UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Analýza využití cloud computingu ve firemním prostředí

Bc. Tomáš Svoboda

Diplomová práce
2015

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2014/2015**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Tomáš Svoboda**
Osobní číslo:	**I13448**
Studijní program:	**N2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Analýza využití cloud computingu ve firemním prostředí**
Zadávající katedra:	**Katedra softwarových technologií**

Zásady pro vypracování:

Cílem práce je realizovat výzkum na využívání cloud computingu firmami a státními organizacemi v ČR a provést analýzu jeho využívání a dopadů na efektivitu organizace. Autor práce představí základní dělení a principy cloud computingu. Provede dotazníkové šetření na jeho využívání v prostředí firem a státních organizací v ČR. Na základě vyhodnocení dotazníkového šetření provede analýzu nasazování cloud technologií v prostředí ČR a důvody pro jeho zavádění a nezavádění. Na závěr práce autor připraví případovou studii pro ukázkové řešení nasazení cloud technologií.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

ERL, Thomas, Richardo PUTTINI a Zaigham MAHMOOD. Cloud computing: concepts, technology,. xxxiv, 487 pages. ISBN 978-013-3387-520.
MILLARD, Christopher J, Richardo PUTTINI a Zaigham MAHMOOD. Cloud computing law: concepts, technology,. xix, 416 pages. ISBN 01-996-7168-0.
KRUTZ, Ronald L a Russell Dean VINES. Cloud security: a comprehensive guide to secure cloud computing. Indianapolis, IN: Wiley Pub., c2010, xxvi, 358 p. ISBN 04-705-8987-6.

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

Datum zadání diplomové práce: **31. října 2014**
Termín odevzdání diplomové práce: **15. května 2015**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

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

V Pardubicích dne 15. listopadu 2014

Prohlášení autora

Prohlašuji, že jsem tuto práci 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 3. 5. 2015 Bc. Tomáš Svoboda

Poděkování

Na tomto místě bych rád poděkoval Mgr. Josefu Horálkovi, Ph.D. za cenné rady a za pomoc, kterou mi poskytl při zpracování této diplomové práce. Dále bych rád poděkoval své rodině a všem, kteří mě během studia podporovali.

Anotace

Cílem práce je realizovat výzkum na využívání cloud computingu firmami a státními organizacemi v ČR a provést analýzu jeho využívání a dopadů na efektivitu organizace. Autor práce představí základní dělení a principy cloud computingu. Provede dotazníkové šetření na jeho využívání v prostředí firem a státních organizací v ČR. Na základě vyhodnocení dotazníkového šetření provede analýzu nasazování cloud technologií v prostředí ČR a důvody pro jeho zavádění a nezavádění. Na závěr práce autor připraví případovou studii pro ukázkové řešení nasazení cloud technologií.

Klíčová slova

Cloud computing, podnik, organizace, výzkum

Title

Cloud computing analysis in a corporate domain

Annotation

The aim of this diploma thesis is to realize research about using cloud computing in companies and organizations in the Czech Republic and analyze its use and impact on organizational effectiveness. Author explain basic principles of cloud computing. Author realize questionnaire survey in a corporate domain and government organizations in the Czech Republic. On the basis of a questionnaire survey he analyzes the deployment of cloud technologies and reasons for using or not using this technology. Author also prepare a case study for deploying cloud technology.

Keywords

Cloud computing, company, organization, research

Obsah

Seznam zkratek

AaaS	Application as a Service
API	Application programming interface
CERT	Computer Emergency Response Team
DoS	Denial of Service
DDoS	Distributed Denial of Service
EU	European Union
FBI	Federal Bureau of Investigation
HaaS	Hardware as a Service
HTTP	Hypertext Transfer Protocol
HW	Hardware
IaaS	Infrastructure as a Service
IM	Instant messaging
IT	Information technology
IP	Internet Protocol
NASA	National Aeronautics and Space Administration
NC	Numerical control
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PC	Personal computer
SaaS	Software as a Service
SLA	Service Level Agreement
SSL	Secure Sockets Layer
SW	Software
TLS	Transport Layer Security
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
XSS	Cross-side script

Seznam obrázků

Seznam tabulek

Úvod

Cloud computing představuje v oblasti informačních technologií relativně nově používaný pojem. Ten se v posledních letech dostává do povědomí stále větší skupiny lidí, kteří využívají informační technologie. Většina lidí si myslí, že se jedná o naprostou novinku, ale ve skutečnosti historie cloud computingu sahá až do 60. let 20. století. Vzhledem k tehdejším technickým možnostem nebylo možné myšlenku cloud computingu realizovat. Poté se tento pojem objevil až v roce 1997 v přednášce Ramnatha Chellapa. Historie této technologie je podrobněji popsána v kapitole 2.

Především pro firemní prostředí je cloud computing technologií budoucnosti. Motivace v podobě úspory finančních nákladů na infrastrukturu, snížení počtu pracovníků IT oddělení a placení pouze za služby, které jsou skutečně využívány, jsou hlavními kritérii pro jeho zavádění.

Diplomová práce se věnuje výzkumu využívání cloudu a cloudových služeb v podnicích a organizacích v České republice. Na základě získaných informací je zhodnocen stávající stav a provedena případová studie.

Diplomová práce je rozdělena na dvě části. Těmi jsou teoretická a praktická část. Teoretická část je rozdělena na dvě kapitoly. V první jsou vysvětleny pojmy z oblasti podniku a organizace. Druhá kapitola se věnuje podrobně technologii cloud computingu, modelům jeho nasazení, využívaným komponentám a vlastnostem této technologie. Samostatná podkapitola je věnována virtualizaci, která s cloud computingem úzce souvisí. Dále jsou popsána bezpečnostní rizika, která s sebou tato technologie přináší. Součástí je také SWOT analýza, a to z pohledu typu cloudu a typu cloudových služeb.

Praktická část je rozdělena do tří kapitol. První kapitola obsahuje popis použité výzkumné metodiky a formu dotazníku, který byl použit k získání odpovědí. Součástí druhé kapitoly je vyhodnocení získaných dat. Výsledky byly vyhodnoceny samostatně podle toho, o jaký typ organizace se jedná. V rámci výzkumu byly osloveny soukromé firmy, státní organizace a pobočky nadnárodní společnosti. Případová studie je obsahem třetí kapitoly. Na základě teoretické části a výsledků praktické části práce je popsáno využití cloud computingu v oblasti činnosti vybrané společnosti.

1 Podnik a podniková informatika

V této kapitole jsou vysvětleny základní pojmy týkající se podniku, organizace a využívání podnikové informatiky.

1.1 Podnik a organizace

Definice podniku není zcela jednoznačná. Je třeba rozlišit definici podle českého práva a evropského práva. Podle §5 Obchodního zákoníku je podnik „soubor hmotných, jakož i osobních a nehmotných složek podnikání. K podniku náleží věci, práva a jiné majetkové hodnoty, které patří podnikateli a slouží k provozování podniku nebo vzhledem k své povaze mají tomuto účelu sloužit.“ (Obchodní zákoník, 1991)

Podle evropského práva je podnik „každý subjekt vykonávající hospodářskou činnost, bez ohledu na jeho právní formu. K těmto subjektům patří zejména osoby samostatně výdělečně činné a rodinné podniky vykonávající řemeslné či jiné činnosti a obchodní společnosti nebo sdružení, která běžně vykonávají hospodářskou činnost.“ (Nařízení komise, 2008)

Klíčovým rozdílem je tedy samotné chápání podniku, kdy podle českého práva je podnik věcí, nikoli subjektem.

Organizaci lze chápat jako organizovanou skupinu lidí, která se vyznačuje zavedenou vnitřní strukturou. Skupina má společnou motivaci k dosažení společného cíle, především s využitím všech dostupných zdrojů. (Tureckiová, Pour, Šedivá, 2009, s. 20)

1.2 Informatika

Podle Gály, Poura a Šedivé (2009, s. 21) je informatika vědní disciplína, zabývající se informacemi. Předmětem jejího studia je vyjádření, podoba, zpracování a přenos informací v rámci systémů. Přenos může být uskutečňován v přirozené (lidé) či umělé (počítače) formě.

1.3 Informační a komunikační technologie

Gála, Pour a Šedivá (2009, s. 30) zahrnují pod pojem informační technologie takové technologie, které jsou orientovány na zpracování informací. Mezi ně patří programové vybavení (software) a technické vybavení (hardware). Komunikační technologie se soustředí na zajištění vzájemné komunikace aplikací v informačním systému.

1.4 Informační systém

Šmíd (2002) definuje informační systém jako systém vzájemně propojených informací a procesů, které tyto informace využívají. Dále za informační systém pokládá softwarové vybavení firmy, které poskytuje vedoucím pracovníkům informace k plánování, koordinaci a kontrole firemních procesů. Obdobně Hronek (2007, s. 19) chápe informační systém jako systém pro sběr, uchování, zpracování a účelného poskytování informací. Není ale

podmínkou využívat automatizaci za pomoci počítačů. S Hronkem (2007, s. 19) se shoduje i Klimeš (2006, s. 7-8).

1.5 Podniková informatika

Podniková informatika využívá principů řízení, provozu a rozvoji ekonomického subjektu (podniku) s pomocí aplikace informatiky. Zahrnuje nejen aplikace a technologie pro vnitřní řízení podniku ale především aplikace realizující externí vztahy podniku, především ke svým obchodním partnerům. (Gála, Pour, Toman, 2006)

Gála, Pour a Šedivá (2009) chápou podnikovou informatiku jako aplikaci studující přenášení, zpracování, podobu a vyjádření informací. Aplikace se omezuje pouze na podnikové prostředí. Principy podnikové informatiky lze podle nich aplikovat i v rámci státu, respektive jeho orgánů a organizací.

Stejně tak Novotný et al. (2009) se ve výkladu tohoto pojmu omezují pouze na podnikové prostředí a organizace. Pod podnikovou informatiku zahrnují informatiku v těchto prostředích.

1.5.1 Vývoj podnikové informatiky

Podniková informatika procházela a stále prochází vývojem a její postavení v rámci podniku či organizace se neustále mění. Změny jsou dány především vývojem a možností využívání stále nových technologií. Z hlediska podniků je vývoj závislý také na aktuální ekonomické situaci. Historie využívání informatiky pro potřeby podniku se datuje do 50. let 20. století.

Dle Pepparda a Warda (2004, s. 167) je klíčové sledování podnikové informatiky v závislosti na využívání informačních systémů. Na ně kladou velký důraz a vidí v nich velký potenciál. Vývoj informačních systémů dále člení do tří etap. Stejného názoru je i Danel (2011):

- Etapa zpracování dat,
- etapa manažerských informačních systémů,
- etapa strategických informačních systémů.

Každá etapa je charakterizována různým využitím informačních technologií v rámci podniku a má tedy i odlišné cíle. Stručnější pohled nabízejí také Novotný et al. (2009, s. 18).

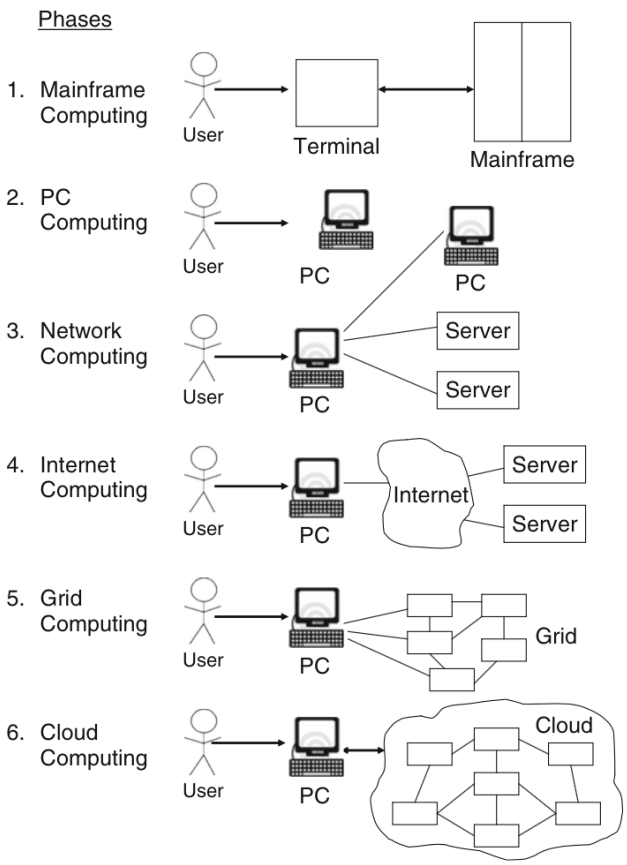
Etapa zpracování dat je dle Pepparda a Warda (2004, s. 167) počátkem podnikové informatiky. Charakteristikou bylo zaměření na automatizaci často se opakujících úkolů, což vedlo ke zvýšení efektivity podniku. Novotný et al. (2009, s. 17) vidí hlavní přínos v použití NC strojů, které toto umožnily. Jejich počátky sahají až do 50. let 20. století, kdy se se také poprvé uvažovalo o myšlence nasazení počítačů do řízení podniku.

Etapa manažerských informačních systémů je zaměřena nejen na automatizaci procesů, ale především podporuje rozhodování na základě přesnějších informací. Produkce podniku je schopna pružně reagovat podle zájmů zákazníka.

Etapa strategických informačních systémů je dle Pepparda a Warda (2004, s. 167) založena na aktivním vyhledávání příležitostí, které zajistí konkurenční výhodu podniku. K tomu využívá informační systémy a s pomocí získaných dat dochází k plánování podnikové strategie. Propojení informatiky a organizace se stává velice těsné. Zvýšení konkurenceschopnosti pokládá i Novotný et al. (2009, s. 18) za hlavní potenciál strategických informačních systémů.

Peppard a Ward (2004, s. 176) dále vidí potřebu v postupném vytěsňování informačních systémů mimo organizaci za použití komunikačních technologií. Cloud computing představuje technologii s jejíž pomocí lze toto uskutečnit a stává se tak logickým krokem ve vývoji podnikové informatiky. Stejný názor zastávají i Furth a Escalante (2010, s. 3-4). Ti rozlišují šest paradigmat řešení informatiky:

- Mainframe systémy,
- pc systémy,
- síťové systémy,
- internetové systémy,
- grid computing,
- cloud computing.



Obrázek 1 - Paradigmata řešení informatiky (zdroj: Furth, 2010, s. 4)

Mainframe systémy jsou typické pro sdílení výpočetního výkonu mezi více uživatelů, kteří pro přístup využívají terminály. Postupem času, se zvyšujícím se výkonem počítačů, se tyto staly natolik výkonné a cenově dostupné aby byly schopny pokrýt většinu potřeb uživatelů. Ve třetí fázi došlo k propojení koncových zařízení (pc, notebooky, servery) pomocí lokálních sítí za účelem sdílení zdrojů. Ve čtvrté fázi byly tyto lokální sítě propojovány s dalšími lokálními sítěmi a vznikla síť podobná dnešnímu Internetu. Cílem bylo především vzdálené využívání aplikací případně jiných zdrojů. S nárůstem výpočetního výkonu bylo možné provádět distribuované výpočty neboli grid computing. Podrobněji se grid computingu věnuje kapitola 2.8.5. V šesté fázi poskytuje cloud computing jednoduše škálovatelné sdílené prostředky prostřednictvím Internetu. (Furth a Escalante, 2010, s. 4)

Cloud computing lze považovat za vrchol současného vývoje. Při bližším porovnání je možné do jisté míry říci, že cloud computing představuje návrat k mainframe systémům. Není to ale zcela přesné. Existuje zde několik klíčových rozdílů. Z hlediska výpočetního výkonu nabízí mainframe systém pouze omezený výkon. Přístupové terminály slouží pouze pro zadávání vstupů a zobrazování výstupů. Naproti tomu v cloud computingu se jeví výpočetní výkon jako téměř neomezený. Přístup do cloudu je typicky přes pracovní stanici, která přidává svůj výpočetní výkon a tím pádem rychlejší a pohodlnější práci pro uživatele. (Furth a Escalante, 2010, s. 4)

2 Cloud computing

2.1 Historie, současnost a budoucnost cloud computingu

Cloud computing je technologie, která je v IT za posledních několik let velice skloňovaným pojmem. Ve skutečnosti byla základní myšlenka cloud computingu představena již v roce 1961, kdy profesor John McCarthy z MIT vyslovil myšlenku, že výpočetní technika by mohla být organizována jako distribuovaná veřejná služba. To znamená, že výpočetní výkon a aplikace by bylo možné prodávat stejně jako elektřinu. V podstatě, když se zapojí zařízení do zásuvky ve zdi, je zřejmé co se očekává, ale neřeší se jakým způsobem a odkud. To je záležitost poskytovatele služby, který se zavazuje na základě smlouvy, uzavřené se zákazníkem, k určitému plnění služeb. (Mácha, 2012)

Myšlenka to byla na tu dobu velice odvážná, ale vzhledem k tehdejšímu výkonu HW, SW a především telekomunikačních technologií, kdy nebyla dostupná vysokorychlostní komunikační síť, nebyla realizovatelná.

Název cloud computing vychází ze symbolu mraku (anglicky cloud), který je ve velké míře používán v diagramech pro znázornění internetu a zároveň všech služeb poskytovaných prostřednictvím internetu. Termín cloud byl ve skutečnosti původně využíván telekomunikačními společnostmi, které až do devadesátých let nabízely pouze služby typu point-to-point. Později začaly nabízet VPN sítě, které měly srovnatelnou kvalitu služeb, ovšem za nižší ceny. Symbol mraku byl použit pro označení hraničního bodu mezi tím, co náleželo poskytovateli a tím, co náleželo uživateli. Na konci devadesátých let dvacátého století, kdy se s rozvojem internetu zlepšila i dostupnost přenosových technologií spolu s prudkým nárůstem výkonu HW a SW, byla myšlenka cloud computingu opět oživena.

Prvním stěžejním rokem byl rok 1999, kdy firma Salesforce nabídla řešení podnikových aplikací prostřednictvím webových stránek (Mohamed, 2009). Průkopnickou společností byla firma Amazon, která po modernizaci svých datových center zjistila, že efektivně využívá zhruba 10 % jejich výkonu. V roce 2002 se proto rozhodla poskytnout nevyužitou kapacitu externím zákazníkům, prostřednictvím služby Amazon Web Service.

Na ní navázal v roce 2006 Amazon Elastic Compute Cloud (EC2), prostřednictvím kterého si kdokoliv může pronajmout virtuální počítač a provozovat své aplikace. Byl zaveden platební model „pay per use“, v některé literatuře označovaný též jako „pay-as-you-go“, kdy zákazník platí pouze za skutečně využívanou výpočetní kapacitu (službu), kterou si pronajme od provozovatele.

V průběhu let se přidávali další společnosti s vlastními řešeními poskytování cloud computingu. Mezi nejznámější patří firma Microsoft se svým řešením Microsoft Azure, VMWare s VCloud či Google s Google App Engine.

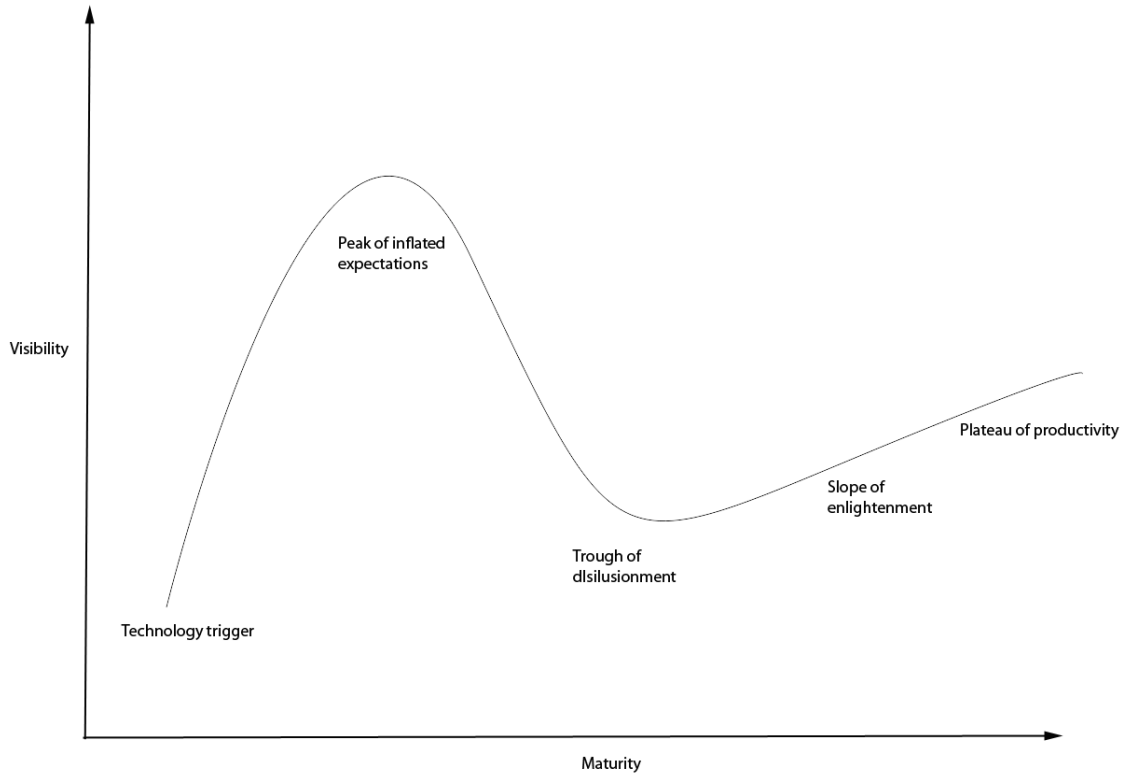
Cloudové služby nevyužívají pouze firmy, ale s rozšířením internetu také běžní uživatelé, kteří o tom mnohdy vůbec netuší. Prakticky každý uživatel má dnes zřízenou emailovou

schránku, případně využívá datová uložiště jako Dropbox či Google Drive. Všechny tyto služby jsou cloudové.

