je jasné, že síťová topologie a její realizace mají nemalý podíl na zabezpečení, dostupnost a kvalitu poskytovaných služeb. Druhým bodem, kterým se máme dle metodiky zabývat je kontrola rizik spojených s typy použitých prvků. V mém případě se jednalo o síťové prvky společnosti Cisco. Konkrétně se jednalo o switche řady Crystals 2960 a router řady 2800. Ani jedno ze zařízení bohužel nedisponuje speciálními schopnostmi, jakými jsou například dynamic ARP inspection, broadcast-storm control a DHCP snooping. Absence těchto vlastností limituje daná zařízení v možnostech nastavení požadovaného zabezpečení. Proto při budování rozsáhlejší sítě, ve které by bylo plánováno využití daných prvků, bych doporučoval doplnit tyto zařízení o prvky zajišťující vyšší stupeň ochrany. Například využití routeru řady 500 od společnosti Cisco. Podrobná specifika použitých zařízení jsou umístěna na CD přiloženém k této diplomové práci.

Daleko lepším řešením než je použití routeru řady 500 ve stávající infrastruktuře, se zdá být využití virtuálních síťových prvků. Tyto prvky s sebou přináší mnoho výhod jako možnost centrální správy, zvýšenou flexibilitu, lepší škálovatelnost bezpečnosti, atd.



Obrázek 16 - Síťová infrastruktura

Posledním bodem zájmu autora dle navržené metodiky v rámci dané kategorie je nastavení samotných výše uvedených síťových prvků. V rámci konfigurace zabezpečení obou použitých zařízení bylo nastaveno přístupové heslo jak při pokusu o přihlášení k routeru, tak i do enable módu, a to pomocí příkazu secrete. Dále byl zaheslován přístup ke konzoli a telnetu. Navíc hesla byla skryta pomocí MD5 šifry. Bylo nastaveno odhlášení uživatele po určité době nečinnosti. Následně byly vypnuty všechny nepoužívané porty a na směrovači nastavené příslušné VLAN. Dále byl využit Spaning Tree Protokol. Při přístupu ke switchi nebyla opomenuta ani kontrola založená na MAC adrese. Na routeru byly použity access listy, které mají filtrovat nežádoucí provoz. U směrovače byl nastaven rozsah povolených IP adres, kterým byl umožněn přístup. Nebyla však nastavená různá administrátorská práva, a to z důvodu existence pouze jednoho administrátora. Proto tento bod nepovažuji za prohřešek vůči bezpečnosti sítě. Stejně tak i nešifrování komunikace v rámci směrování není považováno vzhledem k existenci jednoho routeru za chybu v rámci bezpečnosti. Za bezpečnostní nedostatek ovšem lze považovat nevyužití systému SDM od společnosti Cisco, který zakáže všechny nepoužívané služby a napomáhá eliminovat chyby při konfiguraci v rámci zabezpečení. Následně může být tento nástroj využit k tvorbě robustnějších pravidel pro access listy. Je také doporučeno nahradit přístup přes telnet za přístup pomocí SSH. Dále nebyly použity časové access listy, které by napomáhaly filtrovat síťový provoz v předem definovaných časových intervalech. Dalším

nedostatkem dle metodiky je nedodržení žádné politiky hesel u síťových prvků. Všude bylo použité stejné heslo, které je ke všemu velmi slabé. Kompletní nastavení síťových prvků lze najít na CD, které je přiloženo k této diplomové práci.

6.3.4 Proces nasazování cloud computingu související se zabezpečením použitého softwaru

Prvním bodem zájmu navrhnuté metodiky pro odhalování rizik je typ OS a virtualizační technologie. Jako OS byl použit již zmiňovaný Windows Server 2012, který pro virtualizaci využívá platformu Hyper-V. Pro zvýšení stupně zabezpečení byly použity nejnovější dostupné aktualizace. Avšak žádný nadstavbový software zvyšující bezpečnost serverového virtuálního prostředí nebyl použit. Tento nedostatek je proto z hlediska použité metodiky považován za možné bezpečnostní riziko.

