Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky
Katedra informačních technologií

Studijní program: Aplikovaná informatika
Obor: Informatika

Bezpečnost hybridního cloud computingu

BAKALÁŘSKÁ PRÁCE

Student : Ondřej Koudelka
Vedoucí : Ing. et Ing. Soňa Karkošková
Oponent : Ing. Lucie Šperková

2016

Prohlášení

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

V Praze dne . . . . . .

Ondřej Koudelka

Poděkování

Chtěl bych poděkovat vedoucí své práce Ing. et Ing. Soně Karkoškové za odborné vedení, za pomoc a cenné rady při zpracování této práce.

Abstrakt

Bakalářská práce se věnuje oblasti hybridního cloud computingu, zejména pak jeho bezpečností. Hlavním cílem práce je analýza a srovnání vybraných poskytovatelů hybridního cloudu. Dalším cílem je pak komparace bezpečnostních rizik v hybridním cloudu oproti ostatním modelům nasazení. Pro splnění cílů je v teoretické částí nejdřív vymezen a charakterizován pojem cloud computing a hybrid cloud computing. Poté jsou definovány rizika bezpečnosti v hybridním cloudu. V praktické části práce je na základě určených kritérií provedena analýza a srovnání konkrétních poskytovatelů hybridního cloudu.

Klíčová slova: Hybridní cloud, bezpečnost, šifrování, odpovědnost, SLA, důvěrnost

Abstract

This bachelor thesis deals with the area of hybrid cloud computing, specifically with its security. The major aim of the thesis is to analyze and compare the chosen hybrid cloud providers. For the minor aim this thesis compares the security challenges of hybrid cloud as opponent to other deployment models. In order to accomplish said aims, this thesis defines the terms cloud computing and hybrid cloud computing in its theoretical part. Furthermore the security challenges for cloud computing are defined and specified for hybrid cloud. The comparison of specific hybrid cloud providers is provided in the practical part along with the comparison of hybrid cloud security challenges.

Keywords: Hybrid cloud, security, encryption, responsibility, SLA, privacy

Obsah

1 Úvod

Není potřeba zdůrazňovat dnešní význam a používanost cloud computingu. S navyšujícím se tlakem na efektivnost firem z pohledu informačních technologií, nutí firmy hledat cesty k redukci provozních nákladů. Cloud computing nabízí firmám kromě snížení provozních a investičních nákladů i další výhody, jako je flexibilita, dostupnost, škálovatelnost a další.

Kvůli specifickým požadavkům přestávají organizace používat pouze privátní či veřejný cloud a volí mnohem flexibilnější metodu, hybridní cloud. Ačkoliv s sebou hybridní cloud nese celou řadu výhod, přináší také řadu bezpečnostních rizik. Bezpečnost hybridního cloudu je téma, kterému firmy i poskytovatelé v poslední době věnují velkou pozornost, jelikož si velmi dobře uvědomují jeho důležitost. Na bezpečnost jakéhokoliv informačního systému, ať už je v cloudu nebo ne, je potřeba nahlížet komplexně a navrhnout takovou architekturu, která pokryje všechny oblasti a rizika, kterým systém musí čelit. Jedním z úskalí je fakt, že nelze navrhnout jednotný návrh řízení bezpečnosti tak, aby vyhovoval všem podnikům. Každá organizace, která řeší nasazení cloudového řešení bude mít své specifické požadavky, které vyžadují individuální přístup.

Poskytovatelé hybridních cloudů hrají velkou část v řízení jeho bezpečnosti. Každý poskytovatel k problematice přistupuje trochu jiným způsobem, hlavně z hlediska odpovědnosti a nabízení služeb, které řeší bezpečnost v jednotlivých oblastech.

1.1 Důvod výběru tématu

Téma hybridního cloudu se poslední dobou stává stále používanějším přístupem k řešení podnikových výpočetních zdrojů. Samotné podniky implementující toto

řešení si uvědomují důležitost bezpečnosti svých dat a alokují na řešení bezpečnosti dostatečné zdroje. Toto téma jsem si vybral, protože neexistuje jednotné řešení bezpečnosti dat, které by pokrylo požadavky všech uživatelů, naopak se přistupuje ke každému řešení individuálně.

1.2 Cíle práce

Hlavním cílem práce je analyzovat a následně srovnat poskytovatele hybridního cloudu z hlediska poskytované bezpečnosti dat, a nabídnout tak čtenářům základní představu o situaci na světovém trhu. Mezi dílčí cíle této práce se řadí popis bezpečnostních výzev v oblasti hybridního cloudu a dále srovnání těchto výzev se situací v ostatních modelech nasazení.

1.2 Způsob dosažení cílů

Způsobů a metod pro dosažení určených cílů je několik. Především se jedná využití znalostí získaných při studiu, dále využití znalostí nabytých při čtení a studiu dostupných zdrojů a literatury. Pro praktickou část byla použita zejména analýza jednotlivých subjektů srovnání a následná syntéza zjištěných poznatků. Pro získání znalostí potřebných pro analýzu byly použity dokumentace jednotlivých poskytovatelů, jak jsou uvedeny v seznamu použité literatury. Předmětem analýzy byla specifika bezpečnostních rizik v jednotlivých modelech nasazení cloudu a přístupy k řízení bezpečnosti čtyř poskytovatelů hybridního cloudu.

1.3 Omezení práce

Analýza poskytovatelů hybridního cloudu je do jisté míry omezena množstvím a podrobností informací, které jednotliví poskytovatelé zpřístupňují ve své veřejné

dokumentaci. Pro podrobnější analýzu by byla potřeba úzká spolupráce přímo s poskytovateli.

1.4 Struktura práce

Práce se skládá ze dvou částí. V první, teoretické části, je definován cloud computing, jeho modely nasazení a poskytované služby, a dále jsou rozebírány bezpečnostní rizika v prostředí hybridního cloudu. Na základě těchto poznatků je v praktické části provedena komparace bezpečnosti dat v hybridním, veřejném a privátním cloudu. V další sekci praktické části jsou srovnáváni nejznámější poskytovatelé hybridního cloudu.

1.5 Očekávané přínosy

Očekávaným přínosem práce by měly být co nejkomplexnější informace o bezpečnosti dat v prostředí hybridního cloudu. Práce může být přínosná nejen pro základní seznámení s problematikou bezpečnosti dat v hybridním cloudu, ale může i poskytnout kritéria, která firmám pomůžou při rozhodovacím procesu ohledně nasazení cloudového řešení.

1.6 Definice základních pojmů

Pro větší srozumitelnost a eliminaci případných nejasností tato kapitola vymezuje základní pojmy.

Cloudové řešení – Cloudovým řešením se v této práci má na mysli soubor všech funkcí, služeb a komponent, které zajišťují nasazení cloudové infrastruktury pro dosažení podnikových cílů. Součástí cloudového řešení jsou také přístupy a strategie, pomocí kterých jsou zajišťovány dílčí systémové požadavky jako integrita nebo bezpečnost [ARMBRUST-2010].