Současnou pozici cloud computingu v IT a jeho budoucností se zabývá také agentura Gartner Inc. Jedná se o vědecko-poradenskou společnost, zaměřující se na hledání optimálních řešení pro podnikání v oblasti IT (About Gartner, 2014). Vlastní nástroj Hype Cycle. Jedná se o křivku, pomocí které lze graficky znázornit současný stav dané technologie a dále zda je technologie schopna udržet se na trhu. (Gartner Hype Cycle, 2014)

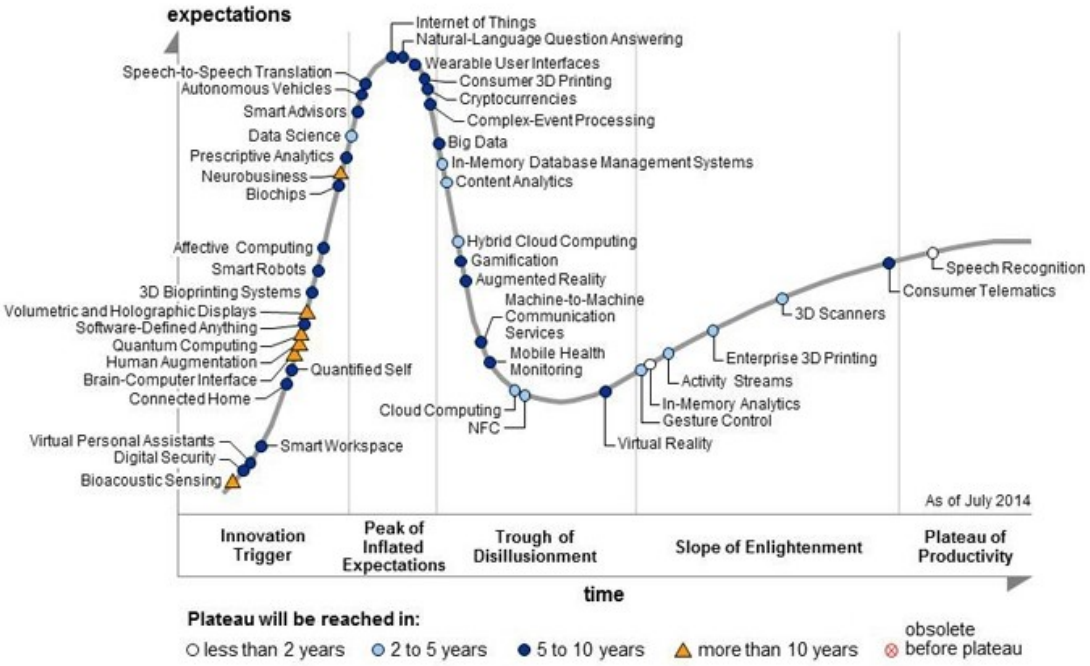
Jak je patrné z následujícího obrázku, křivka je rozdělena na pět částí:

- Technology trigger (počáteční zájem) – nastává průlom dané technologie, o kterou se se začínají zajímat média. Životaschopnost na trhu není prokázána.
- Peak of inflated expectations (vrchol očekávání) – publicita zajišťuje řadu úspěchů doprovázených ve velké míře i neúspěchy. Technologii zavádí pouze malá část podniků (společností).
- Through of disillusionment (deziluze) – velký počet neúspěchů snižuje zájem. Poskytovatelé musí zlepšit své produkty, aby se technologie udržela na trhu.
- Slope of enlightenment (obnova zájmu) – technologie se zdokonaluje a stává se známá široké veřejnosti. Tím dochází k jejímu zavedení do více společností s výjimkou konzervativních, které jsou opatrné.
- Plateau of productivity (přijetí technologie) – vyplácí se masivní přijetí technologie, která je schopna udržet se na trhu.



Obrázek 2 - Hype cycle (zdroj: upraveno dle Gartner, 2013)

V době psaní této práce byla k dispozici Hype Cycle za rok 2013. Cloud computing se umístil v oblasti, kdy je třeba zlepšovat produkty, aby se technologie udržela na trhu. Vzhledem k tomu, že poskytovatelé se snaží zlepšovat bezpečnost, nabízet nové produkty a vyhovovat požadavkům trhu, má cloud computing dobrý začátek pro zajištění své budoucnosti.



Obrázek 3 - Hype cycle 2013 (zdroj: Gartner's 2013)

2.2 Definice

Termín cloud computing dnes nalezneme téměř všude. Je populárním tématem odborných článků, konferencí a diskutovaným pojmem v internetových diskuzích. Definic existuje několik, ale vzájemně se od sebe odlišují. Pro tuto práci byla proto zvolena definice světově uznávané organizace NIST (Národního Institutu pro Normalizaci a Standardy), která byla zřízena v roce 1901 a jejím hlavním úkolem je podpora inovací a konkurenceschopnosti Spojených států amerických, prostřednictvím standardů a technologií. S touto definicí se setkáme v mnoha dokumentech a článcích (Marston et al., 2011, s. 2; Ghaffari, Delgosha a Abdolvand, 2014, s. 14) zabývajících se problematikou cloudu, proto byla zvolena jako relevantní definice.

Dle organizace NIST (Mell a Grance, 2011, s. 2) cloud „umožňuje okamžitý, snadný a na vyžádání dostupný síťový přístup ke sdílené nabídce konfigurovatelných výpočetních zdrojů (sítě, servery, datové uložiště, aplikace a služby), které mohou být v případě potřeby poskytnuty či uvolněny za minimálních administrativních nákladů a potřeby koordinace s poskytovatelem služeb. Tento cloudový model se skládá z pěti základních charakteristik, tří modelů poskytování služeb a čtyř modelů nasazení.“

Jiný pohled má na definici cloud computingu například společnost Gartner Inc. Ta definuje cloud computing jako „škálovatelné a elastické zdroje, které jsou poskytovány jako služba externím zákazníkům s využitím internetových technologií.“ (Pettey a Goasduf, 2009)

Podle Furtha a Escalanteho (2010, s. 3) je cloud computing „nový styl práce na počítači, ve kterém jsou dynamicky škálovatelné a často i virtualizované prostředky poskytovány jako služby přes internet.“

2.3 Charakteristické vlastnosti cloud computingu

Stejně jako existuje mnoho definic cloud computingu, a různé pohledy na tuto problematiku, liší se také definice jeho charakteristických vlastností. Mell a Grance (2011, s. 2) definují pět charakteristických vlastností cloud computingu.

- On-demand self-service (samoobslužné zadávání požadavků) – zákazník si sám může zvolit, kdy bude danou službu využívat a jaké zdroje bude využívat, bez interakce s poskytovatelem dané služby. Zákazníkovi tento přístup umožňuje flexibilně reagovat na jeho potřeby v krátkém čase.

- Broad network access (širokopásmový přístup k síti) – služby jsou dostupné prostřednictvím počítačové sítě, která využívá standardizovaných mechanismů, podporující tenké nebo tlusté klienty (mobilní telefony, tablety, pracovní stanice, notebooky).

- Resource pooling (sdružování zdrojů) – výpočetní zdroje poskytovatele jsou poskytovány jednotlivým zákazníkům kteří je sdílí, ale jsou mezi sebou navzájem izolováni. To samé platí pro jejich data. Zákazník ale nemá možnost zjistit, kde se fyzicky tyto zdroje nachází, což představuje jeden z hlavních problému týkající se bezpečnosti využívání cloudových služeb. Zákazníci by měli mít možnost získat informace ve kterém státě, případně datovém centru, se jejich data nachází. Bezpečnosti a ochraně dat se věnuje kapitola 2.9.

- Rapid elasticity (pružnost zdrojů) – tato vlastnost je důležitá z pohledu poskytovatele služeb, který může dynamicky měnit výpočetní zdroje přidělené jednotlivým zákazníkům, s minimální interakcí s nimi. Zároveň z pohledu zákazníka, kterému se zdroje jeví jako neomezené a lze mu je přidělit v jakémkoli množství a kdykoli.

- Measured service (měřitelnost služby) – cloudové systémy automaticky kontrolují kvalitu poskytovaných služeb a optimalizují využití zdrojů. Využití monitorování služeb poskytuje transparentní pohled pro poskytovatele i zákazníky, kteří platí pouze za skutečně využívané služby.

Podobně jako Mell a Grance (2011, s. 2) uvádí i Pettey a Goasduff (2009) pět základních charakteristických vlastností cloud computingu.

- Orientování na služby – implementační detaily služby jsou zákazníkovi skryty. Pro něj je důležitá především funkčnost služby. Ta je navržena pro specifické potřeby určité skupiny uživatelů.

- Škálovatelnost a elasticita – zdroje mohou být zákazníkovi přiděleny či odebrány podle jeho aktuální potřeby.

- Sdílení zdrojů – služby sdílí společné výpočetní zdroje poskytovatele za účelem jejich maximálního využití.
- Měřitelnost služby – poskytovatel využívá sledování služeb pomocí metrik. Na jejich základě je zákazníkovi účtováno jejich používání. Zároveň může na základě získaných dat vytvářet různé cenové tarify pro zákazníky.
- Použití internetových technologií – transportní službou pro dodávání služeb je internet, respektive jeho standardy a protokoly (HTTP, IP, URL).

2.4 Modely nasazení cloudu

Model nasazení definuje míru poskytování cloudových služeb koncovým uživatelům. V této oblasti dochází k určitým rozporům. Armbrust et al. (2009) definují dva modely: privátní a soukromý. Marston et al. (2011, s. 4) rozšiřuje skupinu modelů o hybridní cloud. Mell a Grance (2011, s. 5) přidávají existenci ještě jednoho modelu nasazení a to komunitní cloud. S tímto konceptem se shoduje řada dalších autorů (Winkler, 2011, s. 35; Halpert, 2011, s. 8).

2.4.1 Veřejný cloud

Halpert (2011, s. 9) definuje veřejný cloud jako cloud, kde jsou služby poskytovány velkému množství zákazníků. Za dostupnost poskytované služby je odpovědný poskytovatel. Výhodou je nízká cena za služby. Nevýhodou je omezená možnost přizpůsobení služby podle potřeb zákazníků, která vyplývá z myšlenky veřejného cloudu a to je poskytnutí služeb co nejvíce zákazníkům.

Jak uvádí Winkler (2011, s. 40) s veřejným cloudem je úzce spjata problematika zabezpečení. Je třeba zajistit, aby každý zákazník měl přístup pouze k vlastním datům a zároveň zamezit přístupu k datům, která mu nenáleží. Veřejný cloud využívá pro ověření uživatele různých mechanismů. Nejčastějším způsobem je autentizace, autorizace a accounting. Podrobněji se zabezpečení věnuje kapitola 2.9.

2.4.2 Privátní cloud

Privátní cloud se od veřejného liší zejména tím, že je využíván pouze pro potřeby organizace v rámci vnitřní sítě (intranetu). Někdy je též nazývaný jako soukromý cloud. Z toho vyplývá, že organizace musí vlastnit celou infrastrukturu. Halpert (2011, s. 9)

Poskytovatelem je nejčastěji IT oddělení, případně je zajištěn prostřednictvím outsorcingu. V porovnání s veřejným cloudem je hlavní předností znalost infrastruktury a především lepší kontrola nad umístěním dat. Při využívání privátního cloudu není nutné řešit problém přístupu více různých zákazníků (podniků) k infrastruktuře, jako u veřejného cloudu.

2.4.3 Komunitní cloud

Komunitní cloud je specifickým případem veřejného cloudu. Infrastruktura je sdílena mezi několika organizacemi, které ji využívají a tvoří uzavřenou komunitu. Může být vlastněna přímo organizacemi v komunitě nebo třetí stranou. Tyto organizace může spojovat

například obor jejich činnosti nebo stejné požadavky na cloudové služby (Mell, Grance, 2009, s. 3). Komunitní cloud nachází uplatnění především ve sféře státní správy.

2.4.4 Hybridní cloud

Hybridní cloud je spojením privátního a veřejného cloudu, kdy je kvůli bezpečnosti část infrastruktury provozována v rámci organizace a část si organizace pronajímá od třetí strany. Organizace tak může mít část svých dat pod kontrolou a část může být mimo.

Dle Mella a Grance (2009, s. 3) zůstávají propojené cloudy unikátními entitami. Jsou vzájemně provázány s pomocí standardizovaných aplikačních rozhraní nebo proprietárních technologií, které umožňují datovou i aplikační přenositelnost.

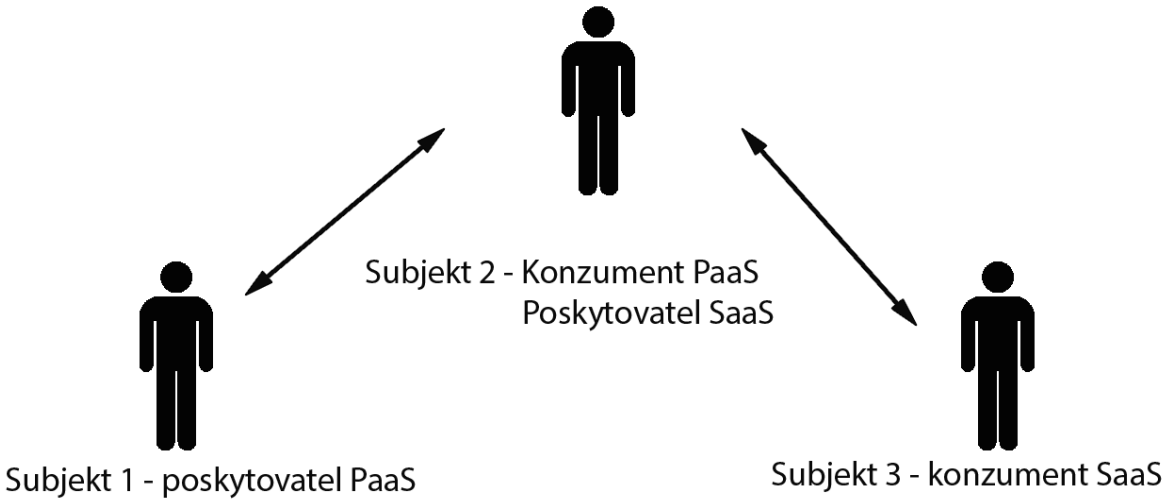
2.5 Uživatelské role

Součástí cloud computingu jsou skupiny účastníků, z nichž každý má jiné odpovědnosti a povinnosti. Účastníci se dělí do tří skupin, resp. rolí. Na konzumenty, poskytovatele a integrátory (Halpert, 2011, s. 4). Účastníci mohou zaujímat více těchto rolí.

- Konzument využívá cloudové služby, které mu poskytuje poskytovatel za určitý poplatek. Nezajímá se o technickou stránku poskytování služby, pouze jí využívá. V roli konzumenta může být nejen koncový zákazník, ale i poskytovatel, který využívá určité služby a může je poskytovat ostatním zákazníkům, případně rozšířit nabídku o další služby.

- Poskytovatel, jak již název napovídá, poskytuje služby zákazníkům. Z technického hlediska je poskytovateli jedno, jestli je jeho zákazníkem další poskytovatel nebo koncový zákazník. Na následujícím obrázku poskytuje subjekt 1 služby subjektu 2, který je zároveň poskytovatelem dalších služeb subjektu 3.

- Integrátor je účastník, který se také někdy označuje jako makléř. Poptává určitý typ služeb od více poskytovatelů a tyto služby poskytuje jako jednu službu dalším zákazníkům. Integrátorem tedy nemůže být nikdy koncový zákazník. V případě poruchy je však plně závislý na poskytovateli služby, na kterého se musí obracet, protože poruchu není schopen sám opravit. Na následujícím obrázku je v roli integrátora subjekt 2.



Obrázek 4 - Uživatelské role cloud computingu (zdroj: upraveno dle Halpert, 2011, s. 7)

2.6 Komponenty cloudu

Základními stavebními prvky cloudu jsou klienti, distribuované servery a datová centra. „Tyto komponenty představují tři součásti řešení cloud computingu. Každý prvek má svůj účel a hraje při poskytování funkční aplikace založené na cloudu nezastupitelnou roli.“ (Velte, Velte a Elsenpeter, 2011, s. 26)

2.6.1 Klienti

Velte, Velte a Elsenpeter, (2011, s. 26) uvádí, že klienti mohou být pracovní stanice, stejně tak notebooky, chytré telefony či tablety. Obecně lze říci, že klientem je zařízení, prostřednictvím kterého může uživatel spravovat data v cloudu. Lze je rozdělit do tří skupin:

- Tlustý – jedná se o běžný počítač připojený prostřednictvím webového prohlížeče ke cloudovým službám. Součástí počítače musí být operační systém, případně další aplikace, které uživatel používá. Pokud potřebuje uživatel mít uloženy soubory ve vlastním počítači, je toto řešení dobrou volbou stejně jako v případě použití aplikací, které nejsou v cloudu k dispozici. Nevýhodou jsou vyšší náklady na údržbu a provoz počítačů. V případě havárie může dojít ke ztrátě dat.

- Tenký – alternativa tlustého klienta. Všechna data jsou zpracována a uložena na serveru. Uživateli jsou zobrazeny pouze výstupní informace, případně se od něj očekává zadání vstupních informací. Fyzicky se jedná o počítače bez interních pevných disků. Výhodou jsou nižší pořizovací náklady a náklady na provoz a údržbu.

- Mobilní – řadí se mezi ně chytré telefony, PDA, tablety, apod.

2.6.2 Datová centra

Datové centrum je složeno z několika serverů, na kterých jsou umístěny aplikace a data, které jsou prostřednictvím cloud computingu využívány. V případě veřejného cloudu může být datové centrum poskytovatele umístěno v jakémkoli státě na světě. Pro privátní cloud je typické, že datové centrum je umístěno v budově firmy, která cloud provozuje a využívá.

2.6.3 Distribuované servery

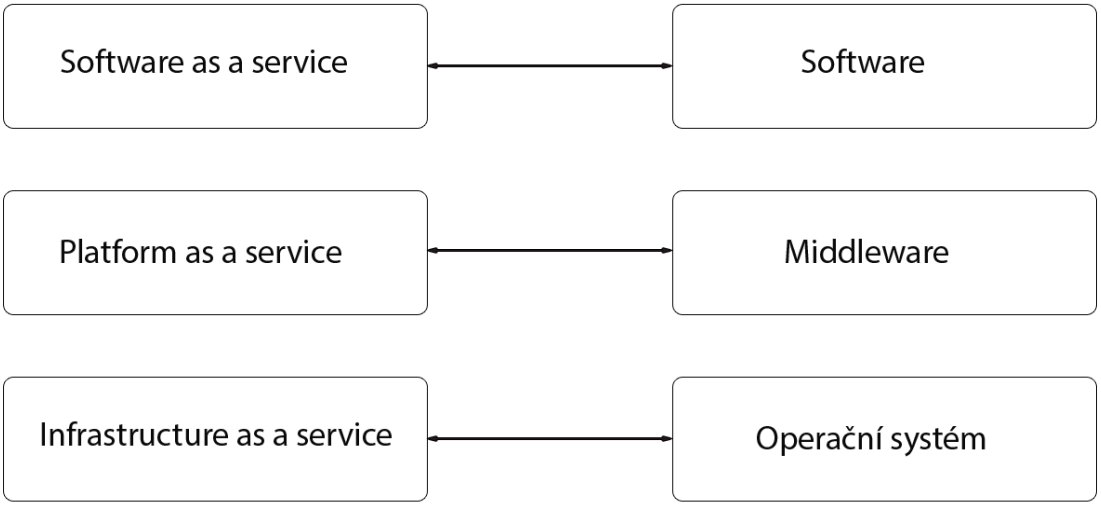
Distribuované servery slouží stejně jako datová centra k hostování aplikací a dat. Zásadním rozdílem je jejich geografické umístění. Servery v datovém centru se nachází všechny na jednom místě. Distribuované servery jsou umístěny v různých částech světa. Z hlediska zákazníka se však jeví tak, jako by byly umístěny vedle sebe a jednalo se o datové centrum.

Z hlediska poskytovatele je zajištěna vyšší bezpečnost poskytovaných služeb. V případě výpadku serveru na jednom místě je služba dostupná z ostatních serverů umístěných v jiných lokalitách. Poskytovatel má rovněž možnost lépe reagovat na poptávku svých služeb. Pokud cloud vyžaduje instalaci dodatečného hardware, stačí servery nakonfigurovat mimo serverovnu a nastavit je jako součást cloudu.(Velte, Velte a Elsenpeter, 2011, s. 28).

2.7 Modely cloudových služeb

Poskytovatelé cloudových služeb nabízí svým zákazníkům různé druhy těchto služeb. Z hlediska typu existuje několik modelů. Ty určují, jaké služby jsou poskytovány. Obvykle se jedná o hardware, software, či jejich kombinaci. Podle NIST jsou zavedeny tři modely (úrovně) poskytování služeb. IaaS (Infrastructure as a Service), PaaS (Platform as a Service) a SaaS (Software as a Service). Vyšší vrstvy v sobě zahrnují nižší vrstvy. Tento způsob pohledu se nazývá Bottom-UP.

Na následujícím obrázku je vidět srovnání klasického modelu a jemu odpovídající vrstvy s využitím cloud computingu.



Obrázek 5 - Tradiční model versus cloud computing model (zdroj: upraveno dle Halpert, 2011, s. 4)

Úroveň poskytovaných služeb je mezi zákazníkem a poskytovatelem definována na základě SLA (Service Level Agreement) smlouvy. Je hojně využívána v prostředí IT při outsorcingu služeb. Její podstatou je jasné vymezení pravidel a případných sankcí. Ve smlouvě by mělo být vymezeno, co je dodáno, za jakou cenu, odpovědnost zúčastněných stran a lhůty případných servisních oprav. (WU, KUMAR GARG a BUYYA, 2012)

2.7.1 IaaS

Velte, Velte a Elsenpeter (2011, s. 35) ji označují také jako HaaS (Hardware as a Service). Jak název napovídá, poskytovatelé této služby poskytují svým zákazníkům určitou část infrastruktury. Typicky se jedná o virtuální stroj, který má přiděleny hardwarové prostředky podle požadavků zákazníka. Pro něj představuje hlavní výhodu to, že si nemusí pořizovat vlastní hardware, který je velice nákladnou záležitostí a platit za jeho uložení v datovém centru. Správa hardwaru je plně v režii poskytovatele, který je za ní zodpovědný. Na pronajaté infrastruktuře může zákazník provozovat vlastní operační systém a aplikace.

Mezi známé poskytovatele této služby patří firma Amazon se svou službou Amazon Elastic Compute Cloud. (Velte, Velte a Elsenpeter 2011, s. 35-36, Winkler, 2011, s. 44)

2.7.2 PaaS

Poskytovatelé PaaS (Platform as a Service) neposkytují pouze infrastrukturu, ale i nástroje pro podporu tvorby sofistikovaných aplikací a služeb. Příkladem jsou databáze, webové aplikační servery, vývojová rozhraní (JRE, atd.). Součástí PaaS je rovněž operační systém na kterém tyto služby běží. Zákazník se nemusí starat o infrastrukturu zahrnující síť, servery, operační systém nebo paměťový prostor. Infrastrukturu může vlastnit buď přímo poskytovatel, nebo ji má pronajatou od dalšího poskytovatele. (Halpert, 2011, s. 5; Winkler, 2011, s. 43)

Pokud se vyskytne problém v IaaS nebo PaaS, komunikuje zákazník pouze se svým poskytovatelem služeb. Ten musí v případě poruchy IaaS kontaktovat svého poskytovatele IaaS aby byl problém vyřešen. Poskytovatel PaaS je tak zodpovědný i za služby IaaS, které jsou mu poskytnuty. Nevýhodou je také snížená schopnost přenosu aplikací mezi jednotlivými poskytovateli.