Dalším bodem zájmu používané metodiky je konfigurace samotného OS. V tomto případě byla snaha nainstalovat pouze nezbytně nutné role a funkce potřebné pro nasazení privátního cloudu. Mezi tyto role a funkce patří například Active Directory Domain Service, služba pro správu souborů a úložiště, IIS (Internet Information Server) server, rozhraní .NET Framework 3.5 a 4.5, nástroj pro vzdálenou správu serveru, rozšířené služby IIS, správa zásad skupin, atd. Jako nadstavba z bezpečnostního hlediska byly na server nainstalovány služby Active Directory Federation Services a nástroj BitLocker Drive Encryption a v neposlední řadě funkce pro zálohování systému. Další služby nebyly instalovány z důvodu redukce zátěže serveru a také jejich nejisté využitelnosti. Dalšími službami, které by mohly zlepšit bezpečnost a zvýšit dostupnost serveru v rámci datového centra by mohly být clustering s podporou převzetí služeb při selhání, služby umožňující ověření pomocí bezpečnostního certifikátu, Windows Biometrick Framework a některé další. Poslední zmiňovaná služba by však vzhledem k absenci čtečky otisků prstů na serveru nemohla být použita. Pro více informací o výše uvedených službách doporučuji navštívit stránky Microsoftu.

Dalším bodem zkoumání mnou použité metodice jsou samotné aplikace a frekvence jejich aktualizace. V tomto konkrétním případě se jedná hlavně o SQL Server 2012 a rodinu programů Systém Center 2012. Při instalaci obou výše zmiňovaných softwarů byly použity updaty dostupné ze strany Microsoftu. Za zmínku stojí funkce obsažená v Systém Center 2012 Managemant Center, která vyžaduje aplikaci silného hesla. Heslo musí mít alespoň 8 znaků, musí obsahovat malá i velká písmena a alespoň jedno číslo. V důsledku takto nastavené politiky je uživatel donucen změnit uživatelské heslo do Windows Serveru 2012. Při využití funkce umožňující přihlašování na SQL server v rámci hesla platného pro Windows Server 2012, se následně změní přístupové heslo i pro SQL server. Vzhledem k povaze všech použitých aplikací na serveru (rodina Systém center 2012, SQL Server 2012, TeamViewer8, Deamon Tools Lite), až na poslední zmiňovanou, si troufám tvrdit, že se jedná o věrohodný a prověřený software, který s sebou

nepřináší další rizika například v podobě obsahu škodlivého kódu. Dále je potřeba dodat, že po nainstalování všech aplikací byla provedena jejich aktualizace. Tento krok zajisté přispěl k lepšímu zabezpečení systému. Z pohledu bezpečnosti vzhledem k použité metodice považuji tento bod za zcela splněný.

Třetím bodem v pořadí jsou ochranné systémy jako firewally, anti spyware, anti malware, atd. V tomto případě byl použit nástroj Systém Center 2012 Endpoint Protection, který plní funkce ochrany před viry, spyware, malwary, rootkity[38], apod. Tento software nadále disponuje možností centrální správy bezpečnostních zásad, umožňuje odhalovat hrozby na základě podezřelého chování, spolupracuje s bránou firewall, atd. Při nastavování daného produktu bohužel nebyly prozkoumány všechny možnosti, které jsou uživatelům nabízeny. V tomto konkrétním případě byl tento software použit pro detekci hrozeb. Dále byl proveden test vzdáleného spuštění kontroly disku. Protože tento nástroj umožňuje daleko rozsáhlejší možnosti zabezpečení, považuje samotnou existenci tohoto produktu za pouze uspokojivé splnění daného bodu zabezpečení.

Čtvrtým bodem zájmu metodiky v této oblasti je izolace uživatelů, jejich dat, procesů a služeb. Na izolaci jednotlivých uživatelů a jejich přístupových práv se myslelo již při konfiguraci síťových prvků. Klíčovou roli v tomto bodě však hrají balíčky služeb rodiny Systém Center 2012. Konkrétně se jedná o Configuration Manager, Service Manager a Virtual Machine Manager. V rámci jednotlivých balíčků byly vytvořeny služby, k nimž měli mít uživatelé přístup. Konkrétně se jednalo o poskytnutí části procesorového výkonu a nepatrného prostoru v paměti RAM. Rád bych zde uvedl, že původní myšlenkou bylo poskytnout uživatelům možnost poptávat místo na fyzickém médiu. V průběhu konfigurace se však ukázalo, že pro tyto potřeby je nutné vlastnit úložiště typu SAN[39] (Storage Area Network), který jsem neměl k dispozici. Dále byly vytvořeny uživatelské skupiny, nakonfigurována přístupová práva k jednotlivým službám, dokonce proběhla konfigurace, při které bylo určeno, kolik příslušných zdrojů může každý uživatel spotřebovat. Systém následně sám zajistil izolaci jednotlivých uživatelů, konkrétně se o tuto činnost postaral Virtual Machine Manager. V důsledku malého množství použitých služeb, uživatelských skupin, druhu rolí a poskytovaných služeb, proběhla konfigurace relativně hladce. Vzhledem k výše uvedeným faktů považuji tento bod, jemuž se použitá metodika věnuje, za dostatečně zabezpečený.