Cloudová infrastruktura – Souhrn všech hardwarových a softwarových prostředků, které zajišťují splnění požadavků na cloudový model, jako například servery, uložiště, sítě, virtualizační software nebo API [DAWOUD-2010].

Hybridní cloud – Kombinace jednoho či více privátních cloudů a jednoho či více veřejných cloudů, společně s řízením propojení jednotlivých částí [CSCC].

Bezpečnost cloudu – Souhrn technologií a nařízení navržené tak, aby splňovaly požadavky na ochranu informací, aplikací a infrastruktury spojené s používáním cloud computingu [CloudSecurityAlliance-2011].

1.7 Rešerše prací na podobné téma

V této kapitole jsou vyzdviženy práce, které se zabývají pojmem hybrid cloud computing nebo bezpečností v cloudovém prostředí. Kapitola se dělí na práce z Českého a zahraničního prostředí.

1.6.1 České publikace

Bakalářská práce Bezpečnostné riziká pre cloudové riešenia od autora Tomáše Kmoštince přibližuje problematiku bezpečnosti v cloudovém prostředí. Identifikuje typické oblasti, které se v oblasti bezpečnosti cloudu řeší, konkrétně pak adresuje zejména oblasti governance, compliance a architektury. Práce je spíše teoretického charakteru, nicméně je kvalitně zpracovaná a nabízí dobrý úvod pro čtenáře do dané problematiky.

Druhou studentskou prací, je bakalářská práce Hybridní cloudová řešení od Jana Ryšavého. Autor popisuje jednotlivé modely cloudu a jejich výhody případně nevýhody. Dále se zabývá některými konkrétními problematickými oblastmi při nasazení hybridního cloudu v praxi. Velkou část práce věnuje autor pojmu virtualizace, který podrobně definuje, a určuje oblasti, ve kterých se virtualizace

používá. Autor poměrně důkladně zpracovává nejdůležitější aspekty v oblasti nasazení hybridního cloudu, a ačkoliv je práce spíše teoretická, nabízí kvalitní základ pro další práci.

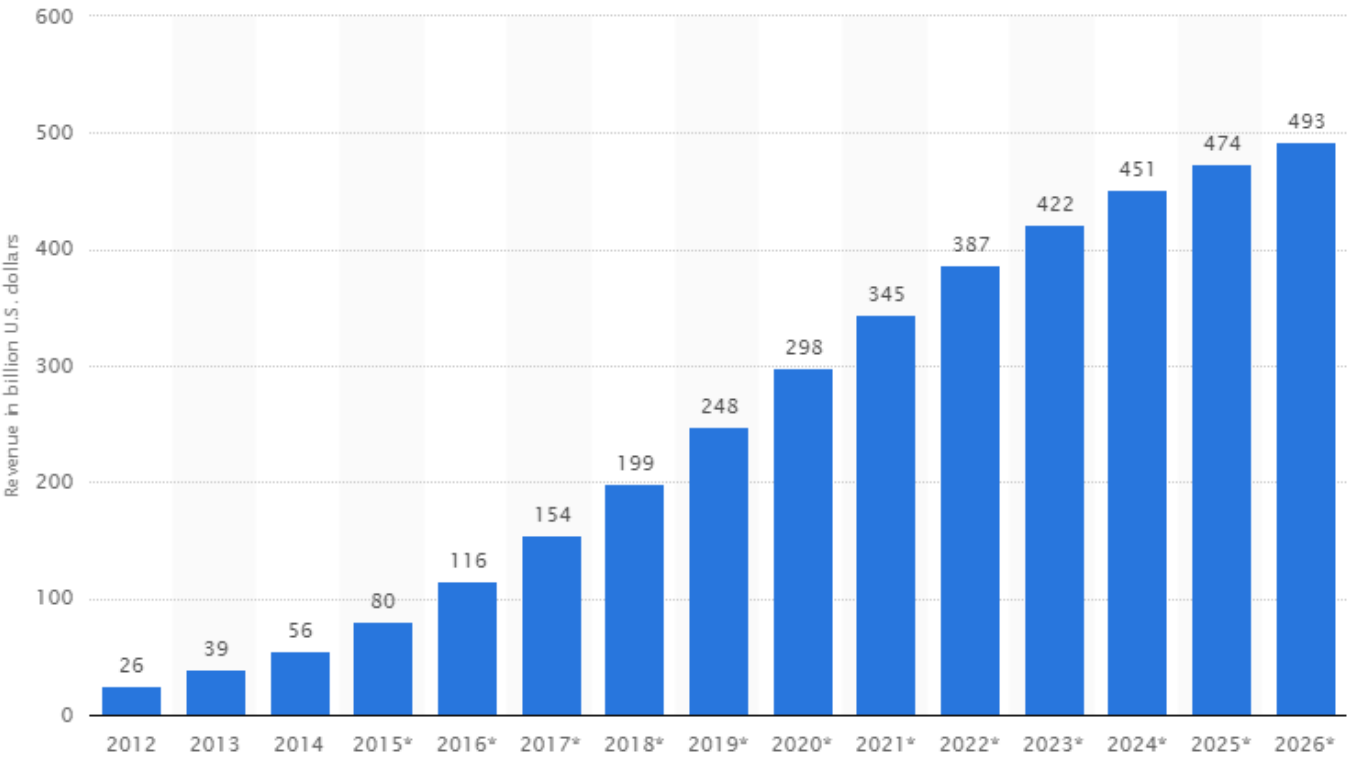
1.6.2 Zahraniční publikace

Ze zahraničních zdrojů bych rád uvedl knihu Cloud Security and Privacy od trojice autorů Tim Marther, Subra Kumaraswamy a Shahed Latif. Autoři v úvodu definují základní pojmy a oblast cloud computingu, následují pak kapitoly věnující se konkrétním oblastem bezpečnosti cloudu. V knize se popisuje bezpečnostní architektura, bezpečnost dat, správa identit a přístupu, řízení bezpečnosti, důvěrnost a auditování. Problematika je v publikaci popsána z velmi komplexního pohledu a dosti podrobně. Představuje proto kvalitní zdroj pro práce v dané oblasti.

Jako další zahraniční publikaci bych uvedl práci Public vs Private vs Hybrid vs Community – Cloud computing: Critical review od autora S. Goyala. Práce nabízí kromě definování základních pojmů i kritické zhodnocení rozdílů mezi jednotlivými modely nasazení cloudu. Hlavním přínosem práce je nastínění charakteristik, která jsou pro jednotlivé modely specifické.

2 Cloud computing

V dnešní době jsou pojmy jako Cloud, Hybridní cloud velmi frekventovaným a známým tématem, což lze vidět z finančních příjmů poskytovatelů cloudu, a jejich předpovědi do budoucna, kterýžto fakt zachycuje *Obrázek 1*. Cílem této kapitoly pro další práci na toto téma je tyto pojmy vyjasnit a zmapovat jejich prostředí a návaznosti.



Obrázek 1 – Vývoj příjmu cloudových poskytovatelů [STATISTA-2016]

Všechno, co bude popisováno a rozebíráno v této práci, bude podléhat pojmu Cloud computing, a proto bude následovat jeho vymezení na základě definice NIST (*National Institute of Standards and Technology*) [MELL-2011].