Hlavní výhoda spočívá v kontrole operačního systému a nasazení vytvořených aplikací.

Nevýhodou je ztráta aplikací v případě ukončení činnosti poskytovatele a omezená míra přenositelnosti aplikací. Pokud je aplikace vytvořena a nasazena u jednoho poskytovatele cloudu a zákazník se rozhodne pro přechod k jinému poskytovateli, není zaručeno, že u něj bude možné aplikaci provozovat (Velte, Velte a Elsenpeter, 2011, s. 34).

Populárním poskytovatelem služeb typu PaaS je Windows Azure od firmy Microsoft.

2.7.3 SaaS

SaaS (Software as a Service), někdy také označována jako AaaS (Application as a Service) je poskytnutí konkrétní aplikace zákazníkovi. Ta je přístupná prostřednictvím tenkého klienta, typicky přes webový prohlížeč, případně přes rozhraní aplikace. Proto mohou být tyto služby poskytovány velkému množství uživatelů. Příkladem jsou emailové služby. (Winkler, 2011, s. 33)

Benefity SaaS jsou především možnost rychlého nasazení aplikace do provozu a možnost vyzkoušení aplikace. Většina dodavatelů poskytuje třicetidenní zkušební lhůtu, po kterou se může zákazník rozhodovat, zda aplikace vyhovuje jeho potřebám, což klasický způsob instalace aplikací obvykle neumožňuje.

Tento typ služeb je pro poskytovatele nejkomplikovanější, protože se musí starat nejen o infrastrukturu, ale i o správu operačního systému a správu poskytovaných aplikací.

Halpert (2011, s. 6) spatřuje problém ve vzájemném ovlivňování kvality služeb mezi jednotlivými zákazníky. Velte, Velte a Elsenpeter (2011, s. 33) vidí nevýhodu modelu SaaS pro organizace se specifickými potřebami na aplikace. Ty nemusí být dostupné a je nutné zakoupit licenci a následně software nainstalovat do jednotlivých pracovních stanic.

2.7.4 CaaS

Poměrně novým modelem je v rámci cloud computingu CaaS (Comunnication as a Service) neboli poskytování komunikačních služeb a věcí s nimi souvisejících, jako je zabezpečení sítě a vyhrazená šířka pásma. Uplatnění je zejména v oblasti audio či video konferencí. Model zahrnuje i technologii VoIP a IM. Pro zákazníka je důležitým faktorem zajištění garantované kvality služeb (QoS). Stejně jako v případě ostatních modelů je velkou výhodou možnost škálování služeb. (Böhm et al., 2010, s. 12)

2.7.5 MaaS

S nasazením cloudového řešení poskytování služeb by měla u každého zákazníka vyvstat otázka, zda infrastruktura případně aplikace budou vyžadovat monitorovací nástroje. Jejich

nasazení by do jisté míry eliminovalo rizika spojená s jejich používáním. To zajistí MaaS (Monitoring as a Service) a umožní snížit provozní náklady spojené s touto činností. Zákazník má všechny své aplikace a infrastrukturu pod kontrolou.

2.8 Virtualizace

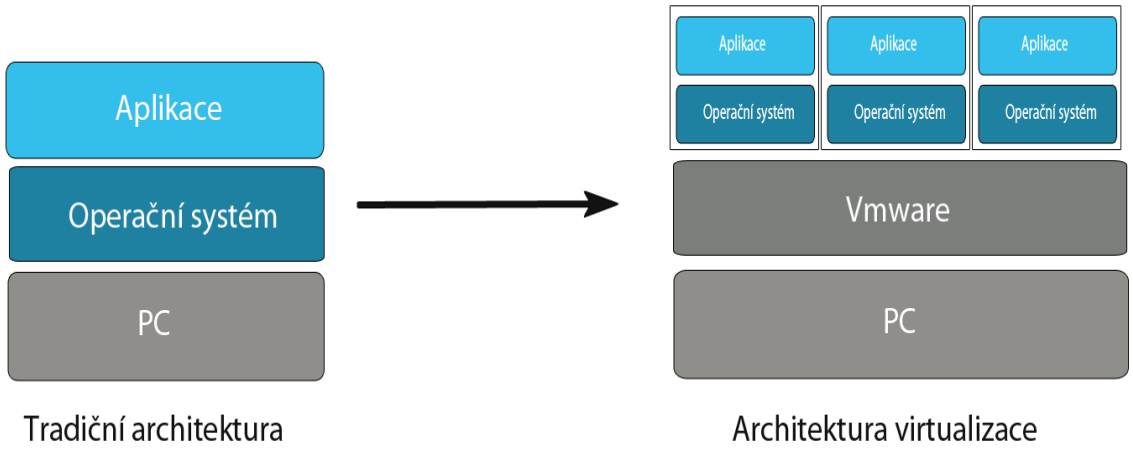
Technologie virtualizace s cloud computingem velice těsně souvisí. Zajišťuje řešení přístupu ke cloudovým službám a především jeho dvě základní vlastnosti: resource pooling a rapid elasticity.

Virtualizací se zabývala už v 60. letech 20. století firma IBM, za účelem rozložení výpočetního výkonu mainframů do více virtuálních strojů, k docílení zpracování více úloh současně. Došlo k eliminaci nevýhody tehdejších pracovních stanic, které mohly zpracovávat současně pouze jednu úlohu. (Havlík, 2010)

S rozšířením modelu klient-server v 80. letech bylo možné spojení více pracovních stanic do jednoho celku. Virtualizace nebyla potřebná v takové míře jako dříve. S dalším rozvojem technologie a nárůstem výpočetního výkonu se objevily nové problémy. Docházelo ke špatnému využívání výkonu, zvyšování nákladů na údržbu a problémem byla i malá ochrana před případnými výpadky. Vhodným řešením bylo opětovné nasazení virtualizace, kdy na fyzickém hardware dochází k emulaci několika virtuálních zařízení, mezi které se rozloží výpočetní výkon a zvýší se efektivnost.

Virtualizaci lze chápat jako abstrakci software, případně hardware od uživatele. Abstrakce je možná na různých úrovních. Může být virtualizováno softwarové prostředí (operační systém), případně hardwarové komponenty (procesor, diskový prostor) nebo celé pracovní stanice (virtuální stroj). Podle těchto úrovní lze rozlišit různé druhy virtualizace.

Asi nejznámější společností, zabývající se problematikou virtualizace, je americká firma VMWare, která nabízí řešení virtualizace serverů i pracovních stanic. Již v roce 1999 vydala svůj první produkt VMWare Workstation, který umožnoval používat různé instance operačních systémů na jednom fyzickém stroji. (VMWare, 2014)



Obrázek 6 - Princip virtualizace (zdroj: upraveno dle VMWARE, 2014))

Hlavními přínosy virtualizace je dle Velte, Velte a Elsenpetera (2011, s. 30) možnost vzájemné izolace uživatelů. Angeles (2014) pokládá za hlavní výhody škálovatelnost zdrojů a snížení nákladů na zdroje. Stejného názoru je i Prodělal (2010).

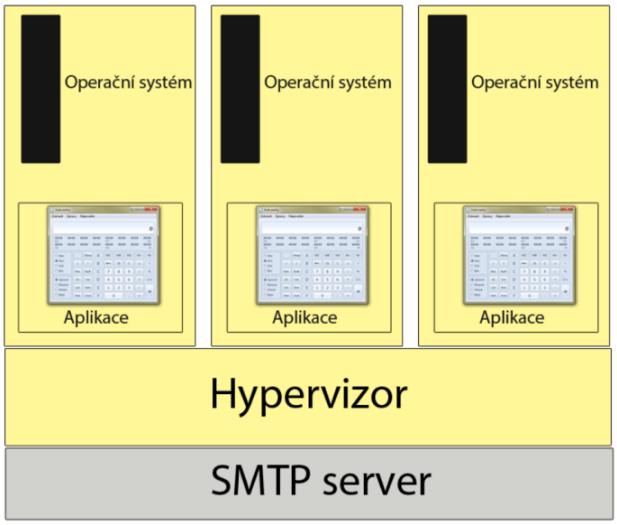
Problematika virtualizace je velice rozsáhlá a není účelem této práce ji detailně popisovat. Jsou zde představeny základní používané principy a techniky. Podrobně se zabývá virtualizací například Šretr (2011) ve své diplomové práci. Navíc uvádí srovnání virtualizačních nástrojů pro platformu x86.

2.8.1 Hypervizor

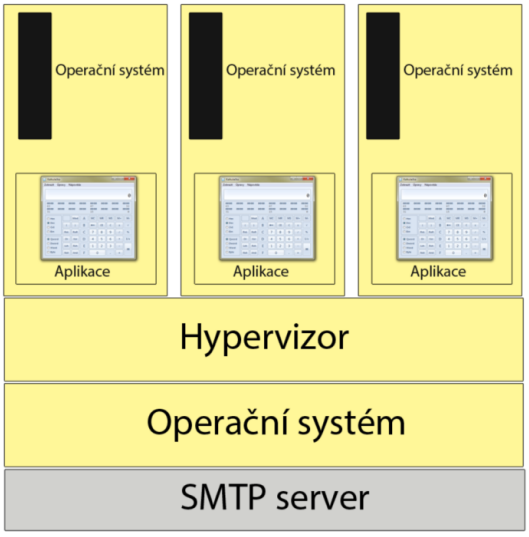
Hypervizor, někdy také označován jako virtual machine manager, je speciální software, který poskytuje hostovaným operačním systémům výpočetní zdroje serveru. Podle (Hurwitze et al., 2009) nachází v cloud computingu velké uplatnění, protože je obvykle třeba poskytnout jednu aplikaci mnoha hostovaným operačním systémům. Bez použití hypervizoru by mohlo dojít k situaci, kdy by více operačních systémů požadovalo přístup k hardware fyzického serveru. Hypervizor zajistí abstrakci hardware a zobrazení aplikace bez nutnosti jejího kopírování do každého systému odděleně.

Jak se shodují (Jannsen, 2014; Virtual systems overview, 2004; Rodríguez-haro et al., 2012, s. 3-4) existují dva typy hypervizoru. První ty je hypervizor instalovaný přímo na hardware serveru. Tuto technologii využívá například Microsoft Hyper-V, Oracle VM nebo VMware ESX. V literatuře je někdy označována jako nativní virtualizace.

Druhý typ využívá operační systém, který je umístěn mezi hardware serveru a hypervizorem a zajišťuje jeho fungování. Ten se chová jako běžící aplikace. Příkladem je Oracle VirtualBox, Parallels Desktop či VMware Fusion (Winkler, 2011, s. 59).



Obrázek 7 - První typ hypervizoru (zdroj: upraveno dle Virtual systems overview, 2004)

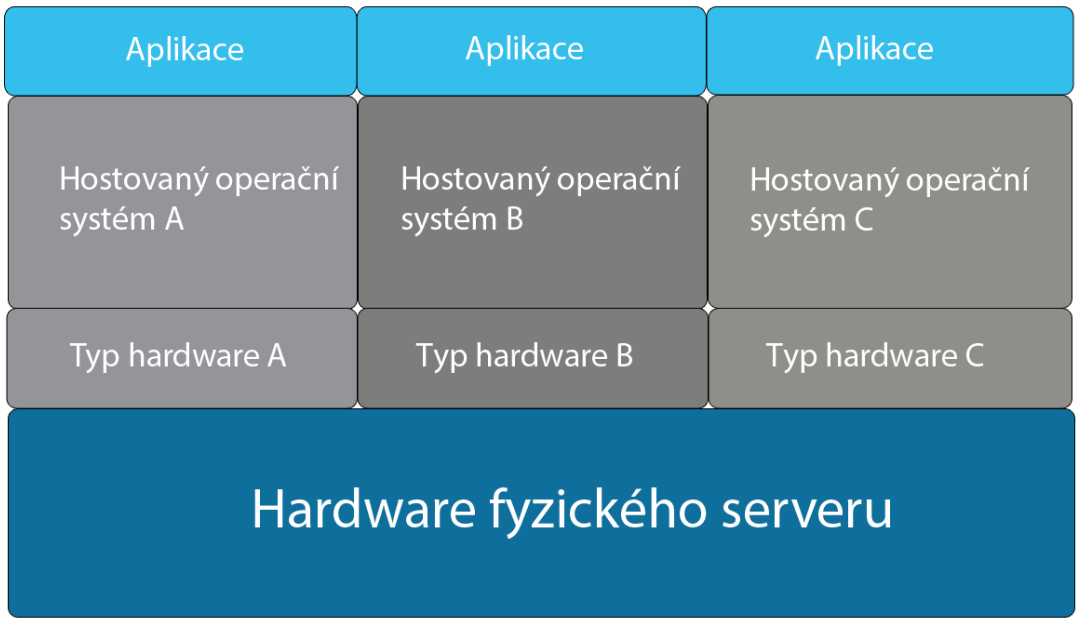


Obrázek 8 - Druhý typ hypervizoru (zdroj: upraveno dle Virtual systems overview, 2004)

2.8.2 Emulace

Principem emulace je spuštění platformy a jejích aplikací na jiné platformě. Strojové instrukce hostovaného systému jsou překládány na strojové instrukce hostitelského stroje (Rodríguez-Haro et al., 2012, s. 3).

Efektivnost je díky rychlosti překladu velmi malá. I přes tuto nevýhodu se jedná o jediný způsob, jakým lze virtualizovat jinou architekturu. Lze emulovat víceprocesorový stroj na jednoprocesorovém stroji. Častým využitím je testování vyvíjených aplikací pro mobilní telefony (Chantry, 2009). Mezi známé emulátory patří BOCHS, QEMU.



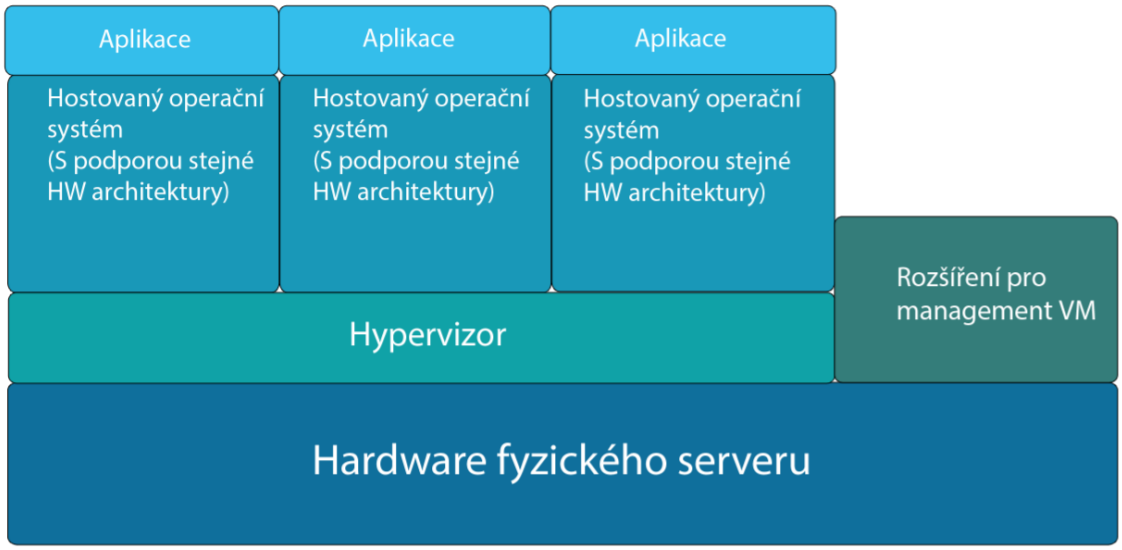
Obrázek 9 - Emulace (zdroj: upraveno dle Chantry, 2009)

2.8.3 Plná virtualizace

Plná virtualizace vytváří kompletní virtuální hardware. Zjednodušeně řečeno umožňuje provozovat kompletní instanci jedné pracovní stanice v jiné pracovní stanici. Operační systém ani aplikace nepotřebují žádné modifikace. Stejně tak nemůže operační systém rozpoznat, že nemá přístup k fyzickému hardware. Výhodou je přizpůsobení virtuálního prostředí podle aktuálních potřeb. Jak uvádí Matyska (2007) mezi virtuálním prostředím a hardware neexistuje přímá vazba a tím je zajištěna plná přenositelnost virtuálního počítače bez nutnosti jeho úprav. Všechny hostované operační systémy běží na stejné hardwarové architektuře. Tím se značně liší od emulace.

Tato technika je často využívána u privátního cloudu. Firmy nemusí nakupovat velké množství serverů, což vede ke snižování nákladů a lepšímu využití výpočetních zdrojů serverů.

Plnou virtualizaci využívají například VirtualBOX, VMware Workstation nebo Parallels Desktop.

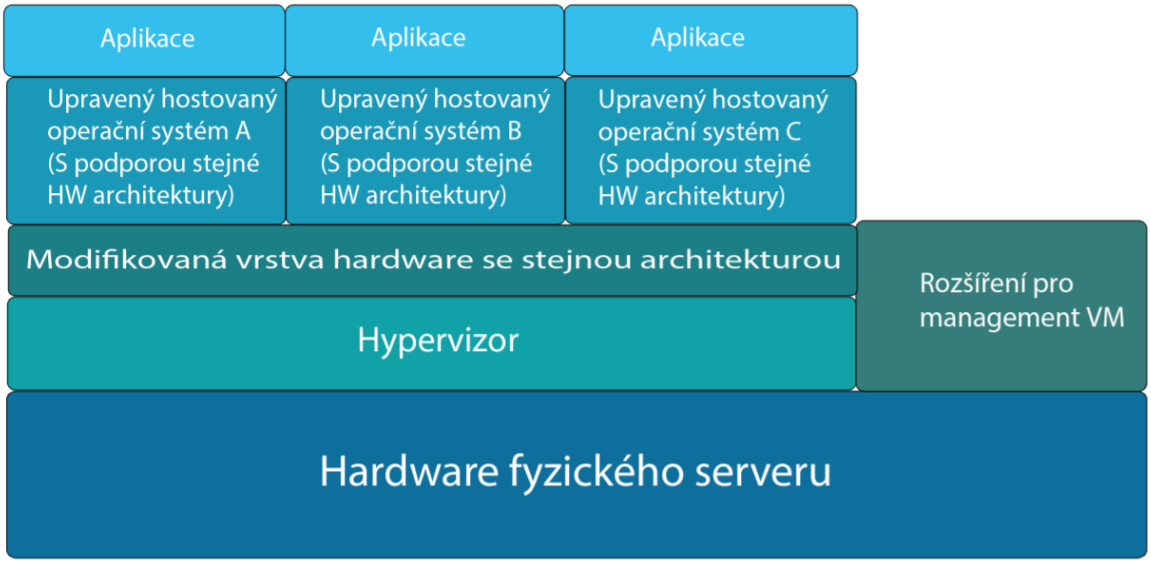


Obrázek 10 - Plná virtualizace (zdroj: upraveno dle Chantry, 2009)

2.8.4 Paravirtualizace

Velte, Velte a Elsenpeter (2011, s. 30), Rodríguez-Haro et al. (2012, s. 2) i Gála, Pour a Šedivá (2009, s. 404) mají stejný pohled na definici paravirtualizace. Při ní nedochází ke kompletní simulaci hardwaru, ale pouze jeho určitých částí. Je možné hostovat více operačních systémů na jednom fyzickém stroji. Jádro hostujícího operačního systému musí být upraveno. Hostovaný operační systém nemá přístup k fyzickému hardware a musí být proto také upraven. Součástí jádra hostujícího operačního systému je též modul pro správu paravirtualizace - hypervizor. Všechny požadavky pro přístup k hardware jsou převedeny na volání hypervizoru (hypercall). Tím je zajištěn vyšší výkon, než u úplné virtualizace. Tento typ virtualizace je vhodné použít v případě shody hardwarových komponent u virtuálního a fyzického stroje.

Velte, Velte a Elsenpeter (2011, s. 30) spatřují hlavní výhody paravirtualizace ve snadném přesunu na nový systém, zotavení po havárii a především škálovatelnosti. Pokud není možné modifikovat operační systém a jeho jádro, nelze použít tento typ virtualizace. Nevýhodou je již zmíněná nutnost modifikace zdrojových kódů hostovaného a hostujícího operačního systému.



Obrázek 11 - Paravirtualizace (zdroj: upraveno dle Chantry, 2009)

2.8.5 Grid computing

Často zaměňovaným pojmem s cloud computingem je grid computing. Ve skutečnosti mají obě technologie společné pouze některé vlastnosti. Grid computing je založen na využití sdílených zdrojů pro řešení jednoho problému, převážně za účelem vědeckého zkoumání. K tomu využívá speciální software, který dokáže rozdělit program na menší celky a distribuovat je pracovním stanicím. Prakticky se tak jedná o velké množství zařízení, která poskytují svůj nevyužitý procesorový čas pro řešení daného problému. Řízení zdrojů je decentralizované. V cloud computingu jsou zdroje řízeny centrálně poskytovatelem služby. (Velte, Velte a Elsenpeter, 2011, s. 28)

Technologie grid computingu byla využita například pro projekt SETI @Home, který má za cíl hledání mimozemské inteligence, kdy pomocí programu počítač analyzuje data z radioteleskopu. Mezi další projekty patří například University of California (2014).

Cloud computing má za cíl paralelní využívání více aplikací, čímž se výrazně odlišuje od grid computingu.

2.9 Bezpečnostní rizika cloud computingu

Zvažuje-li podnik či organizace využívání cloudových služeb, je nutné pečlivě brát na zřetel bezpečnostní požadavky. Hojně diskutovanou záležitostí je bezpečnost dat, protože přechod na cloudové služby znamená jejich přesun z vlastní infrastruktury na servery poskytovatele a tím určitou ztrátu kontroly. K nim je zajištěn přístup prostřednictvím internetu. Rizikem jsou možné hrozby poškození, zneužití či modifikace dat.

Tématu bezpečnosti cloud computingu se věnuje mnoho odborných knih, odborných článků i příspěvků na internetu. Pro účely této práce byl využit dokument organizace Cloud Security Alliance. Jedná se o organizaci založenou v roce 2008, která má za cíl podporovat osvědčené bezpečnostní postupy v rámci cloud computingu a poskytovat informace o cloud computingu jako celku. Mezi její členy patří firmy Microsoft, Hewlett-Packard, SAP, Adobe, atd. V březnu roku 2010 vydala tato organizace dokument popisující sedm největších bezpečnostních rizik cloud computingu. Ty jsou součástí knihy Halperta (2011, s. 38-41). Cloud computing od té doby prošel jistým vývojem, který s sebou přinesl nová rizika. Proto byla v roce 2013 vydána aktualizovaná verze dokumentu. Ta rozšířila počet rizik na devět a uvedla srovnání jejich pořadí z roku 2010 a 2013 a modelů cloudových služeb kterých se týkají (Tabulka 1). Následujících devět podkapitol vysvětluje jednotlivá rizika, jak jsou vnímána Cloud Security Alliance a čerpá výhradně ze zdroje Cloud Security Alliance (2013, s. 8-21), pokud není uvedeno jinak. Desátá kapitola představuje další bezpečnostní rizika cloud computingu spolu s pohledy jiných autorů. V jedenácté kapitole je obsaženo shrnutí a porovnání získaných poznatků.