Posledním krokem, kterému se daná metodika věnuje, je monitoring prostředků, provozu a uživatelů cloudových služeb. Pro tyto účely byl použit nástroj Operation Manager, který je součástí rodiny Systém Center 2012. Vzhledem k nízkému provozu a malé aktivitě jednotlivých použitých uživatelů v nasazeném prostředí cloud computingu, nebyly dosažené adekvátní výsledky z hlediska monitoringu provozu. V prostředí reálné firmy však tento nástroj dokáže poskytnout velice cenné služby. V tomto případě se nástroj využíval převážně ke sledování dostupnosti vytvořených služeb v době jejich nasazování. Dále byl tento nástroj používán ke kontrole správného nastavení parametrů nabízených

[38] Software umožňující získat privilegovaný přístup k systému.
[39] Jedná se o datovou síť sloužící pro připojení externích zařízení k serverům.

služeb a kontrole přihlašování jednotlivých uživatelů. Z bezpečnostního hlediska však monitorovací služby nebyly využity dostatečně. Částečný podíl viny na tom však nese prostředí, v němž byla technologie nasazována.

6.4 Zhodnocení navržené metodiky a návrh jejích možných modifikací

Před samotným hodnocením navržené metodiky a debatě o jejích možných modifikacích bych chtěl zdůraznit, že pro dosažení objektivního hodnocení nově navržené metody testování bezpečnosti je potřeba provést více testů v odlišných testovacích prostředích. Provedením pouze jednoho testu totiž zpravidla dosáhneme značně zkreslených výsledků. Jako další hodnotící kritérium by se dalo využít nasazení druhé, osvědčené metody. Na základě výsledků obou testů by se následně mohly navrhnout možné modifikace nově navržené metodiky. Dalším zásadním faktorem, ovlivňujícím výsledky kontroly je rozsáhlost daného prostředí a množství provozu v něm. Díky nasazení dané metodiky pouze v laboratorním prostředí mohou být dosažené výsledky značně zkresleny. V důsledku této skutečnosti tak mohou být navržené modifikace neefektivní, ne-li dokonce i kontraproduktivní.

V části zaměřující se na netechnologická rizika, metodika odhalila drobné nedostatky, které v současnou chvíli nelze vyřešit. Dalším bodem kontroly byla fyzická bezpečnost. Zde byla věnována pozornost pouze procesu kontroly přístupu oprávněných osob, i přesto v této části byly rovněž odhaleny drobné nedostatky, ty však v daném prostředí nepředstavovaly vážnější hrozbu. Během testování následující části zaměřené na rizika v oblasti podnikové sítě, nemohlo testování vzhledem k použité síťové architektuře proběhnout v plném rozsahu. Přesto však byly odhaleny nedostatky v nasazeném zabezpečení. Navzdory výše uvedeným nálezům by se daná metodika měla ještě více zaměřit na bezpečnost síťových protokolů, které jsou v dané síti využívány. Čtvrtá část testu dle výše uvedené metodiky byla zaměřena na testování bezpečnosti v rámci OS a jím použitých aplikací. Zde nebyla odhalena žádná bezpečnostní rizika. Tento výsledek však může být způsoben mými značně omezenými zkušenostmi v daném oboru. Poslední část metodiky se zaměřila na monitoring celého prostředí nasazeného privátního cloudu. Dosažené výsledky lze bohužel jen stěží hodnotit, neboť byly ovlivněny řadou faktorů, mezi něž například patřila malá členitost nasazeného prostředí a nízký počet uživatelů a služeb. Přínosnou modifikací pro danou metodiku by mohla být implementace detailnějšího popisu potřebných monitorovacích funkcí. To by však mohlo vést k dosažení horších výsledků v rámci požité metodiky, neboť potřebné monitorovací funkce se volí vzhledem k potřebám jednotlivých společností.