Cloud lze definovat jako model, který umožňuje realizaci přístupu ke sdíleným výpočetním zdrojům (např. sítím, službám, serverům, datovým uložištím), a který

bude dostupný jednoduše a na požádání. Zmíněné zdroje mohou být rychle zajištěny i uvolněny s minimálním řídícím úsilím a osobní interakcí poskytovatele [MELL-2011]. Model se dále vyznačuje následujícími pěti charakteristikami.

On-demand self service – Zákazník je schopný si sám požádat výpočetní kapacity podle své aktuální potřeby a alokace výpočetních zdrojů probíhá často automaticky, bez vyžadování lidského zásahu ze strany poskytovatele.

Broad network acces – Služby modelu jsou přístupné přes síť za pomocí standardních klientských platforem (např. mobilní telefony, tablety, laptopy, stolní počítače)

Resource pooling – Poskytovatelovy výpočetní kapacity jsou shromažďovány, aby byly k dispozici více klientům za užití víceuživatelského modelu, kde různé zdroje, fyzické či virtuální, jsou přiřazovány a uvolňovány podle potřeb jednotlivých uživatelů. V jisté míře se jedná o nezávislost zdrojů na lokaci a uživatelé typicky nemají kontrolu nad přesným umístěním zdrojů, nicméně mohou ho specifikovat v širší míře, například na úrovni státu.

Rapid elasticity – Zdroje mohou být elasticky přidělovány a uvolňovány, často automaticky, úměrně podle požadavků. Z pohledu zákazníka se může zdát, že zdroje jsou neomezeny v jakémkoliv množství a čase.

Measured service – Cloudové systémy automaticky kontrolují a optimalizují alokování a používání zdrojů do určité míry v závislosti na dané službě. Nabízí tak transparentnost pro obě strany, klienta i poskytovatele.

Cloud computing přináší následující výhody a nevýhody [IBM-2009]:

Výhody:

- Možnost masivního zvýšení výpočetních kapacit bez počátečních investic na pořízení infrastruktury
- Náklady odvíjející se od spotřeby výpočetních zdrojů
- Dostupnost
- Nízké provozní náklady
- Flexibilita účtování služeb
- Škálovatelnost
- Přístup k nejmodernějším technologiím

Nevýhody:

- Data se nacházejí mimo podnik
- Bezpečnostní rizika
- Závislost na poskytovateli
- Legislativní omezení
- Auditovatelnost třetích stran
- Ukončení činnosti poskytovatele

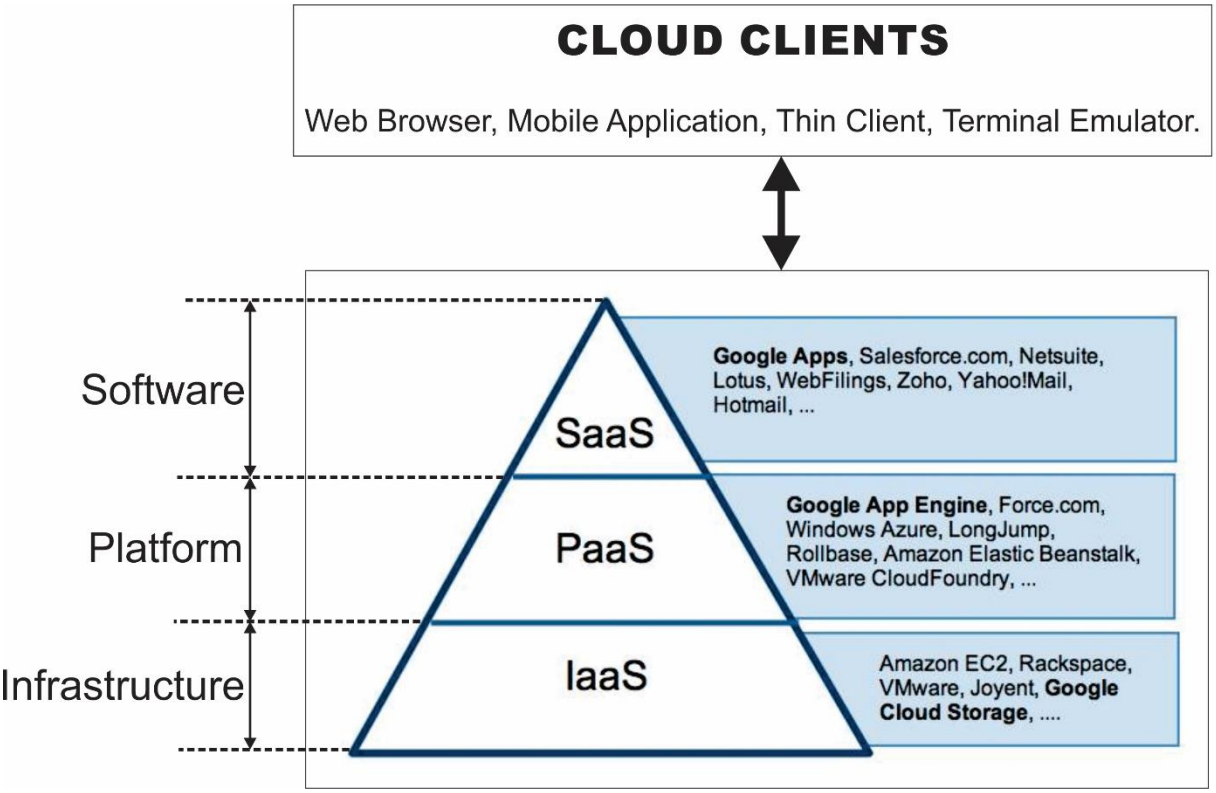
2.1 Modely cloudu

V této kapitole bude rozvedeno dělení cloudových modelů. Konkrétně se jedná o dvojí dělení, a to dělení podle služby, která je na cloudu nabízena, a poté podle nasazení. [SAVOLAINEN-2012]

2.1.1 Modely cloudu podle služby

Cloudová technologie nabízí tři základní úrovně abstrakce a podle toho odpovídající služby. Jedná se o Infrastructure as a service(IaaS), Platform as a

service(PaaS) a Software as a service(SaaS) [SAVOLAINEN-2012]. Na *Obrázku 2* najdeme vizuální znázornění návaznosti všech modelů, a několik příkladů pro lepší představu.



Obrázek 2 – Modely cloudu podle služby [OLUDELE, OGU-2014]

2.1.1.1 Infrastructure as a service

Spotřebitelé IaaS přímo používají IT infrastruktury nabízené poskytovatelem (processing, datová uložiště, sítě). Velmi často se v modelech IaaS používá virtualizace, a to kvůli schopnosti reagovat na poptávku klientů ad-hoc. Princip virtualizace znamená vytvoření virtuálních zdrojů nad zdroji fyzickými tak, aby došlo k naprosté izolaci těchto dvou sfér [PAVLIS]. Pokud tedy nějaký poskytovatel nabízí své servery jako IaaS cloud, nejedná se přímo o fyzické servery, ale o virtuálně vytvořené servery, které pracují nad servery fyzickými

[DAWOUD-2010]. Díky tomu jsou poskytovatelé schopni adekvátně alokovat a dealokovat potřebné zdroje ke konkrétním klientům.