2.9.1 Data Breaches (zneužití dat)

Pro firmy představuje tato hrozba již po dlouhou dobu velké ohrožení jejich konkurenceschopnosti a v krajním případě pro ně může být likvidační. Riziko zneužití citlivých dat firmy jejími konkurenty ve svůj prospěch bylo všudypřítomné ještě před nástupem technologie cloud computingu. S jejím rozvojem přišly zároveň nové možnosti útoků na poskytovatele služeb a riziko krádeže a následné zneužití dat se zvýšilo. V roce 2012 byl zveřejněn článek vědců z University of North Carolina, University of Wisconsin a korporace RSA, ve kterém popsali metodu pomocí které mohl virtuální stroj získat soukromý šifrovací klíč jiného virtuálního stroje běžícího na stejném fyzickém serveru. Dalším velkým možným rizikem je špatně navržená databáze cloudové služby, kdy chyba v aplikaci umožní přístup k údajům o zákazníkovi, případně o všech zákaznících, kteří službu používají.

Ve většině států ve Spojených státech amerických je v platnosti zákon, který ukládá poskytovatelům cloudových služeb povinnost informovat zákazníky o tom, že jejich data byla zneužita a to neprodleně v době zjištění tohoto problému poskytovatelem. Ve smlouvě mezi poskytovatelem a zákazníkem by měl být definován způsob, jakým bude zákazník dostávat tyto informace a v jakém časovém horizontu je mu je schopen poskytovatel poskytnout. Stejně tak pokud zákazník zjistí, že jeho data byla zneužita, měl

by informovat poskytovatele, který zajistí bezpečnostní opatření pro prevenci dalšího zneužití. (Winkler, 2011, s. 84)

Riziko se dá snížit používáním složitého šifrovacího klíče. Stále však existuje možnost jeho odcizení či ztráty a následného odcizení dat. Druhou možností je zálohovat data na externí paměťová média. S tím je však spojena časová náročnost a především zvýšené finanční náklady.

2.9.2 Data Loss (ztráta dat)

Ztráta dat může být pro firmy, stejně jako jejich odcizení, zcela likvidační. Data mohou být ztracena v důsledku útoků crackerů, přírodní katastrofy ale i chybou na straně poskytovatele. Za ztrátu dat není odpovědný ve všech případech pouze poskytovatel, ale i zákazník. Pokud používá šifrovací klíč a dojde k jeho ztrátě, nebude mít zákazník možnost data obnovit.

Cloud Security Alliance (2013, s. 9) dále uvádí případ novináře Mata Honana, kterému v roce 2012 odcizili crackeři přístupové údaje do účtu na Gmailu, Twitteru, Amazonu a Applu. Ty následně využili pro smazání emailové schránky, publikaci rasistických příspěvků na Twitteru a smazání všech dat z iPhonu, iPadu a MacBooku (Honan, 2012).

Legislativa o ochraně osobních údajů není v každé zemi stejná. V roce 2012 proto došlo k novelizování zákona EU z roku 1995 o ochraně, zničení a poškození osobních údajů, který má za cíl jednotný výklad a vymáhání tohoto zákona v rámci EU (European commission, 2012).

Snížení rizika spojeného se ztrátou dat je spojeno s používáním silných hesel a zálohování na externí paměťová média.

2.9.3 Account or service traffic hijacking (odcizení účtu nebo přenášených dat)

Tento typ útoku se neřadí mezi nejnovější hrozby. Cílem je získání přístupových údajů k uživatelskému účtu. Následně může útočník manipulovat s daty uživatele a využívat jeho účet k vlastnímu prospěchu. Amazon v roce 2010 čelil chybě, která umožňovala pomocí XSS přístup k přihlašovacím údajům z webu. V roce 2009 stejná společnost čelila útoku Zeus Botnetů (Whitney, 2009).

Obrana je především v režii zákazníka, který by měl prosazovat jeden uživatelský účet pro každého uživatele a vyhnout se sdíleným účtům. Pokud je to možné měla by se využívat dvouúrovňová autentizace, která využívá kromě uživatelského jména a hesla ještě další způsob ověření uživatelovy identity.

2.9.4 Insecure APIs (nezabezpečené API)

Pro správu cloudových služeb využívají zákazníci softwarové rozhraní, případně API. Dostupnost a bezpečnost služeb je závislá na bezpečnosti základních API, které zajišťují autorizaci, autentizaci, monitoring a další funkce. V případě výskytu bezpečnostní chyby v API není možné zajistit bezpečné fungování služby jako celku. Někteří poskytovatelé se

snaží nabízet zákazníkům rozšířené API, které se tím ale stává komplexnější a mohou se objevit nová bezpečnostní rizika.

Poskytovatel může předcházet těmto hrozbám instalací nejnovějších aktualizací softwaru.

2.9.5 Denial of Service - DoS (odepření služby)

DoS útoků existuje celá řada a není účelem této práce je všechny detailně popisovat. Jsou zde popsány obecné principy útoků. Podrobněji se jim věnoval například Hlaváček (2013) či Hoque et al. (2014).

Cílem tohoto typu útoku je odepření přístupu ke službě, případně ji zpomalit na neúnosnou míru. Nejčastěji je toho dosaženo pomocí konzumace veškerých dostupných systémových prostředků (výkon procesoru, kapacita disku, kapacita operační paměti, atd.) kdy útok probíhá z jednoho PC. Z hlediska cloud computingu je tedy cílem útočníka zabránit zákazníkům aby se dostali ke svým datům a aplikacím. Specifickým případem je útok na konkrétního zákazníka s cílem způsobit mu finanční ztrátu. Varianta kdy aplikace je nedostupná, ale spotřebovává více zdrojů, vede k tomu, že je v konečném důsledku musí zákazník zaplatit, i když ji nevyužíval.

Široce známou variantou je DDoS (Distributed Denial of Service) útok. Princip je stejný jako u DoS, ale jak vyplývá z názvu, k útoku je využíváno více počítačů a typicky se útočí z různých geografických míst. Mezi známé zahraniční skupiny patří Anonymous, která využívá právě DDoS útoky ke svému zviditelnění. V roce 2014 provedla útok proti sponzorům mistrovství světa ve fotbale kvůli údajným vysokým nákladům za toto mistrovství. Již dříve zaútočila na weby Bílého domu, NASA či FBI.

V srpnu 2014 provedla skupina Lizard Squad útok proti PlayStation Network a dalším webům poskytujícím online herní služby. Společnost Sony oznámila, že nedošlo k úniku osobních údajů, avšak výpadek trval v řádu několika hodin. (Etherington, 2014; BBC News, 2014)

Obrana proti tomuto typu útoku není snadná. Jednou z možností je zvýšení výpočetního výkonu serverů. Taková obrana je účinná pouze proti útokům menšího rozsahu. Pořizování infrastruktury aby byla dimenzována na velké útoky je velice neefektivní. Další méně účinnou variantou je omezit na určitou dobu přístup IP adresám z místa útoku. Nabízí se možnost využití firewallu nebo IPS zařízení, které dokáží monitorovat provoz na síti. (Čmelík, 2013)

2.9.6 Malicious insiders (zneužití účtu)

Cloud Security Alliance (2013, s. 16) uvádí definici CERT, což je skupina, která byla založena v roce 1988 s cílem koordinovat reakce na bezpečnostní incidenty na internetu a zveřejňovat bezpečnostní rady. V případě narušení zabezpečení poskytuje také telefonickou podporu pro řešení problémů. CERT (2014) definuje tento typ hrozby jako: „Narušitelem rozumíme současného či bývalého zaměstnance, dodavatele nebo obchodního partnera, který má nebo měl oprávnění k přístupu do podnikové sítě, systému

nebo datům organizace a tento přístup zneužil s úmyslem ovlivnit důvěrnost, integritu, dostupnost informací nebo informačních systémů organizace.“

Velké nebezpečí představuje administrátor poskytovatele, který tak může mít přístup k citlivým informacím. Zákazník by měl mít k dispozici šifrovací klíč, který bude uchovávat mimo cloudové uložiště poskytovatele aby data nemohla být dešifrována. Organizace či podnik by vždy měly zvážit uložení všech šifrovacích klíčů na serveru, který je součástí jejich vnitřní infrastruktury (Velte, Velte a Elsenpeter, 2011, s. 119).

Zejména u veřejného cloudu se musí zákazník plně spoléhat na poskytovatele služby. U privátního cloudu lze riziko omezit definováním uživatelských rolí a případně monitoring služeb a aktivit uživatelů.

2.9.7 Abuse of cloud services (zneužití služeb cloud computingu)

Jak bylo zmíněno dříve, jednou z hlavních výhod cloud computingu je možnost využití velkého výpočetního výkonu bez ohledu na to, zda je zákazníkem velká firma nebo malá organizace. Avšak ne každý využívá tento výkon pro své aktuální potřeby. Ten může být zneužit pro prolamování hesel nebo šifrovacích klíčů. Útočníkovi by běžně trvalo několik let, než by dosáhl úspěchu. Cloud computing poskytuje prostředky, se kterými je možné zkrátit tuto dobu na několik (desítek) minut. Mezi další rizika se řadí šíření malware, distribuce pirátského software či DDoS útok.

Otázkou zůstává jak se takové hrozbě vyvarovat. Poskytovatel si musí odpovědět na otázky, jakým způsobem je možné detekovat zákazníky zneužívající služby a jak jim v tom zabránit.

2.9.8 Insufficient due diligence (neznalost technologie)

S nástupem technologie cloud computingu se mnoho organizací a podniků snažilo tuto technologii implementovat co nejrychleji. Hlavními důvody byla vidina snížení nákladů na infrastrukturu, škálovatelnost, dostupnost na vyžádání, zlepšení bezpečnosti apod. Velké množství z nich ale plně nepochopilo problematiku, kterou s sebou tato technologie přináší jako je reakce poskytovatele v případě incidentu, použití šifrování a monitoring služeb. Vystavují se tak novým rizikům, se kterými se dříve nesetkali.

Zákazník by se měl před přechodem na využívání cloudových služeb důkladně s touto technologií seznámit a zvážit nejen benefity, ale především možná rizika. Také seznámení s poskytovatelem služeb je důležité, především s jeho technologiemi. Zákazník by si měl ověřit schopnost poskytovatele zajistit takové služby, které budou vyžadovány, především z hlediska bezpečnostních požadavků.

2.9.9 Shared technology vulnerabilities (sdílení technologické chyby)

Služby cloud computingu jsou poskytovány škálovatelným způsobem a nezáleží na tom, zda se jedná o infrastrukturu, platformy, případně aplikace. Především komponenty infrastruktury (CPU, atd.) nebyly navrženy tak, aby byla zajištěna izolace uživatelů při přístupu k nim. Důsledkem výskytu této zranitelnosti může být ohrožen celý cloud.

Obrana spočívá v důsledném monitorování služeb a především v detailně popsaném způsobu zabezpečení datových uložišť, sítě, přístupu uživatelů a aplikací.

2.9.10 Další možná rizika spojená s využíváním cloud computingu

Pokud je privátní, hybridní nebo komunitní cloud realizován outsorcingem, nachází se datové centrum typicky mimo budovu podniku (organizace). Zaměstnanci přistupují ke cloudovým službám prostřednictvím sítě Internet a je třeba zajistit zabezpečený vzdálený přístup. Vhodnou variantou je použití sítí typu VPN s využitím protokolu SSL případně TLS, které poskytují zabezpečený přenos dat. Zákazník by měl rovněž obeznámit všechny uživatele s bezpečnostními pravidly, která musí dodržovat při používání služeb. (Velte, Velte a Elsenpeter, 2011, s. 117-118)

Za bezpečnost infrastruktury je plně odpovědný poskytovatel. Z jeho strany by měly být zákazníkovi na vyžádání dány všechny potřebné informace týkající se poskytovaného zabezpečení. Samozřejmě poskytovatel nemůže odhalit podrobnou konfiguraci zabezpečení svých datových center. Tím by se vystavoval, v případě vyzrazení těchto informací, potenciálnímu útoku. Požadavky na bezpečnost cloudu a úrovně poskytované ochrany byly proto standardizovány normami ISO 27001 a ISO 27002 (Published ISO27k standards, 2014) Zákazníka stačí informovat, jakou normu poskytovatel splňuje a tím je jasně uvedeno, jaké zabezpečení je mu schopen nabídnout.

Legislativní a geopolitická rizika představují další problém, který si mnoho zákazníků neuvědomuje, ale mohou mít pro ně i fatální následky. Servery, na kterých jsou uložena jejich data, jsou často rozmístěny po celém světě a zákazník nemusí mít představu, kde se nachází (kapitola 2.6). Jejich umístění má však zásadní roli v tom, kdo k nim může mít přístup. Pokud budou data podniku sídlícího v České republice uložena na serveru českého poskytovatele, který se ale nachází na území Spojených států amerických, budou tato data podléhat legislativě platné ve Spojených státech, nikoli v České republice.

EU uplatňuje specifický přístup při přesunu dat ze serverů umístěných v rámci státu EU na servery nacházející se mimo EU. V takovém případě musí poskytovatel o tomto přesunu dat informovat zákazníky a zároveň mít uzavřenou dohodu s vlastníkem serverů, na které budou data přesunuta. Tato dohoda musí být předem schválena příslušným státním orgánem, který má v kompetenci ochranu údajů. Mezi Spojenými státy a EU existuje vzájemná dohoda o předávání dat, kdy příjemce ve Spojených státech musí být registrován u tamního ministerstva obchodu. Tím je zaručeno, že příjemce je schopen zajistit potřebnou úroveň ochrany dat. Winkler (2011, s. 80-81)

Ochranu osobních údajů, přístup k datům a nakládání s nimi upravuje v rámci EU již zmíněná novela zákona o ochraně osobních údajů (European commission, 2012). V Číně má vláda ze zákona právo neomezeného přístupu k datům bez ohledu na to co je jejich obsahem. Řešením je použití šifrování dat. Ovšem není zaručeno, že na nařízení vlády nedojde k jejich dešifrování (Winkler, 2011, s. 81). Spojené státy americké zavedly zákony HIPPA (United States of America, 1996) a COOPA (United States of America, 1998). První z nich se týká zdravotních záznamů občanů. Druhý ochrany dětí na internetu,

především poskytování jejich osobních údajů. Pokud existuje podezření ze spáchání trestného činu, může si bezpečnostní úřad vyžádat data podezřelé osoby či podniku na základě zákona USA Patriot Act (United States of America, 2001). Kanadská vláda díky tomu učinila zásadní rozhodnutí pro ochranu svých dat. „Kanadská vláda prohlásila, že vládní zaměstnanci IT nemohou používat síťové služby, které působí na území Spojených států amerických." (Velte, Velte a Elsenpeter, 2011, s. 47)

2.9.11 Charakteristiky rizik cloud computingu dle Winklera a Gartnera

Mezi známé a uznávané osobnosti v oblasti cloud computingu patří i J. R. Winkler a společnost Gartner. Tito autoři jsou citovaní v mnoha článcích věnujících se cloudu, například (Sandeepraja et al., 2013, s. 28 – 32; Lemoudden, Bouazza a Ouahidi, 2014; Brogan, 2014; Mahmood, 2013, s. 44). Proto je v této kapitole uveden i jejich pohled na bezpečnostní rizika této technologie.

Winklerův (2011, s. 56) pohled na bezpečnost cloudu zahrnuje osm rizik a to:

- Network availability (dostupnost) – dostupnost je jednou z klíčových vlastností cloud computingu. Poskytované služby musí být dostupné ve chvíli, kdy je zákazník vyžaduje. Potenciální problém nastává v případě výpadku internetového připojení u zákazníka, případně u poskytovatele.

- Privacy and data (ochrana osobních údajů a dat) – data jsou umístěna v datových centrech poskytovatele, která se nemusí nacházet ve stejném státě. Poskytovatel může vlastnit několik datových center v různých státech. Může docházet k situaci, kdy jsou data rozdělena a jednotlivé části jsou uloženy v různých datových centrech.

- Control over data (kontrola nad daty) – data jsou v datovém centru umístěna společně s daty dalších uživatelů. Přístup k nim by měl mít pouze oprávněný vlastník. Mělo by být využíváno odpovídající šifrování, aby se zamezil přístup neoprávněným subjektům.

- Cloud provider viability (konkurenceschopnost poskytovatele) – poskytovatelé cloudu jsou na trhu relativně krátkou dobu a zákazníci musí zvažovat otázku, zda budou plnit své závazky a jaká je míra rizika případného ukončení provozování cloudu jeho poskytovatelem. Zákazník by mohl v takovém případě přijít o všechna data, případně vyvíjené aplikace. Problém je toto zejména u poskytovatelů IaaS (kapitola 2.7.1).

- Security incidents (bezpečnostní incidenty) – zákazníci musí být informováni poskytovatelem v případě výskytu nestandardní události. Ten by měl zároveň zákazníkům zajistit potřebnou technickou podporu při řešení problémů.

- Disaster recovery and business continuity (zotavení po havárii a kontinuita provozu) – zákazníci musí být schopni, v případě poruchy na straně poskytovatele, pokračovat v provozu, aniž by využívali jeho služeb.

- Systems vulnerabilities and risks of common attacks (rizika útoků na systémy poskytovatele) – hardware, software a infrastruktura poskytovatele je do jisté míry zranitelná a může se stát cílem útoků za účelem získání dat, případně vyřazení z provozu.

- Legislativní překážky – používání veřejných cloudů je problematické, pokud data podléhají právním předpisům, případně zákonným omezením.

Lehce odlišný pohled má společnost Gartner, která v roce 2008 definovala sedm bezpečnostních rizik týkající se cloud computingu (Gartner, 2014; Brodkin, 2008):

- Privileged user access (privilegovaný přístup) – dochází k outsorcingu, kdy data jsou uložena na serverech poskytovatele. Zákazník by si měl zjistit co nejvíce informací o společnosti, u které bude mít data uložena. Dále se informovat o tom, které osoby k nim budou mít přístup a jakým způsobem bude kontrolován.

- Regulatory compliance (dodržování předpisů) – i přes umístění dat u poskytovatele služeb je za jejich bezpečnost zodpovědný zákazník. V rámci větších poskytovatelů služeb jsou pravidelně prováděny externí audity, v rámci kterých se zjišťuje, jak zabezpečují svěřená data. Pokud není poskytovatel ochoten se auditů účastnit, případně neposkytne na vyžádání data z těchto auditů, ztrácí důvěryhodnost u zákazníků.

- Data location (umístění dat) – riziko je synonymem rizika ochrana osobních údajů a dat, jak jej definoval Winkler (2011, s. 56). Zákazník nemusí vědět, kde se data nachází fyzicky. Gartner radí, aby se zákazníci ujistili o tom, zda poskytovatel dodržuje ochranu osobních údajů nad svěřenými daty v rámci státu, ve kterém má datové centrum.

- Data segregation (oddělení dat) – data v cloudu se nachází spolu s daty jiných zákazníků. Poskytovatel cloudu by měl použít odpovídající šifrovací mechanismy pro jejich oddělení. Zároveň by měl být schopen doložit informace o tom, jak a kým byly šifrovací mechanismy navrženy. Selhání šifrování může vést až k nepoužitelnosti dat a proto by ho měli navrhovat a testovat pouze odborníci.

- Recovery (zotavení) – Gartner doporučuje zákazníkovi informovat se u poskytovatele, zda v případě selhání je možná obnova dat a za jaký čas je to možné. Poskytovatel by měl průběžně zálohovat data pro zajištění jejich případné obnovy.

- Investigative support (vyšetřování) – v cloud computingu může být nemožné zkoumat nelegální nebo nevhodné činnosti. Cloud služby je velice obtížné

vyšetřovat. Logovací údaje zákazníků jsou umístěny v logovacích souborech různých hostitelů a datových center. Dle Gartnera by zákazníci měli požadovat od poskytovatele podporu šetření spolu s důkazy o tom, že s tímto šetřením má zkušenosti.

- Long-term viability (životaschopnost) – pokud se poskytovatel dostane do finančních problémů, případně ho odkoupí jiná společnost, neměl by tento fakt ovlivnit dostupnost zákazníkových dat. Gartner radí, aby se zákazníci informovali u poskytovatele, jak by v takovém případě dostali svá data zpět a to v takovém formátu, aby je byli schopni importovat do náhradní aplikace.

2.9.12 Shrnutí

Z výše uvedených poznatků je patrná shoda všech autorů týkající se zabezpečení dat, zajištění přístupu k nim a legislativních překážek spojených s jejich umístěním. Dále způsobu komunikace mezi zákazníkem a poskytovatelem v případě výskytu chyb.

Především ochrana dat během přenosu do cloudu, kde existuje riziko odposlechu a jejich samotné uložení na serverech poskytovatele, kdy zákazník nemusí vědět, kde se fyzicky data nachází, je problematické. Správné zajištění šifrování během přenosu a při ukládání dat považují všichni autoři za důležitý aspekt, na který by měl zákazník dbát. Riziko zneužití neoprávněnou osobou je podle všech také nutné brát na zřetel, i když jak bylo zmíněno, je to především záležitost odvíjející se od typu cloudu.

Komunikaci mezi poskytovatelem a zákazníkem a to nejen v případě výskytu chyby, považují také za samozřejmou věc. V neposlední řadě uvádí legislativní překážky spojené s cloud computingem, které si mnozí zákazníci neuvědomují, ale měli by jim věnovat náležitou pozornost a zajímat se o to, v jaké zemi se nachází servery, kde jsou jejich data uložena a jaká je s nimi spojena legislativa.

Tabulka 1 - Bezpečnostní rizika cloud computingu dle společnosti Cloud Security Alliance (zdroj: autor)

Bezpečnostní riziko	Umístění dle míry rizika 2010	Umístění dle míry rizika 2013	Modely cloudových služeb
Data breaches	5	1	IaaS, PaaS, SaaS
Data loss	5	2	IaaS, PaaS, SaaS
Account or service traffic hijacking	6	3	IaaS, PaaS, SaaS
Insecure APIs	2	4	IaaS, PaaS, SaaS
Denial of Service	Nebyl součástí	5	IaaS, PaaS, SaaS
Malicious insiders	3	6	IaaS, PaaS, SaaS
Abuse of cloud services	1	7	IaaS, PaaS
Insufficient due diligence	7	8	IaaS, PaaS, SaaS
Shared technology vulnerabilities	4	9	IaaS, PaaS, SaaS

Z tabulky je patrné že jak se vyvíjí technologie cloud computingu, dochází k přehodnocování bezpečnostních rizik z hlediska míry ohrožení. Zatímco v roce 2010 data breaches a data loos byla brána jako jedno riziko, došlo v roce 2013 k separaci, protože principiálně nevyjadřují to samé. Jsou vnímána jako velice nebezpečná, což dokazuje jejich postup z pátého na první, resp. druhé místo.