Samotný postup pro testování zabezpečení se ukázal jako systematický a při využití vhodných nástrojů v patřičně rozsáhlém a dynamickém prostředí se jeví jako dostatečný. Avšak jednoznačnou slabinou této metodiky je nevyužití kontrolních mechanizmů, které jsou doporučeny normou ISO 27002. Pokud by se daná metodika touto normou více řídila, vzroste jak její účinnost, tak i prokazatelnost získaných výsledků. Další modifikací vytvořené metodiky by mohla být implementace penetračních testů, které by mohly napomoct k odhalení zranitelnosti systému. K tomu by však bylo potřeba zkušenějšího testera, neboť mé znalosti jsou v tomto odvětví značně omezeny.

7 Závěr

Cílem práce bylo v úvodní části představit technologii cloud computingu spolu s důležitými termíny, které jsou s danou technologií spojeny. Dále bylo zapotřebí seznámit čtenáře s problematikou týkající se zabezpečení v dané oblasti. Na základě výše uvedené problematiky bylo potřeba vytvořit metodiku pro odhalování bezpečnostních rizik, která se měla v laboratorních podmínkách pokusit odhalit bezpečnostní rizika v nově nasazovaném cloudovém prostředí. V konečné části práce měla být tato metodika na základě získaných výsledků zhodnocena a měly být navrženy její možné optimalizace.

V úvodu teoretické části byl čtenář seznámen s definici pojmu cloud computing, byly představeny stěžejní pojmy související s danou technologií a základní modely cloud computingu. Následující kapitola si kladla za úkol představit a vysvětlit stěžejní pojmy, které jsou nutné pro porozumění dalších částí této práce. V následujících kapitolách se práce věnovala hrozbám souvisejícím s danou technologii. Následně byly představeny metody, které umožňují těmto hrozbám předejít, nebo je odstranit. Dále byly představeny normy zabývající se problematikou bezpečnosti v prostředí cloud computingu. Zejména se jednalo o skupinu norem ISO 27000. V 5. kapitole byly představeny technologie a přístupy tří vybraných společností poskytujících cloudové služby.

V praktické části práce byla navrhnuta metodika pro odhalování bezpečnostních rizik souvisejících s cloud computingem. Dále byly popsány použité technologie při procesu nasazení privátního cloudu. Jednalo se hlavně o technologie společnosti Microsoft. Další část práce se věnovala procesu nasazení výše uvedených technologií spolu s procesem odhalování bezpečnostních rizik dle navržené metodiky. V závěrečné části byly vyhodnoceny výsledky získané pomocí výše uvedeného postupu, a byla navržena kritéria, která by mohla přispět k optimalizaci dané metodiky. Z dosažených výsledků je patrné, že pro plné ověření metodiky je třeba využít cloudové prostředí reálné firmy. Naopak pro důkladné a věrohodné ověření bezpečnosti v prostředí cloud computingu je potřeba nasadit ověřenou metodiku v kombinaci se vhodnými nástroji a zkušeným testovacím personálem.

Je zřejmé, že technologie cloud computingu je v dnešní době velice populární, ale také, že otázka bezpečnosti je stále pro mnoho společnosti naprosto zásadní. Avšak ačkoli v sobě technologie cloud computingu skrývá nespočet bezpečnostních výzev, při použití kvalitních metodik a nasazen správných technologií může přechod ke cloud computingu v konečném důsledku přinést řadu benefitů, a to nejen na poli bezpečnosti dat.

Na závěr bych chtěl dodat, že v době dokončování této diplomové práce se rozšířily pochybnosti o zabezpečení cloudových služeb. Původ těchto pochybností pramenil z odhalení dokumentů o tajném projektu nazvaném PRISM, jehož tvůrcem je NSA[40] (National Security Agency). Za toto zveřejnění mohl Edward Snowden, jenž byl jedním z pracovníků výše zmiňované organizace. Úkolem tohoto programu byla analýza dat jak