2.1.1.2 Platform as a service

V tomto typu dodavatelé poskytují platformu, která podporuje celý životní cyklus softwaru. Pro klienty se tak nabízí příležitost jak spuštění hotového softwaru, aplikací či služeb, nebo jejich vyvíjení v profesionálním prostředí. Oproti klasickému „necloudovému“ modelu má PaaS několik zásadních výhod [KELLER-2008].

První důležitou věcí pro vývojové týmy je fakt, že s využitím PaaS nepotřebují dopředu vědět, kolik budou potřebovat paměti, výpočetního výkonu, nebo jak budou řešit případné zvýšení potřeby hardwaru. Toto řešení výrazně napomáhá v případech, kdy vyvíjená aplikace je již v provozu, ale potřebuje rychle a pružně reagovat na změny na trhu, požadavky uživatelů či opravovat chyby.

2.1.1.3 Software as a service

Model SaaS se od předchozích liší kromě jiného tím, že často již necílí na vývojáře, nýbrž na koncové uživatele. Jedná se o způsob distribuce softwaru, kdy samotná aplikace běží na serverech a datacentrech poskytovatelů, a uživatel k ní přistupuje zpravidla přes webový prohlížeč [TSAI, XIAOYING, YU-2014]. Veškerá správa softwaru i hardwaru je tedy přenesena na poskytovatele, případně je částečně outsourcována jiným poskytovatelem, a uživateli zůstane v režii pouze správa na administrativní úrovni.

Pro uživatele to přináší několik výhod. Pravděpodobně nejatraktivnější vlastností je redukce nákladů při zavádění softwaru [WATERS-2005]. Jediné, co uživatelé zaplatí, je poplatek za určitě období používání. Odpadají proto náklady na

instalaci, konfiguraci, nový hardware, školení a IT personál. Díky většímu počtu uživatelů softwaru, často z celého světa, nabízí modely SaaS větší pravděpodobnost zralosti a kvality produktu.

2.1.2 Modely nasazení

V oblasti cloudu může hrát velkou roli, jak jsou jednotlivé zdroje situovány. V zásadě rozlišujeme tři situace, které mohou nastat při integraci či vytváření cloudového prostředí [MELL-2011].

2.1.2.1 Veřejný cloud

Cloud je považován za veřejný, pokud je přes internet nabízen veřejnosti. Může se pochopitelně jednat o libovolné služby, aplikace, uložiště, výpočetní techniku nebo infrastrukturu [HOFMANN, WOODS-2010]. Tyto služby jsou ovšem provozovány jedním zprostředkovatelem, a spravovány tímtéž případně třetí stranou (poskytovatel může nabízet například úložné místo, nicméně hardware si bude pronajímat od poskytovatele IaaS). Tento fakt pochopitelně znamená, že veškerá data, ačkoliv jsou stále ve vlastnictví uživatele, jsou lokalizována na jiném, velmi často neznámém místě, než je operativa uživatele. Z toho plynou zásadní výhody i nevýhody tohoto modelu. [JANSEN-2011]

Výhody [ARMBRUST-2010]

- Nízké pořizovací náklady a náklady na provoz
- Vysoká škálovatelnost
- Spolehlivost

Nevýhody a hrozby [HOFMANN, WOODS-2010]

- Bezpečnost

- Limit internetového připojení

V souhrnu nabízí veřejný cloud hlavně finančně lepší možnosti, ovšem za cenu toho, že data mohou být uložena v jiné geografické oblasti, která má jinou legislativu v oblasti bezpečnosti a soukromí, a z kritického pohledu bychom mohli argumentovat, že nemáme dostatečnou kontrolu nad hrozbou v podobě kompromitace našich dat.

2.1.2.2 Privátní cloud

Na rozdíl od veřejného cloudu je privátní cloud realizován vždy jen pro jednu organizaci, ať už organizací samotnou nebo třetí stranou [MELL-2011]. Účelem privátního cloudu není poskytovat služby veřejnosti, ale naopak využívání uvnitř organizace, například pro zpřístupnění dat více pobočkám [GOYAL-2014].

Jedním z hlavních důvodů vytváření privátního cloudu jsou požadavky na zabezpečení citlivých dat. Podniky ovšem mohou využívat takzvaného *cloud burstingu.* To v jednoduchosti znamená přenesení určitého množství necitlivých dat či procesů na cloud veřejný, a uvolnění vlastních zdrojů pro dočasný zvýšený výkon [NAIR-2010]. Bylo již naznačeno, že výhody a nevýhody privátního cloudu se budou zásadně lišit od cloudu veřejného. [GROSSMA-2009]

Výhody

- Kontrola nad bezpečností
- Možnost vytvoření architektury „na míru“
- Flexibilita ve formě Cloud Burstingu

Nevýhody

- Vysoké pořizovací náklady

- Obtížnější zpřístupnění ze vzdálených míst

Privátní cloud je tedy evidentně nezbytným řešením pro organizace, které mají zvýšené nároky na bezpečnost svých dat, případně pro organizace, které mají velmi specifické požadavky na architekturu a funkcionalitu, které žádný veřejný poskytovatel nemůže nabídnout.

2.1.2.3 Komunitní cloud

Komunitní cloud je poměrně atypickým modelem cloudu. Tento model spadá mezi privátní a veřejný cloud, nicméně infrastruktura a výpočetní zdroje jsou určeny výlučně pro dvě a více organizací, které typicky sdílejí stejné regulace ohledně bezpečnosti, soukromí či jiné specifické požadavky [MARINO, BRISCOE-2009].

Výhody

- Nižší pořizovací náklady než privátní cloud

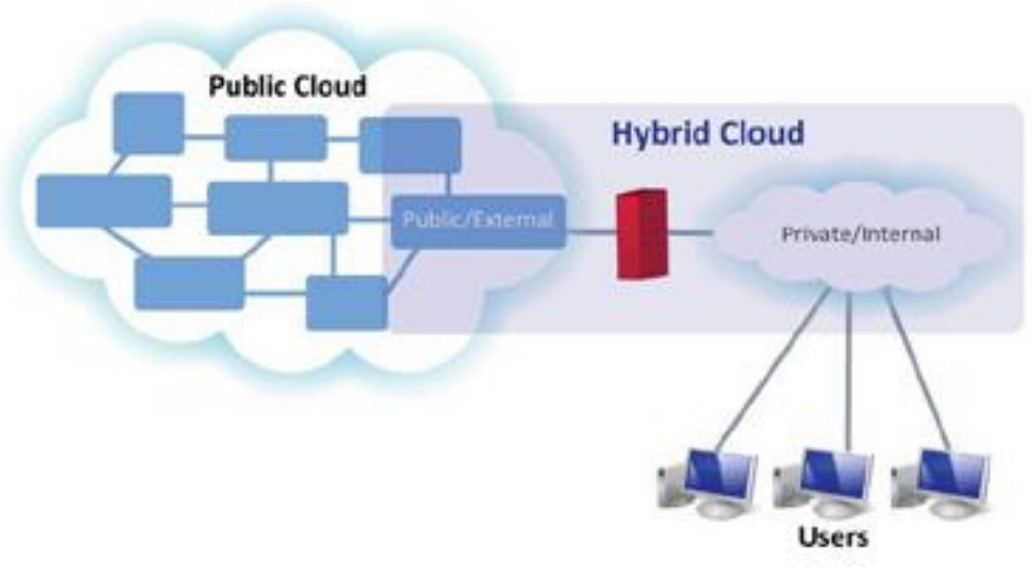
Nevýhody

- Omezená výpočetní kapacita sdílená všemi účastníky
- Vyšší pořizovací náklady než veřejný cloud

Koncept komunitního cloudu zatím tolik rozšířený není, využívá se spíše v menších podnicích či start-upech.