Stejně tak account or service traffic hijacking, který se z původně šesté příčky dostal na třetí. Důvodem může být vzrůstající zájem crackerů, kteří jsou si dobře vědomi, že při získání uživatelských údajů mají přístup k datům, které se stávají v mnoha případech cennou komoditou. V podnikovém prostředí zejména z hlediska konkurenčního boje.

Jistý pokrok je vidět i u vnímání zbývajících rizik, ale opačným směrem. S vývojem cloud computingu došlo postupem času k větší popularitě této technologie. S ní jsou podniky a organizace lépe obeznámeny, než tomu bylo v roce 2010. Pokrok je patrný i na straně poskytovatelů cloudu, kteří se neustále snaží vylepšovat zabezpečení a izolaci uživatelů což vede k omezení rizika sdílení technologické chyby. S vylepšeným zabezpečením souvisí i snížení rizika zneužití poskytovaných služeb k nelegální činnosti. Monitoring uživatelů a správné nastavení uživatelských rolí a práv přispěly také k omezení zneužití účtu zaměstnanců poskytovatele pro přístup k datům zákazníků.

2.10 SWOT analýza využívání cloud computingu

Cloud computing z pohledu zákazníků a to nejen potenciálních ale i těch, kteří ho již využívají, přináší celou řadu výhod. Jako každá technologie s sebou přináší ale i řadu nevýhod. V následujících dvou kapitolách je provedena SWOT analýza zkoumající výhody a nevýhody cloud computingu a to z pohledu typu cloudu a poskytovaných služeb.

2.10.1 Silné stránky

Silnou stránkou je především snížení nákladů na nákup a provoz infrastruktury. Zákazník se nemusí starat o nákup serverů a budování síťové infrastruktury. To vše je v kompetenci poskytovatele služeb. Dochází také k významné úspoře mzdových nákladů na IT zaměstnance, kteří nemusí udržovat hardware a jejich počet tím může být, v některých případech, značně omezen.

Poskytovatel má přístup k hardware a software, který je plně v jeho režii a nemusí být fyzicky přítomen u zákazníka v případě poruchy. Forma plateb za využívané služby či infrastrukturu bývá hrazena formou předplatného. Poskytovatel může odhadovat na základě předchozích plateb budoucí výnosy.

Další silné stránky vyplývají z charakteristických vlastností cloud computingu, jak byly definovány v kapitole 2.3. S nimi se ztotožňují i Marston et al. (2009).

Škálovatelnost je pro mnoho firem vlastností cloud computingu, která rovněž souvisí s úsporou nákladů. Nachází využití zejména při náhlém nárůstu požadavků na výpočetní

výkon. Firma se vyhne drahému nákupu a instalaci dodatečného hardwaru, jehož výkon by byl využit pouze po omezenou dobu. Namísto toho si od poskytovatele služeb pronajme dodatečný výpočetní výkon pouze na potřebnou dobu a dojde k úspoře finančních prostředků. S tím souhlasí i Velte, Velte a Elsenpeter (2011, s. 25).

Marston el al. (2011) dále vidí výhody pro začínající startupy a vytváření inovací v IT.

Podrobně se výhodami cloud computingu v prostředí malých a středních podniků zabývali Ghaffari et al. (2014, s. 16). Tento zdroj je aktuálnější než předchozí, ale naprosto se shoduje s výše uvedenými myšlenkami. Úspora nákladů na provoz, které mohou podniky investovat do svého rozvoje, okamžitá dostupnost využívaných služeb a škálovatelnost považují za klíčové výhody cloud computingu.

2.10.2 Slabé stránky

Tsagklis (2013) považuje dostupnost nejen za výhodu, ale i nevýhodu, která nemusí být vždy zanedbatelná. Servery poskytovatelů, na kterých jsou umístěna zákazníkova data, jsou často umístěny po celém světě. Pokud chce mít zákazník přístup k datům, měla by mu být poskytnuta v přijatelném čase. Pro poskytovatele to může představovat potenciální problém.

Stejně tak stálé internetové připojení může být dle Tsagklise (2014) velkou nevýhodou. S tím se ztotožňují i Velte, Velte a Elsenpeter (2011, s. 25). Všechna data jsou uchovávána na serverech poskytovatele a stále ještě existují oblasti, kde internetové připojení není samozřejmostí. V takových oblastech se zákazník není schopen dostat ke svým datům. To samé nastává při výpadku internetového připojení.

Pro poskytovatele představují náklady na zřízení datového centra vysokou investici.

2.10.3 Příležitosti

Finanční prostředky může podnik investovat do modernizace výrobních technologií a tím zvýšit své tržby a konkurenceschopnost. Sjednocení a úprava legislativy by rovněž přispěla k většímu využívání cloudu. Vzhledem k tomu, že cloud computing představuje rostoucí trend v oblasti využívání informačních technologií, budou se stále objevovat nové příležitosti. Míra využitelnosti cloud computingu bude analyzována v rámci výzkumu v kapitole 4.

2.10.4 Hrozby

Mezi hrozby se řadí bezpečnost dat (kapitola 2.9). Především riziko jejich zneužití třetí stranou. S tím souvisí i případné ukončení činnosti poskytovatele, kdy je zákazník vystaven riziku ztráty dat. Z pohledu poskytovatele prioritní je zajištění požadované dostupnosti služeb, které zákazníci vyžadují v režimu 24/7, zajištění bezpečnosti datového centra a ztráta důvěry zákazníků. Negativní reference byť jednoho jediného zákazníka mohou znamenat ztrátu dalších a jejich důvěru lze zpět získat jen velmi obtížně.

Tabulka 2 - SWOT analýza - výhody a nevýhody cloud computingu z pohledu typu cloudu (zdroj: autor)

Silné stránky	Slabé stránky
Snížení nákladů na provoz infrastruktury	Dostupnost dat
Správa HW a SW plně v režii poskytovatele	Závislost na poskytovateli
Snížení mzdových nákladů	Náročnost na internetové připojení
Škálovatelnost	
Příležitosti	**Hrozby**
Zvýšení konkurenceschopnosti	Zneužití dat
Úprava legislativy	Ukončení činnosti poskytovatele
	Zajištění dostupnosti poskytovaných služeb
	Bezpečnost datového centra
	Negativní reference zákazníků

2.11 SWOT analýza z pohledu poskytovaných služeb

2.11.1 Silné stránky

Dostupnost poskytovaných služeb odkudkoli, kde je dostupné připojení k internetu a pracovní stanice.

Stejně jako v předchozím případě, silnou stránkou je především úspora finančních nákladů z pohledu zákazníka, který si zaplatí pouze za službu, resp. za dobu po kterou ji využívá.

Marston el al. (2011) vidí výhody v možnosti vytváření aplikací a poskytování služeb způsobem, jaký dříve nebyl možný. Jako příklad uvádí aplikace, které jsou schopny v reálném čase reagovat na informace od lidí, ze senzorů, případně od více nezávislých zdrojů (celosvětové údaje o počasí). Dalším příkladem je paralelní zpracování velkého množství dat za použití velkého množství dostupného výpočetního výkonu. Na tomto principu je založen například Apache Hadoop.

Při hlášení chyb aplikací jsou vývojáři schopni vydávat častěji menší opravné aktualizace namísto vydání jedné velké, která by obsahovala opravy více chyb.

2.11.2 Slabé stránky

Velkým problémem je hardwarová závislost. Pokud například firma používá aplikaci, která pro svůj chod vyžaduje specifický hardware, musí být poskytovatel schopen tento hardware zajistit. Firma ale nemá jistotu, že se poskytovatel nerozhodne časem tento

hardware vyměnit za jiný a tím způsobit zákazníkovi závažný problém. (Velte, Velte a Elsenpeter, 2011, s. 25)

Aplikace nemusí být přenositelné mezi jednotlivými poskytovateli cloudu (kapitola 2.7.2). Výběr správného dodavatele je proto klíčovou záležitostí. V případě veřejného cloudu, kdy aplikaci používá velké množství zákazníků, je prakticky nemožné ji přizpůsobovat konkrétním potřebám zákazníka.

2.11.3 Příležitosti

Nové aplikace mohou být ihned dostupné velkému množství uživatelů a zvýšit tak v krátké době zisk provozovatele. Pro něj je výhodné přemístit všechny zákazníkovi aplikace do cloudu a získat tak stálý příjem finančních prostředků.

2.11.4 Hrozby

Hrozby se ztotožňují s hrozbami, které byly popsány v předchozí kapitole u typu cloudu.

Tabulka 3 - SWOT analýza - výhody a nevýhody cloud computingu z pohledu typu služeb (zdroj: autor)

Silné stránky	Slabé stránky
Snížení nákladů na nákup aplikací	Hardwarová závislost aplikací
Aplikace pracující s daty v reálném čase	Přenositelnost aplikací mezi poskytovateli
Rychlá implementace a testování aplikací	Znemožněna úprava aplikací podle konkrétní potřeby zákazníka
Škálovatelnost	
Rychlé opravy chyb v aplikacích	
Příležitosti	**Hrozby**
Růst tržeb poskytovatelů	Zneužití dat
Přesun všech aplikací zákazníka do cloudu	Ukončení činnosti poskytovatele
	Zajištění dostupnosti poskytovaných služeb
	Negativní reference zákazníků

2.12 Překážky nasazení cloud computingu

Výhody a nevýhody cloud computingu by měl zákazník vždy zvážit a posoudit, zda-li je využití této technologie pro něj perspektivní ale zároveň je ochoten podstoupit rizika, která s sebou přináší.

Armbrust et al. (2009, s. 14-19) specifikují deset překážek, které mohou zákazníka odradit od implementace cloud computingu. Jsou rozděleny do tří skupin:

- Překážky pro přijetí cloud computingu,
- překážky pro rozvoj cloud computingu,
- obchodní a legislativní překážky pro přijetí cloud computingu.

Tabulka 4 - Překážky nasazení cloud computingu (Zdroj: upraveno dle: Armbrust et al., 2009, s. 14)

Překážka	Popis	Řešení
Překážky pro přijetí cloud computingu		
Dostupnost služby	Přístup zákazníka ke službě je zajištěn kdykoli ho zákazník vyžaduje	Využívat služeb více cloudových poskytovatelů. Využívat možnost pružně přidělovat zdroje k obraně proti DDoS útokům.
Data Lock-In	Použití nestandardního API nebo programovacího jazyka vede k nepřenositelnosti aplikací od jednoho poskytovatele k druhému.	Standardizovat API
Důvěrnost a auditovatelnost dat	Zákazníkova data nesmí být přístupná neoprávněným subjektům.	Použití šifrování, VLAN sítí a firewallů.
Překážky pro rozvoj cloud computingu		
Problémový přenos dat	Data mohou být umístěna ve více lokalitách na různých serverech poskytovatele. Roustoucí objemy dat vyžadují větší přenosy. Pokud zákazník platí za jednotku přenosu, může dojít ke značnému zvýšení nákladů.	Zálohování dat, archivace dat. Nižší cena WAN routerů. Vyšší přenosová šířka pásma LAN switchů. Posílání disků kurýrní službou.
Nepředvídatelnost výkonu	Sdílení RAM a CPU v rámci virtuálních strojů nepředstavuje problém. To neplatí u vstupně-výstupních operacích pevných disků, které se mezi virtuálními stroji ruší.	Vylepšení architektury virtuálních strojů a operačních systémů. Používání flash pamětí.
Škálovatelnost uložiště	Škálovatelnost (zdroje je možné přidělit či odebrat na požádání, zdánlivě neomezená kapacita). Není jasné, jak si ji představit na perzistentním uložišti.	Řešení je stále předmětem zkoumání. Cílem je vytvoření uložiště, které bude kombinovat výhody cloud computingu s požadavky programátorů.

Chyby v rozsáhlých distribuovaných systémech	Odstranění chyb v rozsáhlých distribuovaných systémech je velmi náročné. Předcházet chybám se musí již při tvorbě datových center.	Debugger, který pracuje s distribuovanými virtuálními stroji.
Rychlá škálovatelnost	Různí poskytovatelé cloud computingu využívají odlišné způsoby přidělení či odebrání zdrojů a jejich účtování, které se může odvíjet podle počtu přidělených-odebraných cyklů, případně časového úseku.	Použít dynamické škálování řízené počítačem
Obchodní a legislativní překážky pro přijetí cloud computingu		
Sdílení pověsti	Špatné chování jednoho zákazníka může ovlivnit celý cloud. Pokud zákazník posílá z cloudu spam, IP adresa poskytovatele se dostane na blacklist.	Převést odpovědnost z poskytovatele na zákazníka. Vytvoření databáze autorizovaných emailů-
Licencování softwaru	Zákazník platí licence za software spolu s poplatky za období, kdy ho využívá. Mnoho poskytovatelů se tak ze začátku spoléhalo na open-source software.	Využití pay-as-you-go licencování software. Využití softwaru více uživateli.

Překážky pro nasazení cloudu byly také předmětem průzkumu na českém trhu, který provedli v roce 2011 George Feuerlicht, Lukáš Burkoň, a Michal Šebesta. Celkem 600 českých organizací oslovili v dotazníkovém průzkumu, ve kterém se tázali na využívání cloud computingu v jejich firmách a na problémy s tím spojené.

Z průzkumu vyplynulo, že se 17 % respondentů obává závislosti na poskytovateli služby, 15 % respondentů má obavy ze zvýšených nákladů spojených s modelem předplatného a 14 % respondentů má obavy o bezpečnost.

Pouhé 4 % respondentů využívaly služeb cloud computingu. 6 % respondentů uvedlo, že plánují jejich využití v horizontu příštích dvou let. Pro 26 % respondentů bylo hlavní motivací snížení nákladů, pro 20 % respondentů rychlé nasazení cloud computingu a lepší škálovatelnost. (Feuerlicht, Burkoň a Šebesta, 2011, s. 2)

Pro lepší interpretaci výsledků byly otázky rozděleny do skupin, z nichž se každá týkala jednoho distribučního modelu cloudu. Podle Feuerlichta, Burkoňě a Šebesty (2011, s. 2) jsou bariéry nasazení cloud computingu tyto:

- Respondenti nikdy neslyšeli o cloud computingu,
- vysoká cena,
- bezpečnostní problémy,
- problémy s IT Governance,
- ztráta kontroly,

- nedostatek relevantních služeb,
- problémy s dostupností,
- problémy s rychlostí internetu,
- závislost na externím provozovateli,
- právní problémy.

3 Výzkum využití cloud computingu

Tato kapitola se věnuje popisu a vyhodnocení výzkumu o využití cloud computingu ve firmách a organizacích v ČR. Nejprve je popsána metodika výzkumu, časový harmonogram, výběr respondentů a následně vyhodnocení získaných dat.

3.1 Metodika výzkumu

Jako metodika výzkumu bylo zvoleno použití dotazníku, kdy odpovědi byly zaznamenávány písemnou formou. Dotazník byl z důvodu objektivnosti a upřímnosti veden jako čistě anonymní. Z důvodů dodržení logické a stylistické správnosti jednotlivých otázek bylo provedeno pilotní šetření, k němuž byli osloveni účastníci osvětových přednášek o problematice cloud computingu a jeho nasazení. Součástí dotazníkového šetření bylo rovněž osobní setkání s odpovědnými osobami, které byly ve firmě za danou problematiku zodpovědné. V rámci pohovoru s nimi byla problematika cloud computingu diskutována za účelem získání objektivních odpovědí. Výzkum byl realizován v období od února do listopadu roku 2014.

Pro vyhodnocení dotazníku byly použity kvantitativní metody, které umožňují rychlý a přímočarý sběr dat a relativně snadné zobecnění výsledků. Významným vlivem na využití kvantitativních metod pro vyhodnocení výzkumu byla maximální eliminace závislosti na konkrétním výzkumníkovi. Vybrané otázky, zaměřené hlavně na charakteristiku zkoumaného subjektu, byly sekundárně ověřeny z odpovědí získaných při počátečním rozhovoru. Výsledky dotazníkového šetření budou následně porovnány s vytvořenou SWOT analýzou v kapitole 2.10 .

3.1.1 Forma dotazníku

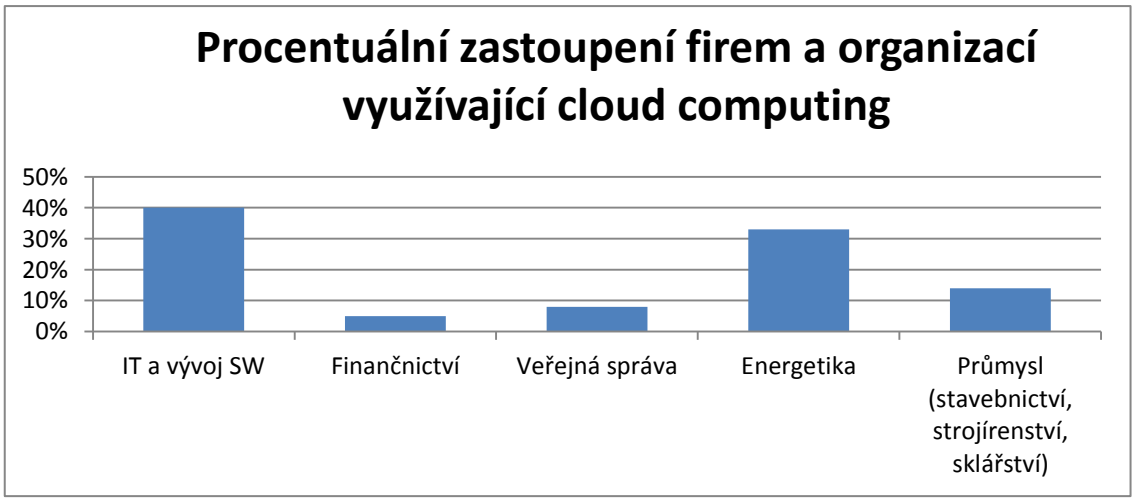
Elektronický dotazník obsahoval celkem 29 otázek s možností výběru odpovědí u každé otázky. Je součástí přílohy A. Část otázek disponuje možností „jiná odpověď“, kde v editačním okně mohli respondenti zadat vlastní odpověď. Dotazník je seskupen do tří logických celků, zaměřených na využívání či nevyužívaní cloud služeb a jejich důvody, otázek z oblasti přechodu a nasazení cloud služeb, problematiku bezpečnosti cloud služeb a v poslední řadě na charakteristiku organizace. Zpřístupňování otázek respondentům bylo závislé na základě jejich prvních odpovědí. Pokud cloud služby již využívají, nebyli logicky dotazováni na otázku, proč je nevyužívají, ale např. jak dlouho jim trval přechod a implementace cloud služby.

4 Výsledky získaných dat a jejich vyhodnocení

Prvním výsledkem bylo zjištění počtu oslovených organizací, které projevily svou účast při spolupráci na výzkumu o využívání cloud služeb. Celkem 43 % se jich na výzkumu podílelo. V rámci šetření a výsledků níže představených byly získány informace ve formě odpovědí v dotazníkovém šetření od 87 organizací. Z nich 73 % cloud služby využívá a 27 % nikoli. Důvodem takto relativně vysoké hodnoty může být to, že organizace, které odmítly poskytnout informace do výzkumu, nemají cloud implementován. Při započtení organizací, které se výzkumu odmítly zúčastnit a u nichž lze předpokládat, že tedy cloud nevyužívají, plyne závěr, že z oslovených organizací v rámci výzkumu jich 35 % cloud služby využívá.

4.1 Struktura organizací v rámci výzkumu

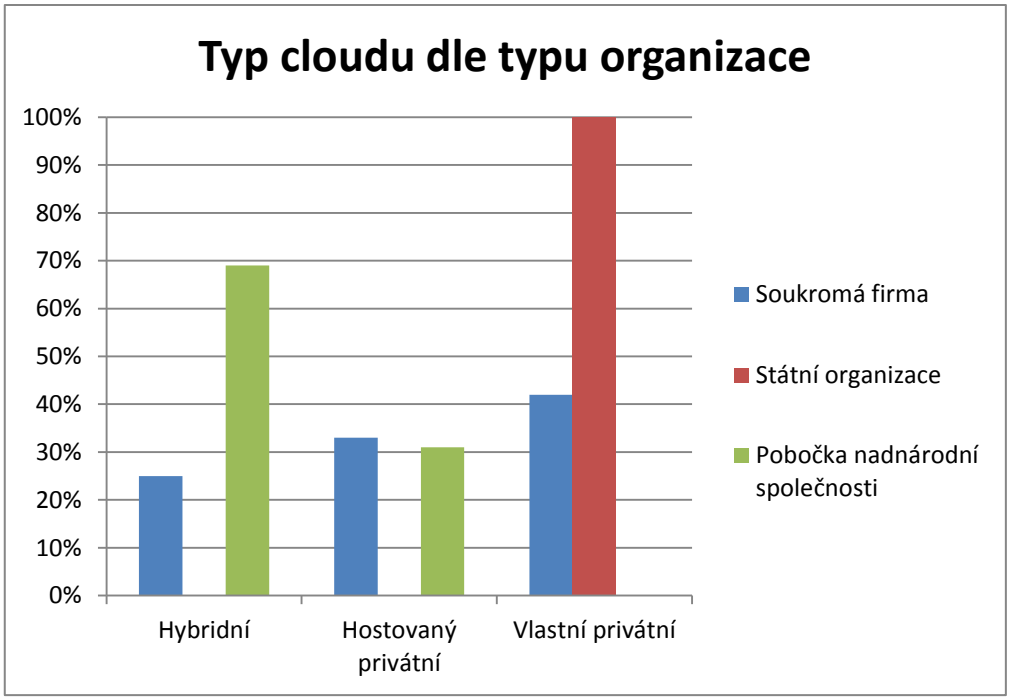
Procentuální zastoupení organizací využívajících cloud služeb je znázorněno na následujícím grafu. Z něj je jasně patrné a nepřekvapivé, že 40 % organizací, jejichž činností je IT, využívá při své činnosti cloud služeb. Za poměrně překvapivý lze také označit 33 % podíl organizací fungujících v oblasti energetiky a to jak výroby, tak správy využívajících cloud služby. Tento výsledek může být přisuzován dynamickému rozvoji nasazování smart networks a smart meteringu, jež je v prostředí České republiky podporován nejen managementem firem, ale také státní dotační politikou. Pouhých 14 % firem, orientovaných na výrobu v oblasti strojírenství, stavebnictví a sklářství, které využívají cloud služby lze přisuzovat relativně vysokým nákladům na inovaci stávajících infrastruktur, které mohou být v některých případech i deset a více let staré. Zajímavé je i zastoupení státních organizací, které je velice nízké a pohybuje se pouze na úrovni 8 %. Z finančních institucí pouze 5 % využívá cloud služeb. Vzhledem k tomu, že tyto instituce disponují poměrně značnými finančními rezervami, které jsou schopny investovat do infrastruktury, je tento podíl značně nízký. Důvody je možné přisuzovat robustnosti, případně poměrně efektivnímu fungování stávajících systémů a jistou neochotu měnit již zavedenou infrastrukturu.