[40] Národní bezpečnostní agentura Spojených států amerických

od mobilních operátorů, tak i od nadnárodních společností, působících zejména v oblast internetu, které mimo jiné poskytují cloudové služby. Dle dokumentů, které Edward Snowden zveřejnil, mělo NSA volný přístup k serverům firem Yahoo, Google, Facebook, Microsoft, Apple, PalTalk a AOL. Dle výčtu zainteresovaných společností je patrné, že byly analyzovány nejen textové dokumenty (emaily, jejích přílohy atd.), ale i multimediální obsah jako zvuk, obraz a video. Na stránkách zdroje [67] lze najít grafické znázornění, které z historického hlediska zobrazuje, od kdy měla NSA přístup k datům z daných serverů. Všechny výše uvedené firmy se od tohoto obvinění okamžitě distancovaly a tato tvrzení dementovaly. V současné situaci se nabízí hned dva různé scénáře, které z dané situace mohou plynout. První scénář připouští možnost, že všechny výše uvedené společnosti poskytovaly svá data NSA, a to bez vědomí svých uživatelů. Takovéto chování daných firem by mohlo vést ke značnému snížení důvěryhodnosti daných společností a následně k možnému snížení využívání jejích služeb. Druhý scénář připouští možnost, že NSA si vytvořila vlastní přístup k daným serverům, a to bez vědomí těchto společností. Tato možnost by však znamenala, že dané společnosti nejsou schopny uchránit data, a to jak svá, tak i svých zákazníků. Následky tohoto scénáře by pak mohly mít obdobný efekt, jako tomu bylo v předchozím případě. Dle dostupných průzkumů provedené společností CSA [68] dokonce k výše uvedeným úpadkům po poptávce o cloudové služby již začalo docházet.

Literatura

1. **Velte, Anthony T, Velte, Toby J a Elsenpeter, Robert.** *Cloud computing - Praktický průvodce.* Brno : Computer Press a. s., 2011. 978-80-251-3333-0.

2. **Halpert, Ben.** *Auditing Cloud Computing.* hoboken : John Wiley & Sons, 2011. 978-0-470-87474-5.

3. **MELL, Peter a GRANCE, Timothy.** The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. *The NIST Definition of Cloud Computing.* [Online] Geithersburg : U.S. Department of Commerce, September 2011. [Citace: 15. 2. 2013.] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

4. **Conroy, Sean.** History of Virtualization. *History of Virtualization.* [Online] 1. 8. 2011. [Citace: 14. 2. 2013.] http://www.everythingvm.com/content/history-virtualization.

5. **PRODĚLAL, Jaroslav.** Virtualizace, Clustery a Cloud computing. *Virtualizace, Clustery a Cloud computing.* [Online] 28. 4. 2009. [Citace: 14. 2. 2013.] http://www.slideshare.net/jprodelal/pednka-virtualizace-clustery-a-cloud-computing-1358537#btnNext.

6. **Jones, M. Tim.** Virtual Linux. *developerWorks.* [Online] 29. Dec 2006. [Citace: 12. 3 2013.] http://www.ibm.com/developerworks/linux/library/l-linuxvirt/.

7. **Darryl Chantry.** Mapping Applications to the Cloud. *MSDN.* [Online] Microsoft Corporation, January 2009. [Citace: 18. 3 2013.] http://msdn.microsoft.com/en-us/library/dd430340.aspx.

8. **Kavička, Antonín.** Studijní materiály. *IS/STAG.* [Online] 2010. https://portal.upce.cz/portal/moje-studium/materialy.html.

9. Xen - paravirtualizace operačních systémů. *Xen - paravirtualizace operačních systémů.* [Online] 2008. [Citace: 14. 2. 2013.] http://www.virtualni-managed-servery.cz/xen.html.

10. Virtual systems overview. *IBM Systems Software Information Center.* [Online] 2004. [Citace: 14. 2. 2013.] http://publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp?topic=/eicay/eicayvservers.htm.

11. **FOSTER, Ian.** What is the Grid? A Three Point Checklist. *What is the Grid? A Three Point Checklist.* [Online] Argonne National Laboratory & University of Chicago, 20. July 2012. [Citace: 25. 2. 2013.] http://dlib.cs.odu.edu/WhatIsTheGrid.pdf.

12. World Community Grid - technology solving problems. *World Community Grid.* [Online] IBM, 2013. [Citace: 25. 2. 2013.] http://www.worldcommunitygrid.org/.

13. SETI@home. *SETI@home.* [Online] University of California, © 2013. [Citace: 25. 2. 2013.] http://setiathome.berkeley.edu/.

14. Utility (Cloud) Computing…Flashback to 1961 Prof. John McCarthy. *Life in the Cloud, Living with Cloud Computing.* [Online] 25. 9. 2008. [Citace: 14. 2. 2013.] http://computinginthecloud.wordpress.com/2008/09/25/utility-cloud-computingflashback-to-1961-prof-john-mccarthy/.