2.1.2.4 Hybridní cloud

Hybridní cloud kombinuje privátní a veřejný cloud dohromady. Typicky se jedná o jeden privátní cloud, který je připojen na jeden nebo více veřejných cloudů. Jedná se o bezpečnější způsob kontroly dat a aplikací, a zároveň umožňuje přístup přes internet. Umožňuje tak organizacím, aby naplnily své potřeby privátního cloudu, a zároveň aby mohly využívat výhody veřejného cloudu [JADEJA, MODI-2012]. *Obrázek 3* ilustruje, jak může hybridní cloud vypadat.



Obrázek 3 - Hybridní cloud [ASSUNCAO]

Je ovšem potřeba mít na paměti, že nasazení hybridního cloudu s sebou nese jisté překážky, zejména v oblasti propojení veřejné a privátní části cloudu. Vše záleží na návrhu, struktuře a implementaci projektu [ZOU-2013]. Základem úspěchu je dobře navržená architektura, která bude odpovídat byznys požadavkům dané organizace. Tato architektura musí kromě jiného zajistit konzistenci struktury veřejné části cloudu a privátní části cloudu. Při úspěšném navržení a konfiguraci modelu můžeme uvažovat následující výhody a nevýhody.

Výhody: [GOYAL-2014]

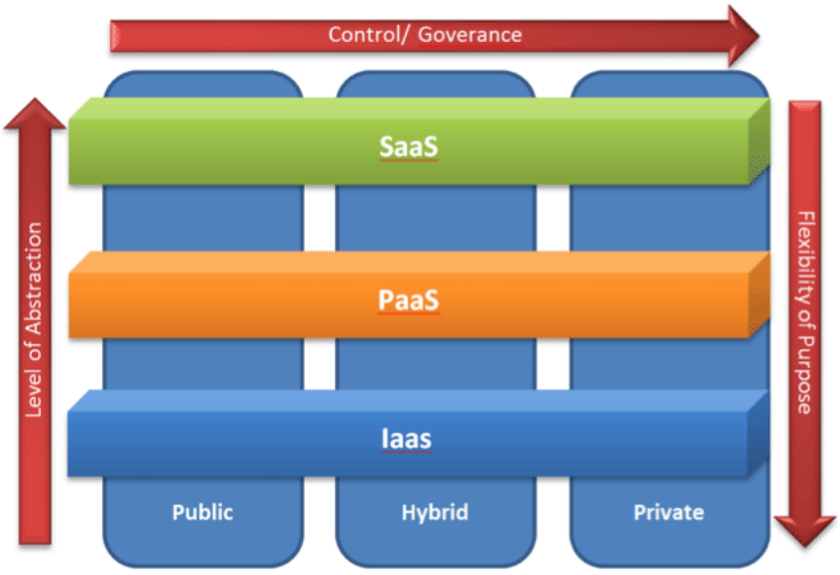
- Redukce nákladů na zavádění a údržbu organizační infrastruktury
- Zefektivnění zajišťování zdrojů pro dočasné projekty a redukce jejich nákladů a počátečních investic
- Optimalizace nákladů při různých životních cyklech vyvíjení softwaru
- Podpora cloud-burstingu

Nevýhody a hrozby: [GOYAL-2014]

- Bezpečnost dat ve veřejném cloudu a při komunikaci mezi veřejným a privátním cloudem

2.1.3 Shrnutí

V této kapitole byly definovány modely cloudu podle služeb a podle nasazení. Pro korektnost a úplnost je třeba zmínit, jak spolu souvisí jednotlivé modely napříč kategorizací. Pro lepší nastínění návaznosti jednotlivých modelů je zde uveden *Obrázek 4* [YOKOGAWA].



Obrázek 4 - Návaznost cloudových modelů [YOKOGAWA]

2.2 Bezpečnost hybridního cloudu

Bezpečnost a důvěrnost jsou pro zákazníky používající hybridní cloud klíčovými záležitostmi [CSCC]. Hybridní cloud je složen z minimálně jednoho privátního a minimálně jednoho veřejného cloudu, a jejich patřičného propojení. Převážně z tohoto faktu budou vyplývat bezpečnostní rizika specifická pro prostředí hybridního cloudu.

Tato práce cílí zejména na bezpečnost informací. Této oblasti se věnuje mezinárodní standard ISO 27001 Information Security Management. Tento standard poskytuje komplexní přístup k řízení informační bezpečnosti v organizacích, a definuje proto tři principy informační bezpečnosti.

Důvěrnost informací – Stav, kdy informace jsou přístupné pouze těm, kteří k nim mají povolený přístup.

Celistvost (integrita) informací – Informace jsou správné, úplné a konzistentní v celém systému.

Dostupnost informací – Uživatelé mají přístup k informacím v okamžik, kdy je potřebují.

2.2.1 Dostupnost

Důležitou součástí funkcionality cloudových služeb je jejich dostupnost [RODRIGUEZ-2011]. To znamená zajištění, že daná služba bude v ideálním případě dostupná odkudkoliv a kdykoliv. Pro monitorování a plánování této vlastnosti se můžou používat různé metriky. Pro příklad to může být doba obnovení, která udává čas potřebný k obnovení funkčnosti služby po výpadku, nebo procentuální vyjádření dostupnosti (pokud má být dostupnost služby 99,99%, může být nedostupná pouze 4 minuty za měsíc) [ZIMORY-2012].

Z hlediska poskytovatele toto představuje značnou výzvu. Každá elektronická komponenta má omezenou životnost, což znamená, že ve všech kritických místech je potřeba tyto komponenty zdvojnásobovat nebo i ztrojnásobovat [ZIMORY-2012]. To samé platí o datech, která musí být zálohována pro případ katastrofy, selhání disků nebo lidského faktoru.

Další riziko pro dostupnost služeb a dat představují cílené útoky. Typickými útoky jsou Zombie attack nebo Denial of service (Dos/DDos).

Zombie attack – Zombie attack spočívá ve v kompromitaci uživatelských počítačů hackery, které se pak označují jako zombie [HOSCH]. Toto označení vychází ze skutečnosti, že majitelé počítačů zpravidla nevědí o tom, že je jejich počítač kompromitován a využíván útočníkem. Po ovládnutí počítače získá útočník přístup do služby, a vytváří potenciální hrozbu.