Obrázek 12 - Procentuální zastoupení firem (zdroj: autor)

4.2 Typ cloudu v závislosti na typu organizace

Z uvedených odpovědí je žádoucí sledovat také závislost mezi nasazeným typem cloudu a typem organizace. Zajímavým výsledkem je, že jsou využívány pouze tři typy cloud řešení a to hybridní cloud, hostovaný privátní cloud a vlastní privátní cloud. Vlastní privátní cloud využívají organizace státní správy, pro které není z důvodů legislativních omezení jiné řešení více méně reálné, protože zde existuje velký důraz na vysokou míru zabezpečení dat uchovávaných v cloudu. Správa a zabezpečení dat organizace je stále nejvýznamnějším prvkem, ovlivňující nasazení cloud služeb, což je zjevné i z využívání hostovaného privátního cloudu a hybridního cloudu, protože obě tyto varianty dávají uživateli možnost uchovávat a chránit svá data dle požadavků daných zákonem o kybernetické bezpečnosti, zákonem o ochraně osobních údajů zaměstnanců i klientů a v neposlední řadě i interních materiálů firmy, jejichž používání musí být stanoveno interními normami organizací, jež jsou v souladu s normami ISO 27000.



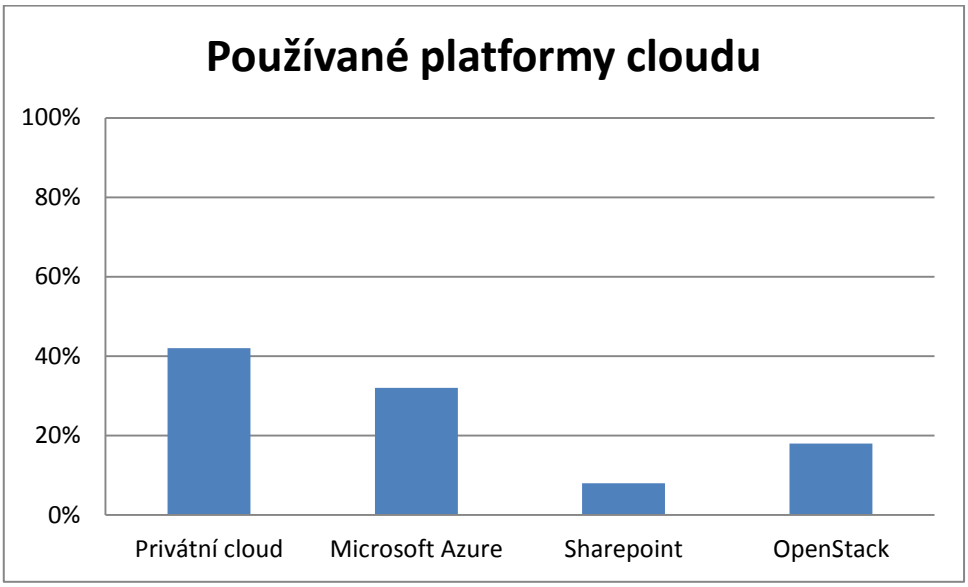
Obrázek 13 - Typ nasazeného cloud řešení dle typu organizace (zdroj: autor)

4.3 Poskytovatel cloudové platformy

Na výsledky v předchozí kapitole navazují následující výsledky zobrazené na následujícím obrázku. Jedná se o využívání platforem, které uživatelé cloud služeb používají. V rámci získaných odpovědí se objevili pouze čtyři využívané platformy. Více než 40 % organizací využívajících cloud služby je využívá ve formě privátního cloudu, jehož technologické řešení poskytuje celá řada distributorů a nepředstavuje z hlediska výzkumu zásadní informaci. Dále je z výsledků patrné, že v České republice je preferováno řešení mezinárodní korporace Microsoft ve formě jejího robustního řešení IaaS a PaaS Microsoft Azure, jež dovoluje využít všech charakteristik těchto modelů. Microsoft Azure podporuje

runtime operační systém Windows Azure a zákazník tak dostává komplexní balík cloud řešení s podporou všech nejpoužívanějších technologií jako je Live Services, SQL Azure, AppFabric, Dynamics CRM Services a SharePoint Services.

Sharepoint platforma byla navíc uvedena jako samostatná služba u 8 % respondentů, z čehož lze vyvodit závěr, že pro jejich potřeby cloud plní pouze formu aplikační platformy webové služby a poskytuje intranetový portál, nástroje pro správu dokumentů a souborů, sociální sítě, vnitropodnikové vyhledávání a nástroje pro analýzu firemních procesů. Nečekaný je i 18% podíl využívání cloud služeb postavených na platformě OpenStack, který je v České republice v největší míře implementován v Technologickém centru Písek.



Obrázek 14 - Používané platformy cloudu (zdroj: autor)

4.4 Distribuční model cloudu

V souvislosti se specifickými potřebami organizace je při přechodu na cloud služby důležité správně uvážit volbu distribučního modelu, který ji bude nejlépe vyhovovat. S tím úzce souvisí i výdaje se službami spojené. V rámci výzkumu byli respondenti dotazováni na otázku, která tuto volbu reflektovala. Zajímavé je, že všechny organizace státní správy používají model MaaS pro zajištění monitoringu aktivit uživatelů. Tento krok je zcela logický jak z pohledu efektivity práce, tak zpětné kontroly aktivit v případě auditu či jiných kontrolních opatření. V soukromé sféře není tato potřeba tak významná, pohybuje se v průměru 14 % a je patrné, že zatím se k ní nepřistupuje v takové míře jako ve státní správě.

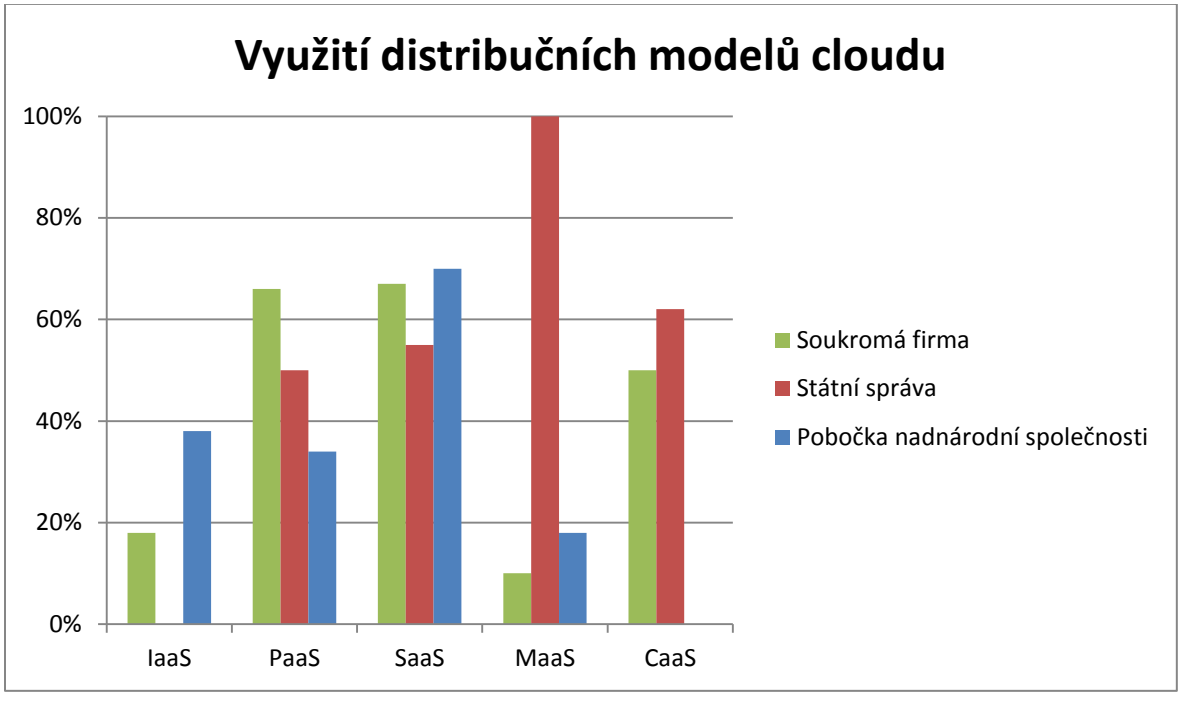
Další významný závěr lze vyvodit při pohledu na využívání aplikací v organizacích, které mohou být vyvíjeny buď na míru, což je záležitost nejen státní správy, ale v dnešní době prakticky každé organizace, tak i využití aplikací od poskytovatele cloud služeb. Z nich jsou dnes nejvíce využívány kancelářské aplikace. Rovných 70 % nadnárodních

společností využívá modelu SaaS, což si lze vysvětlovat zpracováním velkého množství dat a provádění analýz za pomoci těchto programů. U organizací státní správy a soukromých firem se čísla pohybují v průměru kolem 60 %, což je také poměrně vysoké zastoupení.

Téměř stejným podílem (66 %) je u soukromých firem zastoupen model PaaS. Souvislost může být vysvětlena procentuálním zastoupením 40 % firem věnujícím se vývoji HW, SW a ICT, kdy možnost pronajmout si nejen infrastrukturu, ale především i specifické nástroje pro vývoj aplikací, je zcela klíčovým faktorem. U poboček nadnárodních společností a státní správy není potřeba vyvíjet aplikace na míru tak častá, nicméně podíl jejich zastoupení se pohybuje na 34 %, resp. 50 %.

V některých případech je nežádoucím jevem určitá ztráta kontroly, kdy operační systém a aplikace jsou plně v režii poskytovatele. To se odrazilo také v odpovědích respondentů, kdy 38 % poboček nadnárodních společností a 18 % soukromých firem využívá pronajímání infrastruktury (IaaS) a má tak všechny aplikace a operační systém ve své režii.

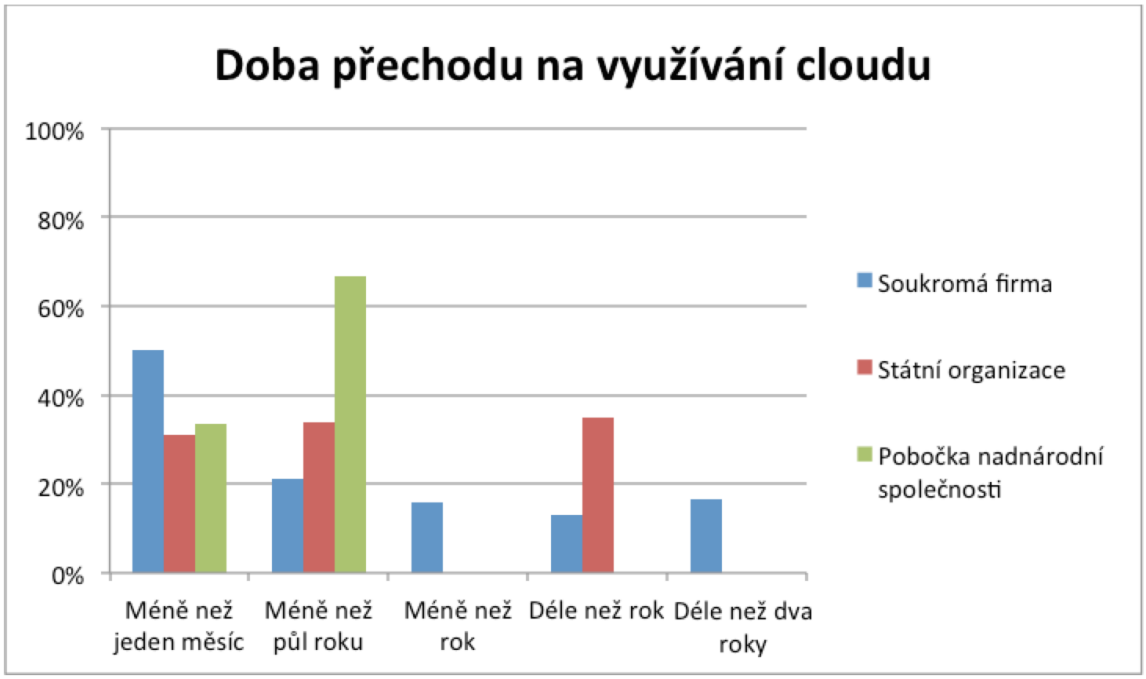
Taktéž bez zajištění komunikace by v dnešní době státní správa nemohla fungovat a 62 % státní správy tedy využívá specifický model cloudu CaaS, který zahrnuje zajištění komunikačních služeb prostřednictvím serverů elektronické pošty, VOIP komunikace, atd. Zajímavý výsledek představuje 50% zastoupení soukromých firem, které CaaS také využívají a dochází tím k dalším úsporám na infrastrukturu a lidské zdroje.



Obrázek 15 - Používaný distribuční model v závislosti na typu organizace (zdroj: autor)

4.5 Doba potřebná pro přechod na cloud služby

Mezi klíčové faktory ovlivňující volbu nasazení nové technologie do stávající infrastruktury patří pro mnoho firem a organizací bezesporu doba její implementace. Každý podnik a organizace má své specifické potřeby a proto je důležité neopomenout dobu na testování a individualizaci dané služby pro potřeby organizace. Ve výzkumu byli tedy respondenti dotazováni na dobu úplné integrace vybraných cloud služeb do organizace. Nejkratší doby implementace dosáhly podle očekávání firmy, jež jsou pobočkou nadnárodní společnosti. Tento výsledek může mít několik příčin ovlivňujících takto krátké doby implementace. Především široké zázemí IT specialistů, zkušenosti zahraničních partnerů a vysoká efektivita práce. Za pozitivní lze považovat výsledek, kdy více než 60 % státních organizací, jež implementovali cloud služby, se tato významná změnu podařila dokončit do šesti měsíců. Na druhou stranu však nelze opomenout fakt, že více než 30 % státních organizací tato změna trvala více než rok. Doby implementací u soukromých firem splnily předpoklady, že jejich implementace je výrazně ovlivněna druhem vybrané cloud služby a především velikostí organizace a rozdílnými zkušenostmi a dostupností IT specialistů.

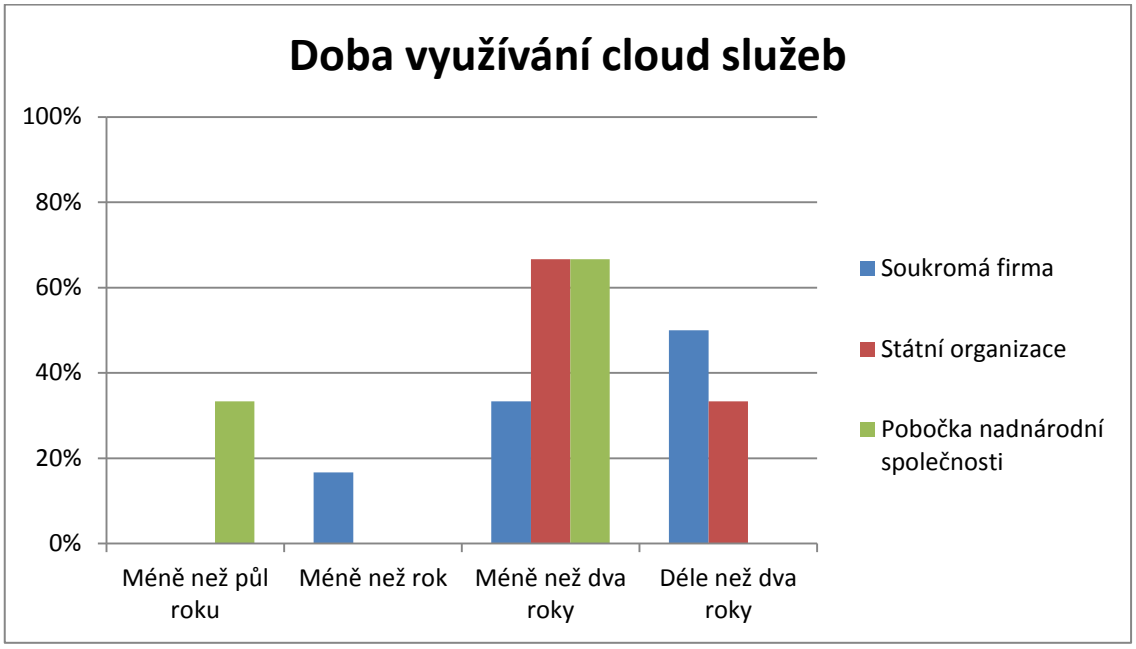


Obrázek 16 - Doba přechodu na využívání cloud služeb (zdroj: autor)

4.6 Doba využívání cloud služeb

V souvislosti s výsledky v předchozí kapitole byli respondenti dotazováni taktéž na dobu, po kterou cloud služby již využívají. Z výsledků se ukazuje, že pobočkám nadnárodních společností trvá doba přechodu na cloud služby nejkratší dobu a přesto více jak 60 % z nich je využívá méně než dva roky. Velice překvapivé a pozitivní se ukázalo využívání cloud služeb státními organizacemi, kdy u 30 % z nich se doba využívání pohybuje od hranice dvou let a výše. Nelze ovšem přehlédnout ani fakt, že u zbylých 70 % se tato doba

pohybuje od jednoho do dvou let. U soukromých firem není procentuální poměr tak jasný, jako v předchozím případě. Hlavní příčinou může být opět velikost organizace, obavy z použití nové technologie a v případě využití privátního cloudu také finanční prostředky. I přesto 85 % soukromých firem využívá cloud služby déle než rok. Z toho 50 % déle než dva roky. Ačkoli je cloud computing relativně nová technologie, je zřejmé, že si našla své místo bez rozdílu zaměření a oblasti působnosti firem a organizací.

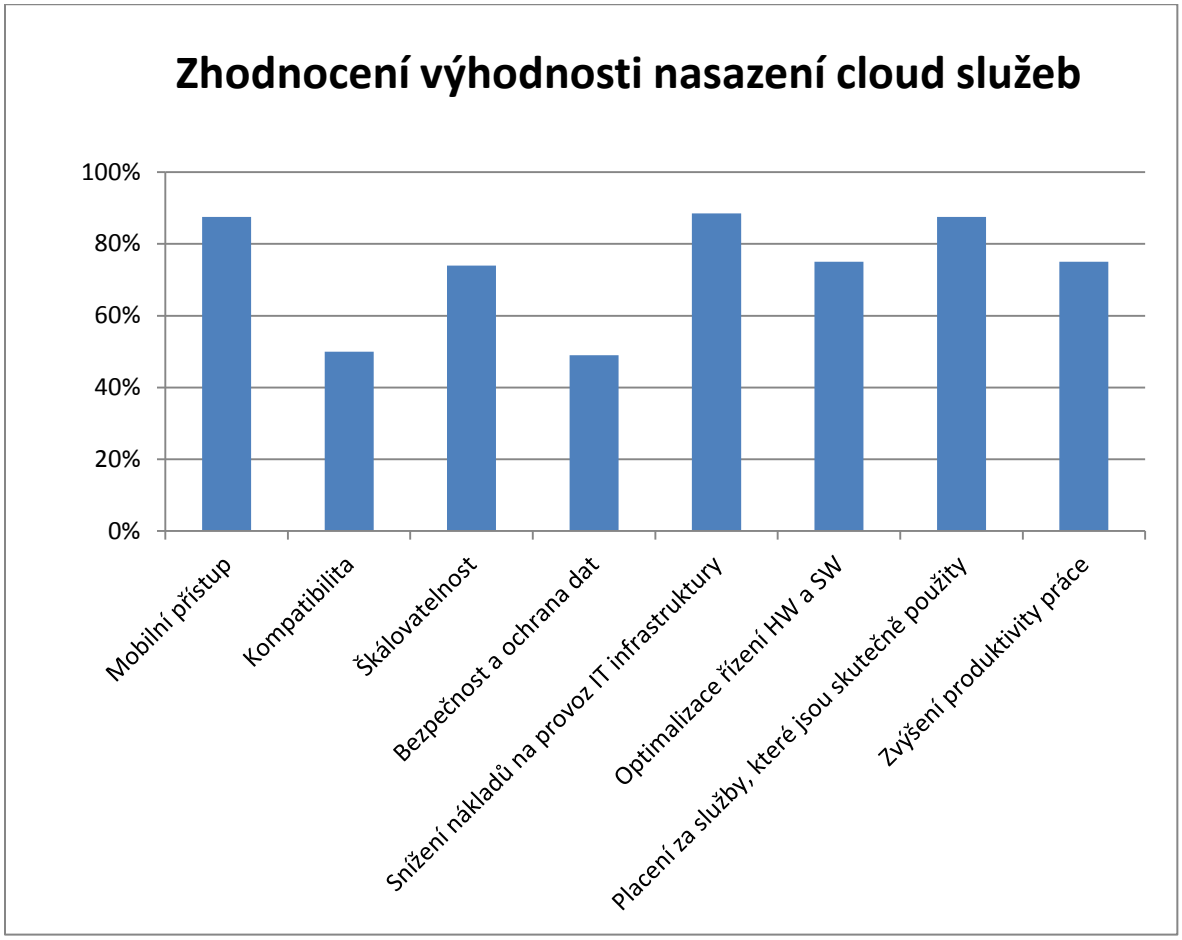


Obrázek 17 - Doba využívání cloud služeb (zdroj: autor)

4.7 Hodnocení výhodnosti nasazení cloud služeb

Při volbě organizace implementovat cloud služby do své infrastruktury je nezbytné si uvědomit pozitiva i negativa, která s sebou tato technologie přináší. Uvědomění si těchto důvodů pak sehrává významnou roli při rozhodování tohoto významného kroku. Logickým krokem tedy bylo dotazování se organizací, jež se pro implementaci cloud služeb rozhodli a provedli ji, na důvody, které byly reflektovány při této volbě. Dotazy byly rozděleny na dvě oblasti. První z nich byla orientována na technické benefity a druhá na přínosy z pohledu managementu a businessu organizace. Ze získaných výsledků je zajímavé, že technické výhody nasazení cloud služeb jako je zvýšení možnosti mobilního přístupu, kompatibility, škálovatelnosti, bezpečnosti a ochrany dat ovlivnila organizace v průměru pouze z 65 %. Oproti tomu manažersko-ekonomické přínosy, mezi které lze zařadit zvýšení produktivity práce, snížení nákladů na infrastrukturu, optimalizaci správy HW a SW a placení za služby, které jsou skutečně využívány, byly jednotlivými organizacemi zohledněny v 80 % případů. Tato data představují významný závěr, že implementace cloud služeb není výhodná jen z pohledu technického, ale především si organizace implementující cloud služby slibují významné ekonomické přínosy. Ať již na úrovni optimalizace nákladů na HW and SW, ale také v oblasti efektivnosti a produktivity práce. Nutno zmínit fakt, že pouze u 17 % společností došlo ke snížení počtu zaměstnanců

v IT oddělení a firmy se tedy spíše přiklánějí k možnosti úspoře nákladů prostřednictvím infrastruktury než lidských zdrojů.