15. **MOHAMED, Arif.** A history of cloud computing. *A history of cloud computing.* [Online] 2009. [Citace: 14. 2. 2013.] http://www.computerweekly.com/feature/A-history-of-cloud-computing.

16. **CHELLAPPA, Ramnath.** Emory University. *Emory University: Goizueta Business School.* [Online] 2012. [Citace: 14. 2. 2013.] http://www.bus.emory.edu/ram/.

17. **Winkler, Vic (J.R.).** *Cloud Computing Security Techniques and Tactics.* Walthamm : Syngress, 2011. 978-1-59749-592-9.

18. **AHRONOVITZ, Miha a AMRHEIN, Dustin.** Cloud Computing Use Cases. *Cloud Computing Use Case Discussion Group.* [Online] 2. July 2010. [Citace: 20. 2. 2013.] Dostupné z: cloudusecases.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.odt.

19. **SCHULLER, Sinclair.** Demystifying The Cloud: Where Do SaaS, PaaS and Other Acronyms Fit In? *SaaSBlogs.* [Online] 1. December 2008. [Citace: 20. 2. 2013.] http://www.saasblogs.com/saas/demystifying-the-cloud-where-do-saas-paas-and-other-acronyms-fit-in/.

20. **DANIELITO, C.** Cloud Computing : Tips for Financial Industry. *Danielito C. Vizcayno Blogs.* [Online] 2012. [Citace: 20. 2. 2013.] http://dcvizcayno.wordpress.com/2012/04/13/cloud-computing-tips-for-financial-industry/.

21. Security of Cloud Computing Providers Study. *CA Technology.* [Online] April 2011. [Citace: 6. 3. 2013.] http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf.

22. Commission proposes a comprehensive reform of the data protection rules. [Online] European Commission JUSTICE, 25. 1 2012. [Citace: 12. 6 2013.] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

23. TOP THREATS TO CLOUD COMPUTING. *CSA Cloud Security Alliance.* [Online] February 2013. [Citace: 2. 5 2013.] https://cloudsecurityalliance.org/research/top-threats/.

24. **HONAN, MAT.** How Apple and Amazon Security Flaws Led to My Epic Hacking. *WIRED.* [Online] 8. 6 2012. [Citace: 13. 5 2013.] http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/.

25. **Schofield, Jack.** How to avoid being hacked like Honan. *The Guardian.* [Online] Guardian News and Media Limited, 9. August 2012. [Citace: 2. 5 2013.] http://www.theguardian.com/technology/askjack/2012/aug/09/hacking-internet-email-cloud-computing?INTCMP=SRCH.

26. **Goodin, Dan.** Amazon purges account hijacking threat from site. *The Register.* [Online] 20. April 2010. [Citace: 13. 5 2013.] http://www.theregister.co.uk/2010/04/20/amazon_website_treat/.

27. The CERT Insider Threat Center. *cert software engineering institute* . [Online] 5. June 2012. [Citace: 14. 5 2013.] http://www.cert.org/insider_threat/.

28. **Walter.** Insider Threats To Cloud Computing. *Cloud Tweaks.* [Online] 1. October 2012. [Citace: 1. 5 2013.] http://www.cloudtweaks.com/2012/10/insider-threats-to-cloud-computing/.

29. DDoS attack - Distributed Denial of Service. *Webopedia.* [Online] 2013 . [Citace: 14. 4 2013.] http://www.webopedia.com/TERM/D/DDoS_attack.html.

30. Application Denial of Service. *OWASP.* [Online] OWASP Foundation, 22. April 2010. [Citace: 19. 4 2013.] https://www.owasp.org/index.php/Application_Denial_of_Service.

31. **Polesný, David.** České zpravodajské weby čelily masivnímu útoku. *Živě.* [Online] Mladá fronta a. s., 4. 3 2013. [Citace: 4. 3 2013.] http://www.zive.cz/clanky/ceske-zpravodajske-weby-celily-masivnimu-utoku/sc-3-a-167837/default.aspx.

32. **Chickowski, Ericka.** Web Services Single Sign-On Contain Big Flaws. *Dark Reading.* [Online] 19. March 2012. [Citace: 19. 4 2013.] http://www.darkreading.com/authentication/web-services-single-sign-on-contain-big/232602844.