Denial of service – Cílem DoS útoku je znepřístupnit případně znefunkčnit službu cílovým uživatelům [McDOWELL-2013]. Obecně může útočník využít chybu v cílovém systému, nebo masivního zahlcení systému požadavky. Jedním typem je tzv. DDoS útok (Distributed Denial of Service), který využívá většího množství počítačů, typicky infikovaných bez vědomí majitelů, pro zahlcení cíle útoku.

Existují různé úrovně dostupnosti služeb, [ZIMORY-2012] definuje následující:

- **AEC-0/Conventional:** Služba může být přerušena, integrita dat není zásadní
- **AEC-1/Highly Reliable:** Služba může být přerušena, ale integrita dat musí být zachována
- **AEC-2/High Availability:** Funkce může být přerušena pouze v daných časových rozmezích nebo na krátké časové úseky

- **AEC-3/Fault Resilient:** Služba musí být dostupná v domluvených časových rozmezích
- **AEC-4/Fault Tolerant:** Služba musí být dostupná nepřetržitě
- **AEC-5/Disaster Tolerant:** Služba musí být dostupná za všech podmínek

Pro prostředí hybridního cloudu je typické, že se skládá z více spolupracujících celků a služeb. V případě výpadku či nedostupnosti jednoho celku by měl celý systém řešit podle předem definovaného postupu, který by měl zajistit co nejlepší funkcionalitu zbylých celků.

2.2.2 Ochrana osobních údajů

Problém ochrany osobních údajů vzniká faktem, že pokud jsou data uložena na veřejném cloudu, je pravděpodobné, že toto uložiště bude fyzicky ležet do jiného státu než podnik, který cloud využívá, a bude podléhat odlišné legislativě [KULKARNI-2012]. Regulace ohledně nakládání s osobními údaji se může v různých státech lišit, a může dojít ke konfliktu mezi podnikem a poskytovatelem veřejného cloudu.

V každém případě je odpovědností klienta, tedy například podniku, který si zařizuje cloudové řešení u určitého poskytovatele, aby si tato fakta ověřil předem.

2.2.3 Přístup k datům

2.2.3.1 Identifikace, autentizace a autorizace

Identifikace – Proces, kdy uživatel udává svoji identitu, a systém kontroluje, zda tato identita v rámci systému existuje. Typicky se používají uživatelská jména.

Autentizace – Proces ověření pravosti identity, tedy potvrzení, že uživatel je skutečně tím, co tvrdí. Příkladem typu autentizace jsou kombinace jména a hesla, klíče, tokenů či biometrických prvků.

Autorizace – Proces ověření práva přístupu k jednotlivým datovým objektům, částem aplikací či systému.

Proces ověření identity a správa uživatelů je jedním z hlavních nástrojů pro řízení přístupu k podnikovým systémům a datům. Hlavním cílem je zabránění neautorizovaného přístupu, ať už externí či interní. Při řešení autentizace v hybridním cloudu vyvstává problém konzistence [JANSEN-2011]. Typickou situací může být, když podnik bude mít svůj systém pro ověřování identit, který ovšem nebude snadno rozšiřitelný pro spolupráci s veřejným cloudem. A pokud se podnik rozhodne řešit situaci druhým systémem, který bude identitu ověřovat v cloudu, může dojít k nekonzistentnosti obou systémů a potažmo k vytvoření bezpečnostní slabiny celého systému. V souvislosti s tím řeší společnosti přístup SSO (Single Sign-On) [PŘIBYL].

V prostředí hybridního cloudu se systémem SSO myslí služba, která zajistí jedno přihlašování do všech částí cloudu. Eliminuje tedy nutnost několika přihlašovacích metod, jmen a hesel. Zavádění takového systému vytváří potřebu zabezpečení komunikace, která bude potvrzovat autentizaci uživatelů mezi jednotlivými celky cloudu. Pokud se například nějaký zaměstnanec přihlásí do privátní části cloudu, a pak bude potřebovat pracovat s veřejnou částí, tento systém musí zajistit zabezpečený přenos informace, že tento uživatel může skutečně přistupovat k veřejné části cloudu. Zabezpečení této transakce zajistit například SAML (Security Assertion Markup Language) [HALLAM-BAKER-2001].

Jedním ze specifik hybridního cloudu je propojení privátní a veřejné části. Toto propojení představuje potenciální riziko v případě, nebude-li zabezpečené [LI, JEN-2015]. Například v případě neautorizovaného přístupu k veřejnému cloudu, by útočník mohl získat přístup k privátní části cloudu, což může být i infrastruktura samotného podniku, a to je rozhodně nežádoucí.

Dalším ohledem je správa přihlašovacích údajů, které by se nikde neměly vyskytovat v clear-textu. Pro ukládání hesel se nejčastěji používají hashovací funkce, například SHA-1 nebo SHA-2 [HAJNÝ-2009].

Další výzvou pro zabezpečení cloudu je zajistit uživatelskou odpovědnost [LI, JEN-2010]. Zásadní činností je proto sledování uživatelské aktivity, čímž se má na mysli zejména změny či mazání dat nebo extrakce dat mimo systém. Cílem je schopnost zpětného vystopování viníka při kompromitaci dat.

2.2.3.2 Řízení přístupu

Dalším důležitým prvkem při vytváření bezpečného cloudu je řízení uživatelského přístupu k datům. Různí uživatelé mají k výkonu své práce potřebu přistupovat k různým datům, a je třeba tento fakt zohlednit. V rozsáhlejších organizacích je vhodné při řízení přístupu k datům neuvažovat každého uživatele zvlášť, ale seskupovat uživatele do skupin podle rolí v organizaci, a práva pak přidělovat jednotlivým skupinám na základě pracovní náplně [CloudSecurityAlliance-2011].

Pro řízení přístupu již není výše zmíněný SAML dostačujícím prvkem. Typicky může být použit standard XACML (eXtensible Acces Control Markup Language), který řízení přístupu umožňuje [MATHER-2009].

Na druhé straně je třeba zohlednit i druhou stránku věci, a tou je řízení přístupu jednotlivých klientů poskytovatele cloudu. Jeden poskytovatel typicky má více klientů, tedy více podniků, kterým zprostředkovává své služby, což vyvolává hrozbu konfliktu mezi jednotlivými klienty a jejich daty. Je tedy důležité, aby poskytovatelé zajistili logickou izolaci jednotlivých sítí klientů, ačkoliv budou zpravidla pracovat na stejném hardwaru [SUBASHINI-2011].

Nesprávné řízení přístupu k datům může vést ke kompromitaci dat, nežádoucí změny v datech a zvýšení možnosti útoku.