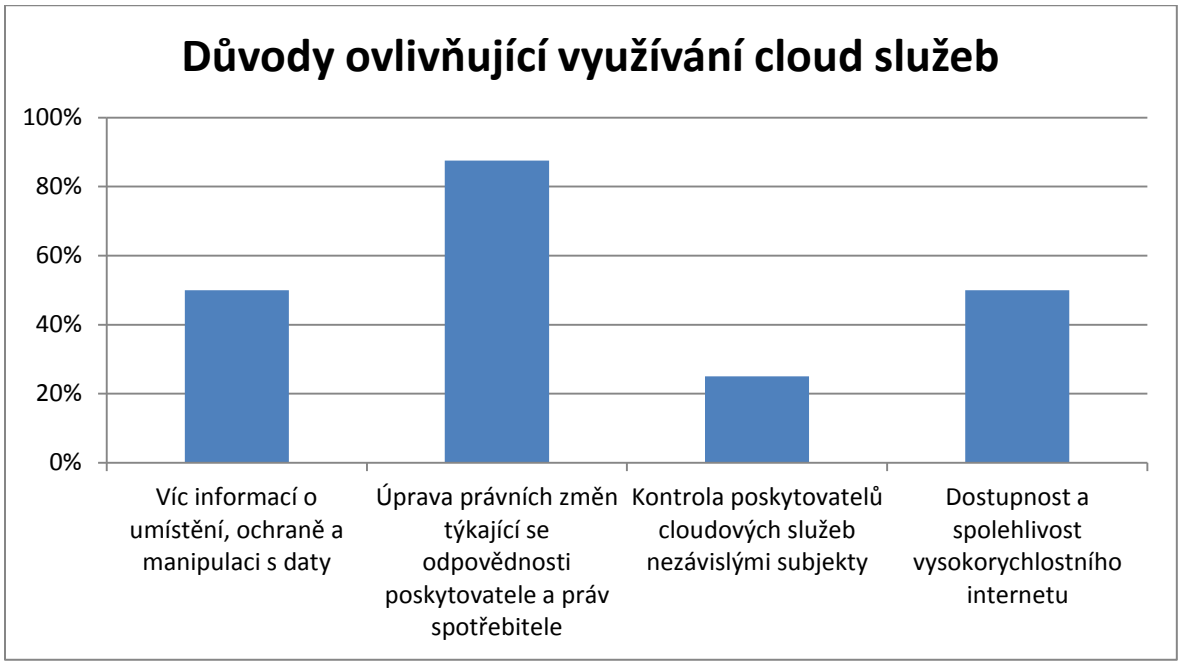
Obrázek 18 - Výhodnost nasazení cloud služeb (zdroj: autor)

4.8 Důvody ovlivňující využívání cloud sloužeb

Předposledními výsledky, které budou představeny, jsou důvody ovlivňující organizace, jež ještě cloud služby nemají implementovány a považují je za nezbytné pro jejich implementaci. Za málo významný aspekt se ze získaných výsledků jeví nezávislá kontrola poskytovatelů cloud služeb externími nezávislými subjekty. Toto hledisko, týkající se logicky pouze veřejných a hybridních cloud služeb, je rozhodující jen pro necelých 25 % subjektů. Dalším aspektem, jež lze považovat za značně omezující pro neimplementaci cloud služeb je nedostupnost rychlé konektivity pro koncové zákazníky. Její zvýšení je klíčovým prvkem pro implementaci cloud služeb u více než 49 % organizací. Tento výsledek je významný zejména pro korporátní organizace poskytující jak konektivitu, tak i cloud služby, jichž je v prostředí České republiky nepřeberné množství a měli by jej reflektovat při nabídkách svých služeb koncovým klientům. Pro 50 % organizací je důležitý nedostatek poskytovaných informací o umístění, ochraně a manipulaci s daty umístěných v cloudu. Tento výsledek zcela koresponduje s interpretací předchozích částí výzkumu, kde se organizace přiklánějí k implementaci privátního nebo

hybridního cloud řešení, právě z důvodů zabezpečení a kontroly nad daty. Nejvýznamnějším aspektem z pohledu respondentů je pak nedostatečný či komplikovaný legislativní rámec definující vztahy mezi provozovatelem a klientem cloudu a zabývající se právní zodpovědností v případě výpadku, zneužití či ztrátě dat umístěných v cloudu.

V porovnání s výzkumem, který v roce 2008 provedli Feuerlicht, Burkoň a Šebesta, vzrostl podíl organizací využívající cloud computing z původních 4 % na 35 %. Tento nárůst zcela koresponduje s tím, že technologie cloud computingu má budoucnost a procento zastoupení v České republice se bude nadále zvyšovat. Dále je možné pozorovat i postoj v přístupu respondentů k benefitům, které cloud coumputing poskytuje. Ve srovnání s výzkumem Feuerlichta, Burkoně a Šebesty, kde manažersko-ekonomické přínosy byly zastoupeny ve 26 % odpovědí, zatímco technické benefity pouze ve 20 %. V provedeném výzkumu se tento podíl zvýšil na 80 %, resp. 65 %. Důvodem je především vzrůstající povědomí o cloud computingu a možnostech jeho využití. Dalším zajímavým srovnáním jsou vzrůstající obavy o bezpečnost dat. Zatímco v průzkumu Feuerlichta, Burkoně a Šebesty byla tato volba reflektována ze 14 %, nyní se pohybuje na úrovni 50 %. Částečné řešení lze najít v úpravě legislativního rámce, který by jasně definoval odpovědnost poskytovatele a práva spotřebitele. To byl také nejvýznamnější aspekt, který respondenti reflektovali v 88 % svých odpovědí.



Obrázek 19 - Důvody ovlivňující využívání cloud služeb (zdroj: autor)

4.8.1 Bezpečnostní rizika

Ve vývoji rizik, ovlivňujících potenciální zákazníky při přechodu na cloud služby, nenastaly žádné výrazné změny, což plyne ze srovnání výsledků z provedeného šetření s riziky definovanými Gartnerem v roce 2008 a Winklerem v roce 2011 (kapitola 2.9.11). Gartner poukazuje především na velké riziko spočívající v ochraně dat, což respondenti reflektovali v 50 % odpovědí. V souladu s předchozím zjištěním komplikovaného

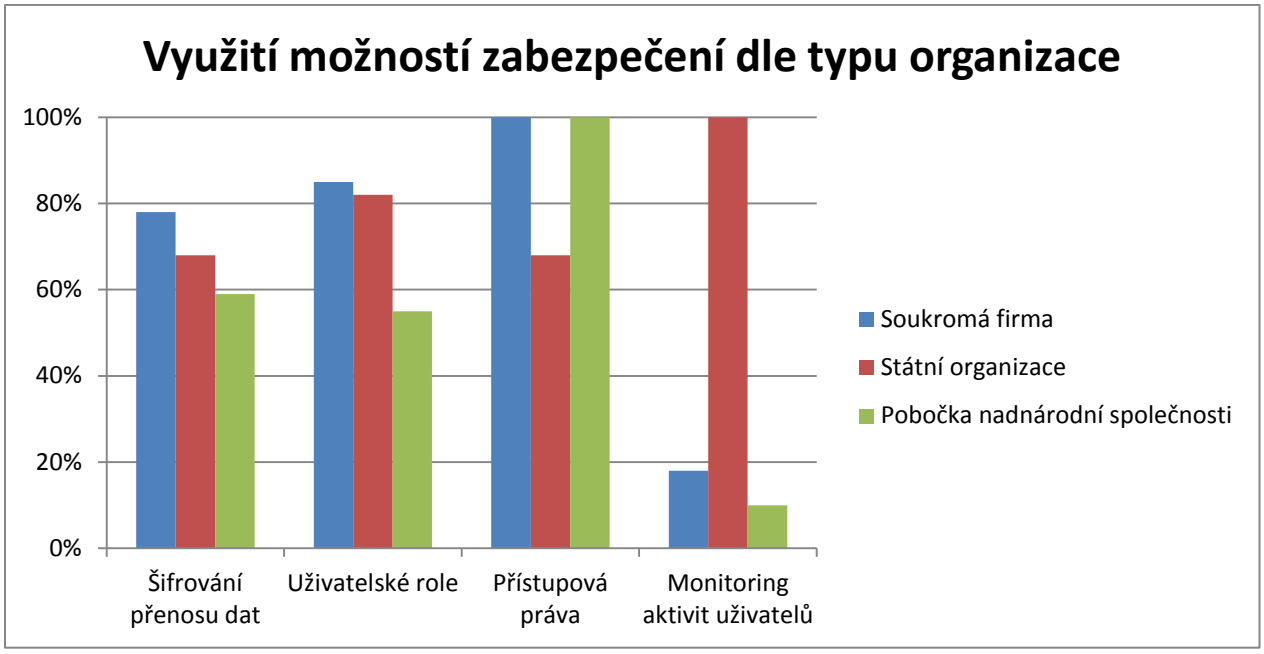
legislativního rámce týkajícího se právní odpovědnosti poskytovatele a klienta lze rovněž najít shodu s Gartnerem, který legislativní překážky pokládá také za významné riziko.

4.9 Typ využívaného zabezpečení dle typu organizace

Poslední představené výsledky souvisí s používanými možnostmi zabezpečení při využívání cloud služeb. Problematika bezpečnosti cloudu je velice rozsáhlá a měla by být brána na zřetel všemi, kdo cloud využívají, jak dokládá kapitola 2.9. Různorodost ve výběru možností zabezpečení dává možnost každé organizaci vybrat si volbu, která odpovídá jejím potřebám. Z tohoto důvodu bylo logické a žádoucí v rámci výzkumu zmapovat situaci, jaké možnosti a v jaké míře jsou v České republice nejvíce využívány. Zabezpečení se dle očekávání nejvíce využívá ve sféře státních organizací, v průměru z 80 %. Ovšem soukromé firmy a pobočky nadnárodních společností nezaostávají za tímto číslem nijak výrazně, pohybují se průměrně na 62 %. Již několikrát zmíněným faktorem je ochrana dat. Zejména během přenosu do cloudu je nežádoucí situací odposlech dat a jejich případné zneužití. Jednoduchým a účinným řešením je zabezpečení šifrovaného přenosu dat například za využití šifrovacích klíčů. Jak plyne z výsledků průzkumu, organizace berou problém vážně a průměrně 67 % jich využívá této možnosti zabezpečení.

Vhodnou volbou je řešení Virtula Private Data (VPD), resp. Virtual Key Management společnosti Porticor, která se zabývá šifrováním a správou šifrovacích klíčů. Jedná se o software, který je rovněž hostován v cloudu a je integrován do cloudové infrastruktury. Využívá se inovativní přístup k využívání tzv. rozděleného klíče, kde veškerá kontrola nad šifrovacími klíči je v režii zákazníka. Klíč je rozdělen tak, že jedna část je v držení společnosti Porticor a druhá část (hlavní klíč) je v držení zákazníka. Ani jedna strana nemůže dešifrovat data, pokud nemá k dispozici obě části klíče. Druhým stupněm ochrany je zašifrování klíčů pomocí hlavního klíče zákazníka. Toto řešení je zajímavé také z pohledu možnosti jeho využívání na více úrovních. Nemusí být tedy šifrováno například celé uložiště souborů, ale pouze ta data, u kterých je šifrování žádoucí. Významnost používání tohoto přístupu si uvědomila společnost HP, když si Porticor zvolila za partnera při realizaci svého bezpečnostního cloudového řešení Atalla a jeho technologii začlenila do poskytovaných služeb.

Dalším poměrně zajímavým, ale nepřekvapivým výsledkem je fakt, že všechny organizace státní správy využívají možnosti monitorování aktivit uživatelů. Tento výsledek je zcela logickým krokem z důvodu manipulace s citlivými daty a může případně sloužit i jako závazný podklad v případě provádění auditů. S monitorováním uživatelů logicky souvisí potřeba rozlišit, o kterého uživatele se jedná. K tomu slouží využití uživatelských účtů a především rolí, kdy každé roli přísluší přístupová práva. Každý uživatel může provádět pouze operace příslušící jeho uživatelské roli. Tuto možnost reflektovalo 92 % soukromých firem a stejným podílem 75 % státní organizace a pobočky nadnárodních společností, z čehož lze učinit významný závěr, že nejen státní, ale i soukromé firmy či organizace nepodceňují ochranu svých dat nejen z hlediska jejich přenosu do cloudu ale také následným sledováním kdo a jakým způsobem s nimi nakládá.



Obrázek 20 - Zabezpečení dle typu organizace (zdroj: autor)

5 Návrh nasazení cloud computingu v energetice

Cílem této kapitoly je provedení návrhu nasazení cloud computingu. Bude demonstrováno efektivní využití cloud computingu popsaného v teoretické části práce, společně s výsledky výzkumu, který je součástí praktické části práce. V první podkapitole je vybrán podnik či organizace, případně oblast jeho činnosti, který se rozhodl začít využívat cloud computing. Dále výběr vhodného typu cloudu a poskytovatele cloudové platformy. Druhá podkapitola se věnuje konkrétním oblastem vybraného subjektu, kde cloud computing nalezne využití. Její součástí bude také zhodnocení situací, ve kterých není uplatnění této technologie vhodné.

5.1 Představení návrhu

Součástí kapitoly 4.1 je procentuální zastoupení oblastí činnosti podniků a organizací, které se podílely na provedeném výzkumu. Vzhledem k vysokému podílu (33 %) podniků působících v oblasti energetiky, z nichž 75 % zaměstnává více než 1000 zaměstnanců a výzkumnému zaměření vedoucího práce byla tato oblast zvolena jako vhodný subjekt výzkumu pro případovou studii. Praktické využití je tedy popsáno na velké fiktivní energetické společnosti, s více než 1000 zaměstnanci, která se rozhodne využívat cloudové služby. Předpokladem takto velké společnosti je existence poboček po celé České republice.

Pokud se takto velká energetická společnost rozhodně implementovat využívání cloud služeb, za nejvhodnější lze doporučit implementaci privátního cloudu. Především z hlediska bezpečnosti, jak bylo uvedeno v teoretické části práce. Situace kdy by například data o počtu vyrobených megawattů elektřiny, či konkrétní spotřebě u zákazníků, byla umístěna ve veřejném cloudu a došlo by k jejich zneužití, mohlo by se jednat o poskytnutí velké výhody pro konkurenci a společnost by tím byla značně poškozena především po finanční stránce. Z výsledků výzkumu je jasně patrné, že všechny energetické společnosti, které se výzkumu účastnily, jsou si bezpečnostních rizik dobře vědomy a využívají pouze privátní cloud.

Hlavní přínos vyžívání cloudu v energetice lze najít především v centralizaci dat a přístupu k nim. Nelze opomenout také možnost jejich pravidelného zálohování. Správně zvolený typ cloudu ovšem nepokryje všechna bezpečnostní rizika, která jsou způsobena lidským faktorem a to jak úmyslně, či neúmyslně. Je doporučeno využívat přídavné mechanismy pro zamezení ztráty či zneužití dat. Mezi ně patří uživatelské role, přístupová práva a monitoring aktivit uživatelů. Ty umožní, na základě autentizace a autorizace uživatelů, snížit rizika odcizení, případně manipulace s daty. Přístup energetických firem v České republice je v tomto směru na dobré úrovni, kdy průměrně 75 % z nich tyto mechanismy využívá. Společnost je rovněž využívá.

5.2 Oblast činnosti subjektu

Oblast činnosti energetické firmy lze rozdělit do několika oblastí od výroby elektrické energie, dále distribuci, měření spotřeby a v neposlední řadě management. Ty jsou součástí následujících podkapitol.

5.2.1 Výroba

První oblastí, kde lze najít potenciál při využívání cloudu je při výrobě elektřiny. Na základě nejen historických dat, ale především online dat o spotřebě elektřiny, umístěných v cloudu, má společnost možnost pružně reagovat na poptávku po elektrické energii a tím zvýšit efektivitu výroby a s tím souvisejících vyšších výnosů z prodeje.

5.2.2 Distribuce

S výrobou je úzce spjata rovněž distribuce elektřiny k zákazníkům a to nejen v rámci České republiky, ale také do zahraničí, kdy se jedná o výpomoc mezi provozovatelem přenosové soustavy a zahraničním poskytovatelem elektřiny. Přenosové soustavy jsou propojeny synchronně což znamená, že je možný přenos energie z jedné soustavy do druhé bez příslušných úprav (změny napětí, atd.). Možnost nákupu a prodeje elektřiny je využívána především v případě výskytu mimořádné situace (přetížení mezistátních přenosových cest, nedostatku a přebytku energie v elektrizační soustavě, atd.). Online data umístěná v cloudu nachází využití jako vstupy pro algoritmy, které zajišťují rozhodovací procesy pro cesty elektřiny. V případě jejího přebytku může být prodána mimo území České republiky, což pro společnost znamená nárůst finančních zisků.

Zde lze najít další klíčový faktor pro nasazení cloudu. Systém zajišťující obchodování s elektrickou energií je pro energetickou firmu klíčový a je třeba maximalizovat jeho dostupnost. Odstavení systému i na jeden den, za účelem instalace novějších verzí aplikací, by stálo velké finanční prostředky. V nejhorším případě by se systém znovu ani zapojovat nemusel, protože v době odstávky by společnost mohla být nahrazena jiným dodavatelem. Servery, na kterých jsou provozovány takové aplikace, vyžadují škálovatelnost a instalaci updatů aplikací a operačního systému za provozu. Cloud tyto problémy eliminuje. Za použití cloudu je možné instalovat novou verzi aplikace na nový virtuální počítač a následně po jejím otestování přepnout data ze starého na nový virtuální počítač. Časová prodleva výpadku se zkrátí z několika hodin na sekundy.

5.2.3 Měření

Aby bylo možné realizovat optimalizaci výroby a distribuce, je třeba mít relevantní podkladová data. Společnost využívá novou koncepci měření elektrické energie, která se rozvíjí v posledních letech – smart metering. Jedná se o technologii, která má základ v obousměrné komunikaci mezi centrálou a měřícím přístrojem, kdy měřící přístroj odesílá data na koncentrátor. Jedná se o inteligentní zařízení, na které se připojují odečtová zařízení. Buď s pomocí odesílání dat po elektrické síti nebo na rádiové frekvenci. Koncentrátor dále odesílá data do datové centrály prostřednictvím protokolu GPRS. GPRS nabízí možnost šifrování dat a to opět především proto, aby nemohla být data při přenosu do centrály odposlechnuta či pozměněna. Mnoho dnešních výrobců odečtových zařízení

podporuje ve svých přístrojích šifrování AES 128/256, SSL. V souladu s teoretickou částí práce, kde byly popsány bezpečnostní problémy týkající se přenosu dat a výsledků výzkumu, kdy šifrování přenosu dat využívají energetické společnosti pouze z 50 %, plyne jasné doporučení využívat všechny dostupné možnosti šifrování.

Datová centrála společnosti bude umístěna v cloudu. Na základě vyhodnocení online dat, které centrála shromažďuje, se rozšiřuje možnost dynamicky optimalizovat datové tarify a přizpůsobovat nabídku produktů koncovým zákazníkům.

5.2.4 Management

Data v cloudu mají využití také pro management společnosti. Na jejich základě lze sestavovat různé výstupy. Jedná se například o ekonomické pohledy nebo analýzy množství prodané a vyrobené elektřiny.

Důležitou součástí podniku je komunikace. Nejedná se však pouze o vnitrofiremní komunikaci, ale je třeba zahrnout i subdodavatele spolupracující s podnikem, obchodní partnery a v neposlední řadě i koncové zákazníky. Velkým přínosem v používání cloudu je možnost sdílení podnikových dokumentů. Množství informací, které musí být dostupné napříč celým podnikem, je velmi vysoké a ukládání do cloudu je z hlediska centralizace přístupu vhodnou variantou, což podnik reflektuje při rozhodnutí využívat cloud computingu.

5.2.5 Rizika nasazení

Ne ve všech oblastech energetiky je ale nasazení cloud computingu žádoucí. Zejména při výrobě elektřiny. Konkrétním případem může být řízení jaderné elektrárny, kterou společnost provozuje a kde je z bezpečnostního hlediska nutné, aby data z měřících přístrojů byla dostupná v reálném čase a obsluha byla fyzicky přítomna v elektrárně a mohla na případné problémy reagovat ihned. Situace kdy by elektrárna byla řízena z centrálního místa a data z měřících přístrojů byla přenášena a ukládána do cloudu, nacházejícího se mimo elektrárnu, je nežádoucí. Nelze se spolehnout na stabilitu a rychlost internetového připojení, která je kritická pro přístup ke cloudu. V případě výpadku připojení a vzniku problému v elektrárně by obsluha neměla k dispozici relevantní data a nemohla tak reagovat na vzniklou situaci. To by mohlo mít v krajním případě kritické následky.

Závěr

Diplomová práce byla z důvodu přehlednosti rozdělena na dva logické celky. Cílem teoretické části bylo, s využitím literárních zdrojů, představit problematiku cloud computingu. Na základě těchto znalostí byla provedena SWOT analýza z pohledu typu cloudu a typu poskytovaných služeb.

Náplní teoretické části bylo prostudování materiálů, kterých je v zahraničí velké množství. Do českého jazyka bylo přeloženo také několik knih týkajících se cloud computingu, což umožňuje seznámení s touto technologií i lidem, kteří nemají dostatečnou znalost anglického jazyka nebo se nepohybují v oboru IT.

V úvodní kapitole je čtenář seznámen s technologií cloud computingu. Je zřejmé, že pojem cloud computing je vykládán pokaždé částečně odlišně. Za relevantní byla zvolena definice Národního Institutu Standardů a Technologií. Jedná se o poskytování škálovatelných výpočetních zdrojů za poplatek. Důležité je si uvědomit, že se nejedná o novou technologii. Její myšlenka byla nastíněna již v 60. letech 20. století. Tehdejší technologická úroveň ale neumožnila její nasazení.

Primárním cílem práce nebylo poukazovat na bezpečnostní rizika cloud computingu. Ovšem jako každá technologie, i tato s sebou určitá rizika přináší a v rámci výzkumu bylo žádoucí sledovat cloud computing i z pohledu bezpečnosti. V další části práce byla zdůrazněna bezpečnostní rizika definovaná společností Cloud Security Alliance, která podporuje osvědčené bezpečnostní postupy v rámci cloud computingu. Za uznávanou společnost věnující se problematice bezpečnosti cloudu je rovněž považována společnost Gartner a v literatuře hojně citovaný autor J. R. Winkler. Součástí kapitoly o bezpečnosti je tedy i jejich vnímání rizik, která s cloud computingem souvisí.