33. **Lemos, Robert.** Insecure API Implementations Threaten Cloud. *Dark Reading.* [Online] 23. April 2012. [Citace: 18. 4 2013.] http://www.darkreading.com/cloud/insecure-api-implementations-threaten-cl/232900809.

34. **Schwartz, Mathew J.** New Virtualization Vulnerability Allows Escape To Hypervisor Attacks. *Information Week Security.* [Online] 13. June 2012. [Citace: 14. 5 2013.] http://www.informationweek.com/security/application-security/new-virtualization-vulnerability-allows/240001996.

35. **Deutch, John M.** *US aid.* [Online] 1. July 1997. [Citace: 3. 6 2013.] http://transition.usaid.gov/policy/ads/500/d522022m.pdf.

36. **Kean, Ryan.** Security of Cloud Computing. *Cloud Standards Customer Council.* [Online] August 2012. [Citace: 12. 5 2013.] http://www.cloudstandardscustomercouncil.org/Security_for_Cloud_Computing-Final_080912.pdf.

37. **Lejsek, Zdeněk.** Nové přístupy k bezpečnosti cloudu. *SystemOnLine.* [Online] Symantec, © 2001 - 2013. [Citace: 5. 5 2013.] http://www.systemonline.cz/virtualizace/nove-pristupy-k-bezpecnosti-cloudu.htm.

38. itil-officialsite. *ITIL.* [Online] APM Group Ltd, 3. 7 2013. [Citace: 1. 7 2013.] http://www.itil-officialsite.com/.

39. INTERNATIONAL STANDARD ISO 19011. *cnis.* [Online] 15. 11 2011. [Citace: 2. 7 2013.] http://www.cnis.gov.cn/wzgg/201202/P020120229378899282521.pdf.

40. Ernst-young. *Big4.* [Online] 2013. [Citace: 2. 7 2013.] http://www.big4.com/ernst-young/.

41. Google Apps for Business Audit & Certification Summary. *cloud-computing.* [Online] 2012. [Citace: 2. 7 2013.] http://www.cloud-computing.org.il/wp-content/uploads/2012/05/Google_Apps_3rd_Party_Certs_May_2012.pdf.

42. **Netolická, Barbora.** Jak na bezpečnostní audit. *SystemOnLine.* [Online] 3 2013. [Citace: 16. 6 2013.] http://www.systemonline.cz/it-security/jak-na-bezpecnostni-audit.htm.

43. Abaout ISO 27k standards. *ISO 27000 Security.* [Online] IsecT Ltd., 2013. [Citace: 2. 7 2013.] http://www.iso27001security.com/html/others.html#Top.

44. O-nás. *IBAcz.* [Online] IBA CZ s.r.o., 2013. [Citace: 3. 7 2013.] https://www.ibacz.eu/o-nas.

45. **Zitta, Stanislav.** Vysokoškolské kvalifikační práce. *Digitální knihovna Univerzity Pardubice.* [Online] 17. 5 2013. [Citace: 25. 6 2013.] http://dspace.upce.cz/handle/10195/51826.

46. Licence Agreement for standards made available through the ITTF web site. *ISO.* [Online] 2012. [Citace: 24. 6 2013.] http://standards.iso.org/ittf/licence.html.

47. ISO - popis a druhy. *ISO Fin.* [Online] ISOFIN CZ s.r.o., 2012. [Citace: 23. 6 2013.] http://www.isofin.cz/iso.htm.

48. An Introduction to ISO 27001, ISO 27002....ISO 27008. *ISO 27000.* [Online] Farr Cry Mollio, 2012. [Citace: 8. 6 2013.] http://www.27000.org/.

49. ISO/IEC Standard 15408. *ENISA - European Network and information Security Agency.* [Online] ENISA, 2013. [Citace: 19. 6 2013.]

http://www.enisa.europa.eu/activities/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15408.

50. ISO/IEC 13335-2. *ENISA - Europe Network of Information Security Agent.* [Online] ENISA, 2013. [Citace: 13. 6 2013.] http://rm-inv.enisa.europa.eu/methods/m_iso133352.html.

51. IBM cloud computing. *Wikipedia.* [Online] 8. June 2013. [Citace: 23. 6 2013.] http://en.wikipedia.org/wiki/IBM_cloud_computing#cite_note-eWeek-10.