2.2.4 Bezpečnost dat v uložištích

Bezpečnost uložených dat lze do jisté míry zajistit správným řízením přístupu, tedy kdo a do jaké míry může k datům přistupovat. Vzhledem k tomu, že poskytovatelé cloudů nabízejí jednu infrastrukturu pro více klientů, je potřeba data v uložištích šifrovat, aby v případě, že se někdo dostane k našim datům, aby tato data byla pro útočníka nečitelná a nepoužitelná [CARLIN, CURRAN-2011]. Šifrování zaručí zvýšení bezpečnosti dat, nicméně bude znamenat také větší výpočetní zátěž [NADEEM, JAVED-2005]. Proto je třeba zvolit vhodný způsob šifrování pro konkrétní případ.

Způsoby šifrování [YOUNG]**:**

- Symetrické šifrování – Šifrovací algoritmus, který používá jeden klíč k šifrování i dešifrování obsahu. Průmyslovým standardem pro symetrické šifrování dat je algoritmus AES [ASPNET].
- Asymetrické šifrování – V tomto případě algoritmus používá dvojici klíčů, privátní a veřejný. Jeden klíč se používá k zašifrování obsahu, a jen odpovídající druhý klíč dokáže obsah dešifrovat. Nejtypičtější asymetrickou šifrou je algoritmus RSA [ROUSE-2014].

Asymetrické šifry bývají většinou časově a výpočetně náročnější, a proto pro šifrování většího množství dat se zpravidla využívá symetrických šifer [HIGASHI-2013]. Při použití většího množství klíčů vyvstává potenciální problém se zajištění bezpečnosti a zároveň dostupnosti těchto klíčů. Tato oblast se obecně označuje jako Key management [YOUNG].

Jednou z otázek, kterou by měli klienti v prostředí hybridního cloudu řešit, je, jestli poskytovatel může číst jejich data [ORACLE-2016]. Odpověď musí být pochopitelně ne. Tato otázka souvisí s výše zmíněnou správou šifrovacích klíčů. Pokud je zajištěno zašifrování všech citlivých dat v cloudu, je taky nutné zajistit, aby šifrovací klíče byly ukládány v rámci klientovi infrastruktury. Tím mohou společnosti značně snížit riziko úniku dat.

Při uložení šifrovacích klíčů v podnikové infrastruktuře či privátním cloudu ovšem znamená problém s šifrováním a dešifrováním dat na straně veřejného cloudu [O'REILLY-2015]. Příkladem může být veřejná aplikace v cloudu, která nějakým způsobem sbírá informace o jejích uživatelích. Po získání, případně zpracování těchto informací je potřeba data zašifrovat a uložit, nicméně klíče se ukládají v oddělené části. Typickým řešením by mohl být transakční protokol pro přenos klíčů mezi cloudy.

2.2.5 Bezpečnost dat v pohybu

Přenosy dat v cloudovém prostředí již z definice probíhají přes internet, ať už se jedná o komunikaci cloudu s koncovým uživatelem, nebo o komunikaci mezi jednotlivými částmi cloudu (například mezi privátní a veřejnou částí), a proto během těchto datových přenosů musí být zajištěna jejich důvěrnost a jejich integrita [PRIYANKA, SUGATA-2013].

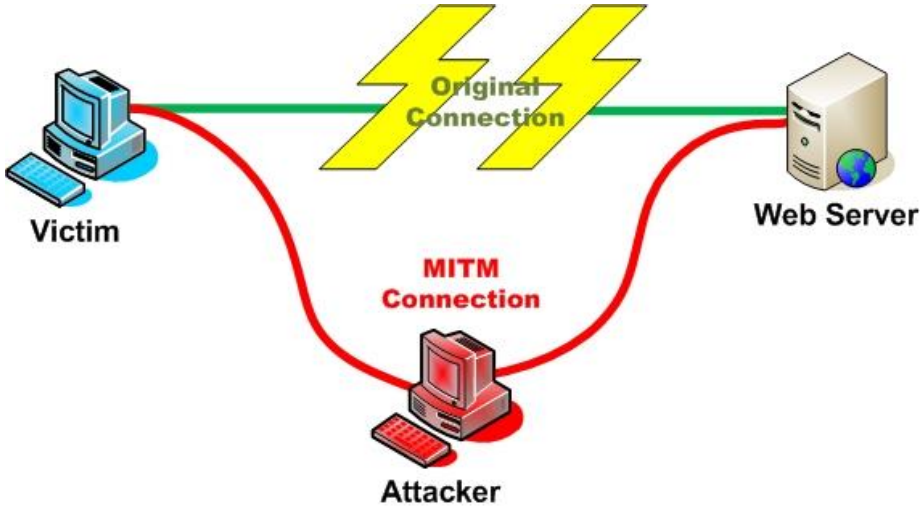
Důležitou částí bezpečného přenosu dat jsou rozhraní a API (Application Programming Interface), které poskytují zákazníkům cloudových poskytovatelů spravovat jejich cloudové služby. Zejména by se měly uvažovat následující oblasti.

Bezpečnost přenosu – API by měly nabízet zabezpečené kanály pro přenos dat, jako jsou SSL/TLS nebo IPSec [RESCORLA, MODADUGU-2012]. Použití těchto kanálů s sebou nese nutnost generování a spravování validních certifikátů.

Bezpečnost obsahu – Po zabezpečení přenosu je nutné vzít v úvahu zabezpečení samotného obsahu. V úvahu připadá návrh struktury zprávy, ověření integrity, kódování a šifrování.

Bezpečnost kódu – API, která zpracovává obsah v XML nebo JSON, případně přijímá input od uživatelů či aplikací, musí být dostatečně ošetřená a otestovaná proti standardním SQL Injection, Cross-site a dalším útokům na nedostatky v kódu.

Typickým útokem na nezabezpečený přenos dat je *Man in the middle,* kdy se útočník dostane do pozice mezi dvěma účastníky komunikace, jak je ilustrováno na *Obrázku 5,* a manipuluje jí podle své vůle [ORNAGHI, VALLERI-2003].



Obrázek 5 – Man in the middle [BRIGHTHUB-2008]

2.2.6 Odpovědnost za správu bezpečnosti

Při nasazování cloudového řešení je důležité vědět, za co je zodpovědný poskytovatel a za co klient. Typicky se celková odpovědnost za bezpečnost rozděluje podle typu modelu cloudu a podle přístupů jednotlivých poskytovatelů. Pro znázornění se často používají RACI matice (Responsible, Accountable, Consulted, Informed). Zjednodušený příklad takové matice v případě IaaS poskytovatele je v tabulce 1.

Tabulka 1: *RACI matice odpovědností [HAUGHEY]*

Oblast	Uživatel	Poskytovatel
Fyzická	C, I	R, A
Výpočetní	C, I	R, A
Data	R, A	C, I
Síť	C, I	R, A
Uložiště	C, I	R, A
Aplikace	R, A	C, I

2.2.7 Service level agreement

SLA je dokument, který z právního hlediska zajišťuje povinnosti stran při poskytování cloudového řešení [KUČERA-2014]. V zásadě se nejedná o bezpečnostní hrozbu v obvyklém slova smyslu, nicméně se jí může stát. Jelikož SLA ustanovuje, co jsou strany smlouvy zavázány splňovat, pro zákazníka může být tento dokument do jisté míry řešením některých bezpečnostních problémů. Typicky se v SLA ustanovuje dostupnost, ochrana osobních údajů, zabezpečení dat v závislosti na konkrétním poskytovateli. Nejdůležitější informací v SLA

dokumentu z hlediska bezpečnosti je definování odpovědností a scénářů při incidentech (např. výpadek, živelná pohroma, nedostupnost)

SLA obsahuje tři hlavní entity [PATEL, AJITH, RANABAHU-2009]:

Strany – Můžou se zde vyskytovat tři strany – Poskytovatel služby, klient, třetí strany.