Pro praktickou část práce byla zvolena metoda sběru dat prostřednictvím dotazníkového šetření, které probíhalo od února do listopadu roku 2014. Součástí dotazníkového šetření bylo rovněž osobní setkání s osobami, které byly ve firmě za danou problematiku zodpovědné. V rámci pohovoru s nimi byla problematika cloud computingu diskutována za účelem získání objektivních odpovědí. Vybrané otázky byly sekundárně ověřeny z odpovědí získaných při počátečním rozhovoru.

Z provedeného výzkumu je zřejmé, že cloud computing jak z pohledu organizací, a to nejen potenciálních, ale i těch, kteří ho již využívají, přináší celou řadu výhod a příležitostí. Závěrem lze shrnout výsledky provedené SWOT analýzy, jež korespondují s komplexními výsledky provedeného výzkumu. Silnou stránkou je především snížení nákladů na nákup a provoz infrastruktury. Zákazník se nemusí starat o nákup serverů a budování síťové infrastruktury. Za slabé stránky lze považovat dostupnost. Pokud chce mít zákazník přístup k datům, měla by mu být poskytnuta v přijatelném čase. Stejně tak stálé internetové připojení může být velkou nevýhodou, jak mimo jiné ukazuje i analýza výsledků výzkumu.

Při implementaci cloud služeb lze identifikovat i příležitosti, a to ve formě finančních prostředků, které může organizace investovat do modernizace výrobních technologií a tím zvýšit své tržby a konkurenceschopnost. Další příležitostí je tlak na sjednocení a úpravu legislativy, která by přispěla k většímu využívání cloudu, což potvrzují i výsledky výzkumu. Na závěr je nutné zmínit i možné hrozby, mezi které se řadí bezpečnost dat a především riziko jejich zneužití třetí stranou. S tím souvisí i případné ukončení činnosti poskytovatele, kdy je zákazník vystaven riziku ztráty dat, na což respondenti poukazovali ve svých odpovědích.

Na závěr lze říci, že implementace cloud služeb v prostředí České republiky je na průměrné úrovni, ale jako pozitivní lze konstatovat, že si organizace, jež cloud využívají, uvědomují jeho možnosti, kladné stránky a poukazují na možná rizika a hrozby s ním spojené. Větší podpora využívání cloud služeb ze strany legislativy a korporací jež tyto služby poskytují by vedla i ke zvýšení kvality datových spojení a jejich využití.

Literatura

About Gartner, 2014. Gartner, Inc. *Gartner* [online]. [cit. 2014-08-28]. Dostupné z: http://www.gartner.com/technology/about.jsp

ANGELES, Sara, 2014. The Pros and Cons of Virtualization. *Business news Daily* [online]. 3. března 2014 [cit. 2014-07-30]. Dostupné z: http://www.businessnewsdaily.com/6014-pros-cons-virtualization.html

ARMBRUST, M. et al., 2009. *Above the Clouds: A Berkeley View of Cloud Computing.* Berkely: University of California.

BBC NEWS, 2014. Sony PlayStation Network and other game services attacked. *BBC News* [online]. 25. srpna 2014 [cit. 2014-09-23]. Dostupné z: http://www.bbc.com/news/technology-28925052.

BRODKIN, Jon, 2008. InfoWorld. *Infoworld, Inc.* [online]. 2. června 2008 [cit. 2014-08-28]. Dostupné z: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0

BROGAN, David B, 2014. Cloud Computing and Security. [online]. [cit. 2015-01-27]. Dostupné z: http://csis.pace.edu/~ctappert/srd2014/c6.pdf

CHANTRY, Darryl, 2009. Mapping Applications to the Cloud. *MSDN* [online]. Microsoft Corporation, Leden 2009 [cit. 2014-07-30]. Dostupné z: http://msdn.microsoft.com/en-us/library/dd430340.aspx

CERT, 2014. About Us. CARNEGIE MELLON UNIVERSITY. *The CERT Division* [online]. [cit. 2014-09-23]. Dostupné z: http://www.cert.org/about/

Cloud security alliance, 2013. Cloud Computing Top Threats in 2013: The Notorious Nine. Cloud security alliance [online]. [cit. 2014-09-23]. Dostupné z: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

ČMELÍK, Martin, 2013. Seznamte se – DoS a DDoS útoky. *Security portal* [online]. 7. března 2013 [cit. 2014-09-23]. Dostupné z: http://www.security-portal.cz/clanky/seznamte-se-–-dos-ddos-útoky

DANEL, Roman, 2011. Historické etapy ve vývoji informačních systémů. *VŠB - Technická univerzita Ostrava* [online]. [cit. 2014-08-25]. Dostupné z: http://homel.vsb.cz/~dan11/is_skripta/IS%202011%20-%20Historicke%20etapy%20ve%20vyvoji%20informacnich%20systemu.pdf

EUROPEAN COMMISSION, 2012. Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century. *European Commission* [online]. Brusel, 25. ledna 2012 [cit. 2014-09-23]. Dostupné z: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf

ETHERINGTON, Darrell, 2014. PlayStation Network Suffers DDOS Attack, Hackers Claim To Have Grounded SOE President's Plane. *TechCrunch* [online]. 24. srpna 2014 [cit. 2014-09-23]. Dostupné z: http://techcrunch.com/2014/08/24/playstation-network-suffers-ddos-attack-hackers-claim-to-have-grounded-soe-presidents-plane/

FEUERLICHT, George, Lukáš BURKOŇ a Michal ŠEBESTA, 2011. Cloud Computing Adoption: What are the Issues?. *Systems Integration (Systemova Integrace)* [online]. Červen 2011, roč. 18, č. 2, s. 187-192 [cit. 2014-08-14]. Dostupné z: http://cloud-computing.vse.cz/uploads/IGA_2010_summary.pdf

FURHT, Borivoje a Armando ESCALANTE, 2010. *Handbook of cloud computing*. New York: Springer, xix, 634 p. ISBN 978-1-4419-6523-3.

GÁLA, Libor, Jan POUR a Prokop TOMAN, 2006. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky. 1. vyd. Praha: Grada, 482 s. ISBN 80-247-1278-4

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ, 2009. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky. 2., přeprac. a aktualiz. vyd. Praha: Grada, 496 s. Expert (Grada). ISBN 978-80-247-2615-1.

Gartner Hype Cycle, 2014. *Gartner* [online]. [cit. 2014-10-06]. Dostupné z: http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp

Gartner's 2013 Hype Cycle for Emerging Technologies Maps Out Evolving Relationship Between Humans and Machines, 2013. *Gartner* [online]. 19. srpna 2013 [cit. 2014-10-06]. Dostupné z: http://www.gartner.com/newsroom/id/2575515

GHAFFARI, Kimia, Mohammad Soltani DELGOSHA a Neda ABDOLVAND, 2014. Towards Cloud Computing: A Swot Analysis on its Adoption in Smes. *International Journal of Information Technology Convergence and Services* [online]. 30. dubna 2014, roč. 4, č. 2, s. 13-20 [cit. 2014-09-10]. DOI: 10.5121/ijitcs.2014.4202. Dostupné z: http://www.airccse.org/journal/ijitcs/papers/4214ijitcs02.pdf

HALPERT, Ben, 2011. *Auditing cloud computing: a security and privacy guide*. Hoboken, N.J.: John Wiley, xvi, 206 p. ISBN 978-047-0874-745.

HAVLÍK, Petr, 2010. Virtualizace – bezpečná cesta k úsporám. *Setkáni uživatelů technologií IBM 2010* [online]. 13. května 2010 [cit. 2014-08-10]. Dostupné z: http://www-05.ibm.com/cz/events/setkani2010/pdf/Virtualizace_-_bezpecna_cesta_k_usporam.pdf

HONAN, Mat, 2012. How Apple and Amazon Security Flaws Led to My Epic Hacking. *WIRED* [online]. 8. června 2012 [cit. 2014-09-23]. Dostupné z: http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/all/

HOQUE, N., Monowar H. BHUYAN, R.C. BAISHYA, D.K. BHATTACHARYYA a J.K. KALITA, 2014. Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications* [online]. duben 2014, roč. 40, s. 307-324 [cit. 2014-09-23]. DOI: 10.1016/j.jnca.2013.08.001. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1084804513001756

HLAVÁČEK, Tomáš, 2013. DoS a DDoS útoky na vzestupu cílených útoků. *CD-R server* [online]. 12. prosince 2013 [cit. 2014-09-23]. Dostupné z: http://diit.cz/blog/dos-a-ddos-utoky-na-vzestupu-cilenych-utoku

HRONEK, Jiří, 2007. Informační systémy. *Univerzita Palackého* [online].[cit. 2014-08-25]. Dostupné z: http://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf

HURWITZ, Judith, Robin BLOOR, Marcia KAUFMANN a Fern HALPERT, 2013. How to Use a Hypervisor in Cloud Computing Virtualization. *How to Use a Hypervisor in Cloud Computing Virtualization - For Dummies* [online]. [cit. 2014-07-30]. Dostupné z: http://www.dummies.com/how-to/content/how-to-use-a-hypervisor-in-cloud-computing-virtual.html

JANNSEN, Cory, 2014. Hypervisor. *Technopedia* [online]. [cit. 2014-07-30]. Dostupné z: http://www.techopedia.com/definition/4790/hypervisor

KLIMEŠ, Cyril. Informační systémy, 2006. *Ostravská univerzita v Ostravě* [online]. [cit. 2014-08-25]. Dostupné z: http://www1.osu.cz/~prochazka/rpri/skripta.pdf

LEMOUDDEN, M., N. Ben BOUAZZA a B. El OUAHIDI, 2014. Towards achieving discernment and correlation in cloud logging. In: *Applications of Information Systems in Engineering and Bioscienc* [online]. [cit. 2015-01-27]. Dostupné z: http://www.wseas.us/e-library/conferences/2014/Gdansk/SEBIO/SEBIO-24.pdf

MAHMOOD, Zaigham, 2013. *Cloud Computing: Methods and Practical Approaches*. Springer science. ISBN 1447151070.

MÁCHA, Petr, 2012. Cloud computing – historie a budoucnost. *DD Connect* [online]. Březen 2012 [cit. 2014-08-14]. Dostupné z: http://www.ddconnect.cz/brezen-2012/datova-centra.html

MARSTON, Sean, Zhi LI, Subhajyoti BANDYOPADHYAY, Juheng ZHANG a Anand GHALSASI, 2011. Cloud computing - the business perspective. *Decision Support Systems* [online]. Duben 2011, č. 1 [cit. 2014-08-10]. Dostupné z: http://www.sciencedirect.com/science/article/pii/S0167923610002393

MATYSKA, Luděk, 2007. Techniky virtualizace počítačů (2). *Zpravodaj ÚVT MU* [online], roč. 17, č. 3 [cit. 2014-07-30]. Dostupné z: http://www.ics.muni.cz/bulletin/articles/545.html

MOHAMED, Arif, 2009. A history of cloud computing. *A history of cloud computing* [online]. [cit. 2014-07-22]. Dostupné z: http://www.computerweekly.com/feature/A-history-of-cloud-computing

MELL, Peter a Timothy GRANCE, 2011. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. *The NIST Definition of Cloud Computing* [online]. September 2011 [cit. 2014-07-22]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Nařízení komise (es) č. 800/2008, 2008. In: *Úřední věstník Evropské unie*. 2008, č. 800. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:214:0003:0047:cs:PDF

NOVOTNÝ, Ota, Jan POUR, Miloš MARYŠKA a Josef BASL, 2010. *Řízení výkonnosti podnikové informatiky*. 1. vyd. Praha: Professional Publishing, 275 s. ISBN 978-80-7431-040-9.

Obchodní zákoník. In: *Sbírka zákonů České republiky*. Česká republika, 1991, č. 513, 98. Dostupné z: http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx

PEPPARD, Joe a John WARD, 2004. Beyond strategic information systems: towards an IS capability. *The Journal of Strategic Information Systems* [online]. roč. 13, č. 2, s. 167-194 [cit. 2014-08-25]. DOI: 10.1016/j.jsis.2004.02.002. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0963868704000046

PETTEY, Christy a Laurence GOASDUFF, 2009. Gartner Highlights Five Attributes of Cloud Computing. *Gartner* [online]. 23. června 2009 [cit. 2014-08-28]. Dostupné z: http://www.gartner.com/newsroom/id/1035013

PRODĚLAL, Jaroslav, 2010. Virtualizace, clustery a cloud computing. *Co je to virtualizace?* [online]. [cit. 2014-07-30]. Dostupné z: http://www.oldanygroup.cz/virtualizace-vmware-zakladni-informace-9/

Published ISO27k standards, 2014. ISECT. *Information security standards* [online]. [cit. 2014-09-25]. Dostupné z: http://www.iso27001security.com/index.html

RODRÍGUEZ-HARO, Fernando, Felix FREITAG, Leandro NAVARRO, Efraín HERNÁNCHEZ-SÁNCHEZ, Nicandro FARÍAS-MENDOZA, Juan Antonio GUERRERO-IBÁÑEZ a Apolinar GONZÁLEZ-POTES, 2012. A summary of virtualization techniques. *Procedia Technology* [online]. č. 3, s. 267-272 [cit. 2014-08-14]. DOI: 10.1016/j.protcy.2012.03.029. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S2212017312002587

SANDEEPRAJA, Batchu, J.N. CHAITANYA, N. SAI SAGAR a Patnala ESWAR, 2013. A study on Security Issues Associated with Public Clouds in Cloud Computing. *International Journal of Advanced Computer Technology* [online], č. 2, s. 28-32 [cit. 2015-01-27]. Dostupné z: http://ijact.org/volume2issue2/IJ0220013.pdf

ŠMÍD, Vladimír, 2002. Pojem informačního systému. *Fakulta informatiky Masarykovy univerzity* [online].[cit. 2014-08-25]. Dostupné z: http://www.fi.muni.cz/~smid/mis-infsys.htm

ŠRETR, Vít. *Analýza nástrojů pro virtualizaci*. Pardubice, 2014. Dostupné z: http://hdl.handle.net/10195/56022. Diplomová práce. Univerzita Pardubice. Vedoucí práce Mgr. Josef Horálek, Ph.D.

TSAGKLIS, Ilias, 2013. Advantages and Disadvantages of Cloud Computing – Cloud computing pros and cons. *Java code geeks* [online]. 23. dubna 2013 [cit. 2014-08-10]. Dostupné z: http://www.javacodegeeks.com/2013/04/advantages-and-disadvantages-of-cloud-computing-cloud-computing-pros-and-cons.html

TURECKIOVÁ, Michaela, Jan POUR a Zuzana ŠEDIVÁ, 2004. Řízení a rozvoj lidí ve firmách: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky. Vyd. 1. Praha: Grada, 168 s. Expert (Grada). ISBN 80-247-0405-6.

UNIVERSITY OF CALIFORNIA, © 2014. *Open-source software pro dobrovolnické počítání a grid computing.* [online]. [cit. 2014-07-29]. Dostupné z: http://boinc.berkeley.edu

United States of America, 1998. Children's online privacy and protection act. In: *Public Law*. Dostupné z: http://www.coppa.org/coppa.htm

United States of America, 1996. Health insurance portability and accountability act. In: *Public Law*. Dostupné z: http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf

United States of America,2001. Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism. In: *Public Law*. Dostupné z: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

Virtual systems overview, 2004. *IBM Systems Software Information Center.* [online] [cit. 2014-07-29.]. Dostupné z: http://publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp?topic=/eicay/eicayvserver s.htm.

WHITNEY, Lance. Amazon EC2 cloud service hit by botnet, outage. *CNET* [online]. 2009 [cit. 2014-09-23]. Dostupné z: http://www.cnet.com/news/amazon-ec2-cloud-service-hit-by-botnet-outage/

VMWARE, ©2014. Virtualization Basics. *VMware* [online]. [cit. 2014-07-30]. Dostupné z: https://www.vmware.com/virtualization/virtualization-basics/how-virtualization-works.html

WINKLER, Vic (J.R.), 2011. *Securing the cloud: cloud computer security techniques and tactics*. Waltham, MA: Syngress/Elsevier, 290 p. ISBN 978-159-7495-929

WU, Linlin, Saurabh KUMAR GARG a Rajkumar BUYYA, 2012. SLA-based admission control for a Software-as-a-Service provider in Cloud computing environments. *Journal of Computer and System Sciences* [online]. Roč. 78, č. 5, s. 1280-1299 [cit. 2014-08-28]. DOI: 10.1016/j.jcss.2011.12.014. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0022000011001590

Seznam příloh

Příloha A

1. Využíváte ve Vaší organizaci cloudové řešení poskytování služeb?
- ano
- ne

Pokud respondenti využívají cloud, je jim zpřístupněna následující část otázek:

A. Jaký typ cloudu využíváte?
- Vlastní privátní
- Hostovaný privátní
- Veřejný
- Hybridní (kombinace privátního a veřejného)
- Komunitní

B. Služeb kolika cloudových poskytovatelů využíváte?
- 0 - vlastníme privátní cloud
- 1
- 2
- 3
- 4 a více

C. Jakého poskytovatele cloudu využíváte (v případě hostovaného nebo veřejného cloudu)?
- Využíváme pouze privátní cloud
- Microsoft Azure
- Google App Engine
- VMware vCloud
- Comparex
- Jiné:

D. Jaký byl Váš důvod pro přechod na využívání cloudu?

- Úspora finančních nákladů na infrastrukturu
- Redukce počtu zaměstnanců
- Zvýšení bezpečnosti dat
- Zajištění spolehlivosti a dostupnosti poskytovaných služeb
- Jiné:

E. Jaké distribuční modely cloudu využíváte?
- IaaS (Infrastructure as a service) - pronajímání infrastruktury
- Saas (Software as a Service) - pronajímaní infrastruktury společně se softwarem
- CaaS (Comunication as a Service) - zajištění komunikačních služeb (Mailservery, atd…)
- PaaS (Platform as a Service) - prostředky pro vývoj a testování aplikací
- MaaS (Monitoring as a Service) - monitoring aplikací
- Jiné:

F. V případě že máte ve firmě IT zaměstnance jejich počet se následkem využívání cloudového řešení služeb?

- Snížil
- Zvýšil
- Nezměnil
- Nemáme IT zaměstnance

G. Vznikly ve Vaší firmě další pracovní pozice jako následek využívání cloudového řešení služeb?

- Ne
- Ano, IT pozice
- Ano, manažerské pozice
- Ano, analytické pozice
- Jiné:

H. Kdo je odpovědný za komunikaci s poskytovatelem cloudových služeb?

- Pověřený zaměstnanec
- IT oddělení
- Jiné:

I. Jaké využíváte prostředky pro ochranu a přístup k datům?

- Šifrování přenosu dat
- Uživatelské role
- Přístupová práva
- Monitoring aktivit uživatelů
- Zabezpečená VPN
- Jiné:

J. Jak dlouho Vám trval přechod, než jste začali využívat cloudové řešení?

- méně než jeden měsíc
- méně než půl roku
- méně než rok
- déle než rok

K. Jak dlouho již využíváte cloudové řešení?

- méně než půl roku
- méně než rok
- méně než dva roky
- déle než dva roky

Pokud respondenti nevyužívají cloud, je jim zpřístupněna následující část otázek:

V případě jakých změn byste uvažovali o přechodu na využívání cloudových služeb?

1. Víc informací o umístění, ochraně a manipulaci s daty

- Začneme využívat cloudové služby
- Zvážíme využití cloudových služeb
- Nezačneme využívat cloudových služeb
- Cloudové služby pro nás nejsou perspektivním řešením

2. Úprava právních změn týkající se odpovědnosti poskytovatele a práv spotřebitele

- Začneme využívat cloudové služby
- Zvážíme využití cloudových služeb
- Nezačneme využívat cloudových služeb
- Cloudové služby pro nás nejsou perspektivním řešením

3. Kontrola poskytovatelů cloudových služeb nezávislými subjekty

- Začneme využívat cloudové služby
- Zvážíme využití cloudových služeb
- Nezačneme využívat cloudových služeb
- Cloudové služby pro nás nejsou perspektivním řešením

4. Dostupnost a spolehlivost vysokorychlostního internetu

- Začneme využívat cloudové služby
- Zvážíme využití cloudových služeb
- Nezačneme využívat cloudových služeb
- Cloudové služby pro nás nejsou perspektivním řešením

5. V jakém časovém horizontu plánujete začít využívat cloudové služby?

- Méně než půl roku
- Méně než rok
- Méně než dva roky
- Neplánujeme využití cloudových služeb

Společná část pro obě skupiny respondentů, bez ohledu zda využívají cloud, či ne.

Na základě Vašich současných poznatků o využívání cloudových služeb ohodnoťte jejich výhody a nevýhody.
Stupnice:

1 - maximálně výhodné
2 - výhodné
3 - srovnatelné se službami, které nejsou poskytovány jako cloudové řešení
4 - nevýhodné
5 - maximálně nevýhodné

I. Mobilní přístup (přístup přes internet kdekoliv, nejen z firemních prostor,...)

- 1
- 2
- 3
- 4
- 5

II. Kompatibilita (s ostatními systémy,…)

- 1
- 2
- 3
- 4
- 5

III. Zvýšení produktivity práce

- 1
- 2
- 3
- 4
- 5

IV. Škálovatelnost (Možnost využívání většího výpočetního výkonu pouze pokud je to třeba,…) *

- 1
- 2
- 3
- 4
- 5

V. Bezpečnost a ochrana dat (Ochrana budov, používání přístupových údajů,…)

- 1
- 2
- 3
- 4
- 5

VI. Změna výdajů na provoz IT infrastruktury

- 1
- 2
- 3
- 4
- 5

VII. Změna výdajů na platy zaměstnanců

- 1
- 2
- 3
- 4
- 5

VIII. Placení za služby, které skutečně využíváte

- 1
- 2
- 3
- 4
- 5

IX. Správa hardwaru a softwaru (technická podpora ze strany poskytovatele, aktualizace,…)

- 1
- 2
- 3
- 4
- 5

A. Jaká je oblast činnosti Vaší organizace?

- Vývoj hardware nebo software
- Strojní výroba
- Finančnictví
- Reality
- Stavebnictví
- Cestovní ruch
- Energetika
- Reklama, marketing
- Jiné:

B. Jaký je typ Vaší organizace?

- Státní organizace
- Soukromá firma
- Pobočka nadnárodní společnosti
- Jiné:

C. Jaký je počet zaměstnanců Vaší organizace?

- do 20 zaměstnanců
- 20 až 50 zaměstnanců
- 50 až 100 zaměstnanců
- 100 až 200 zaměstnanců
- 200 až 500 zaměstnanců
- 500 až 1000 zaměstnanců
- více než 1000 zaměstnanců