52. IBM acquires SoftLayer. *IBM.* [Online] 2013. [Citace: 13. 6 2013.] http://www.ibm.com/cloud-computing/us/en/softlayer.html.

53. Security and high availability in cloud computing environments. *IBM.* [Online] June 2011. [Citace: 23. 6 2013.] http://www-935.ibm.com/services/za/gts/cloud/Security_and_high_availability_in_cloud_computing_environments.pdf.

54. Security. *IBM.* [Online] IBM, 2013. [Citace: 2. 7 2013.] http://www-03.ibm.com/software/products/us/en/category/SWI00#products.

55. **Coleman, Nick.** How does IBM deliver cloud security? *IBM.* [Online] May 2012. [Citace: 28. 6 2013.] http://www-935.ibm.com/services/be/en/attachments/pdf/2012_05_23_3728_Cloud_Security_How_does_IBM_D.pdf.

56. SC Magazine Award. *SC Magazine.* [Online] SC Magazine, 2012. [Citace: 2. 7 2013.] http://awards.scmagazine.com/winners/2012/105.

57. **LOHR, STEVE.** Challenging Microsoft With a New Technology. *The New Yourk Times.* [Online] NEW YORK TIMES, 30. August 2009. [Citace: 4. 7 2013.] http://www.nytimes.com/2009/08/31/technology/business-computing/31virtual.html?pagewanted=2&_r=2&partner=rss&emc=rss.

58. **Sedlák, Jan.** Michal Stachník: Cloud od Microsoftu je jen marketing. *Connect.* [Online] Mladá Fronta, 9. 12 2012. [Citace: 13. 12 2012.] http://connect.zive.cz/clanky/michal-stachnik-cloud-od-microsoftu-je-jen-marketing/sc-320-a-166703.

59. Accelerate IT. Inovate with Your Cloud. *VMware.* [Online] VMware Inc, 2012. [Citace: 4. 7 2013.] http://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf.

60. Architecting a vCloud. *VMware vCloud.* [Online] 2010. [Citace: 12. 7 2013.] http://www.vmware.com/files/pdf/VMware-Architecting-vCloud-WP.pdf.

61. **Kačmář, Dalibor.** Program konference 2012. *Bezpečnost v Cloudu.* [Online] 2012. [Citace: 2. 4 2013.] http://www.bezpecnostvcloudu.cz/bezpecnost-v-cloudu-2012/program.htm.

62. Windows Azure: Government cloud computing. *Microsoft.* [Online] 2013. [Citace: 12. 7 2013.] http://www.microsoft.com/government/en-us/products/Pages/azure.aspx.

63. Microsoft Private Cloud. *Server and Cloud Platform.* [Online] November 2012. [Citace: 2. 6 2013.] http://www.microsoft.com/en-us/server-cloud/private-cloud/default.aspx.

64. Microsoft Private Cloud Economics Tools. *cloudeconomics.* [Online] [Citace: 6. 7 2013.] http://cloudeconomics.cloudapp.net/#.

65. **Boden, Pete a Estberg, Mark .** Delivering and Implementing a Secure Cloud Infrastructure. *dlbmodigital.microsoft.* [Online] 2009. [Citace: 2. 3 2013.] http://dlbmodigital.microsoft.com/ppt/TN-100323-PBoden_MEstberg-1032444383-FINAL.pdf.

66. Addressing Cloud Computing Security Considerations with a Partner Private Cloud and Addressing Cloud Computing Security Considerations with Office 365. *Microsoft Download Center.* [Online] 2011. [Citace: 4. 3 2013.] CloudSecurityConsiderations_MicrosoftOffice365.

67. **Greenwald, Glenn a MacAskill, Ewen.** NSA Prism program taps in to user data of Apple, Google and others. *The Guardian.* [Online] 7. June 2013. [Citace: 2. 7 2013.] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

68. NSA/PRISM Survey. *Cloud Security Alliance.* [Online] July 2013. [Citace: 7. 7 2013.] https://cloudsecurityalliance.org/research/surveys/#_nsa_prism.

69. IBM Security Virtual Server Protection for VMware. *IBM.* [Online] IBM, 2013. [Citace: 2. 7 2013.] http://www-03.ibm.com/software/products/us/en/virtual-server-protection/.

Seznam příloh

Příloha 1 – CD se skripty použitými při konfiguraci OS Microsoft Server 2012 a dokumenty obsahující parametry a detailní konfiguraci použitých síťových prvků.