Parametry – V SLA jsou parametry specifikovány metrikami. Každá metrika určuje, jakým způsobem se budou parametry služby měřit. Rozeznáváme dva základní typy metrik, a to metriky zdrojové, které jsou měřené přímo u poskytovatele, a dále se nijak nezpracovávají, a metriky složené, které se získávají kombinací či jiným zpracováním metrik zdrojových. Zdrojová metrika může být například počet transakcí, kdežto složená metrika by mohla být například počet transakcí za hodinu.

Cíle služby (SLO) – Jedná se o přesné cíle, které musí služba plnit, které se ustanovují, aby se předešlo nedorozuměním v této oblasti. Tyto cíle se definují jako specifické a měřitelné charakteristiky služby, příkladem může být dostupnost nebo odezva služby.

SLA dokumenty se skládají ze tří hlavních částí. V první se definují strany, které v dokumentu figurují. Ve druhé se popisuje služba, která bude nabízena, pomocí stanovených metrik. Ve třetí části se ustanovují povinnosti, podmínky a garance.

Poskytovatelé hybridního cloudu budou zpravidla používat jeden standardizovaný SLA dokument pro svoje zákazníky [MURPHY-2014]. A jelikož každá společnost bude mít jiné požadavky na realizaci jejího cloudového řešení, vyvstává v této oblasti konflikt.

3 Srovnání bezpečnosti cloudových modelů podle nasazení

Bezpečnostní rizika, která jsou potřeba adresovat, napříč jednotlivými modely nasazení nebudou vždy stejná. Proto tato kapitola nabídne identifikaci a popsání základních specifik modelů podle nasazení z hlediska bezpečnosti.

3.1 Privátní cloud

Privátní cloud by měl zajišťovat největší možnou bezpečnost v oblasti cloudových řešení, a to proto, že již z definice vyplývá, že nikdo jiný, než samotný klient, nemá ke cloudu přístup. Proto je nutné adresovat následující oblasti.

Největším rizikem, co podnik s privátním cloudem musí řešit, je řízení a monitorování uživatelského přístupu [DIOGENES, SHINDER, STEVENS-2016]. Tím se má na mysli zejména autentizace, autorizace, přístup založený na rolích v organizace a monitorování uživatelů.

Z hlediska poskytovatele je potřeba zajistit, aby byl cloud skutečně privátní. Fyzické výpočetní zdroje, které jsou v rámci jednoho poskytovatele, jsou sdíleny více uživateli, a musí být zajištěno, aby každý klient měl přístup pouze ke svým datům a službám. [DIOGENES, SHINDER, STEVENS-2016]. A proto v momentě, kdy se zdroje jednoho uživatele uvolní a mají se přidělit jinému klientovi, je nutné, aby zdroje byly vyčištěné od všech dat od předešlého klienta. Další riziko vychází ze skutečnosti, že cloud má mít vysokou elasticitu. Vyvstává obava, že škodlivá aplikace, klient nebo útočník může destabilizovat datové centrum poskytovatele vytvářením velkého množství požadavků na výpočetní zdroje.

3.2 Veřejný cloud

V privátním cloudu za předpokladu dostatečného zabezpečení ze strany poskytovatele podnik řeší pouze přístup svých zaměstnanců. Interface aplikací ve veřejném cloudu je zpravidla internetový prohlížeč, což zvyšuje důležitost správy přístupu, hesel a identit [IBM]. Přechodem aplikace do veřejného cloudu vkládá podnik velkou důvěru do poskytovatele cloudu, jelikož ztrácí přímou kontrolu nad bezpečnostním managementem a předává tuto kontrolu částečně svému poskytovateli [JANSEN-2011].

Ve veřejném cloudu přibývá další bezpečnostní perspektiva, a to jsou koncoví uživatelé služby, kterou podnik prostřednictvím internetu nabízí. Služba musí být na jednu stranu zabezpečená oproti útokům ze strany uživatelů, a na druhou stranu zabezpečovat uživatele a jejich data.

3.3 Hybridní cloud

Jak je již popsáno v této práci, hybridní cloud se skládá z veřejné a privátní části. Z toho vyplývá, že hybridní cloud bude dědit všechny bezpečnostní rizika cloudu privátního a veřejného.

Aby tyto samostatné části mohly vůbec spolupracovat, musí mezi nimi existovat vhodná komunikace, která je dalším zdrojem bezpečnostních rizik. Je nutné, aby tato komunikace byla zabezpečená proti potenciálním útočníkům [CHEN-2012].

Při nasazování hybridního cloudu může nastat problém s kompatibilitou jednotlivých částí. Například pokud má podnik privátní cloud vyvinutý svými silami, případně jiným poskytovatelem než veřejný cloud, do kterého se chce rozšířit, vyvstává otázka, zda jednotlivé části budou kompatibilní například v oblasti řízení přístupu [GOYAL-2014].

3.4 Shrnutí

Na závěr je důležité zmínit, že nelze jednoznačně určit, který model je nejbezpečnější. Každý z modelů čelí trochu odlišným bezpečnostním výzvám, a výsledná bezpečnost bude výsledkem konkrétního přístupu k jejich řešení. Záleží hlavně na poskytovatelích cloudu, jak zabezpečují svojí architekturu, a jakou nabízí podporu pro svoje klienty, a na klientech, aby zabezpečili svá data a aplikace.

4 Analýza poskytovatelů hybridního cloud computingu z hlediska bezpečnosti

V této kapitole budou analyzováni a srovnáváni jednotliví poskytovatelé platforem hybridního cloud computingu na základě jejich přístupů a řešení bezpečnostních rizik a výzev. Pro tuto analýzu byli vybráni následující poskytovatelé: Microsoft, VMWare, Amazon Web Services, IBM a Hewlett-Packard.

Je třeba zmínit, že tato práce hodnotí pouze skutečnosti, které poskytovatelé garantují a popisují ve svých dokumentacích. Není bohužel možné hodnotit konkrétní návrhy a implementace, jelikož, jak je zřejmé, tyto informace nejsou veřejné.

Kritéria pro srovnání vycházejí z teoretické části této práce a budou založena na skutečnosti, jak přistupují jednotliví poskytovatelé k:

- Zabezpečení dat v uložištích
- Zabezpečení dat v pohybu
- Řízení přístupu k datům

4.1 Microsoft

Společnost nabízí sadu integrovaných cloudových služeb pod jednotným názvem Microsoft Azure. Azure poskytuje klientům jak model IaaS tak i PaaS. Jako zdroje byla použita [MICROSOFT-2015-2] a [MICROSOFT-2015-4]

3.1.1 Bezpečnost dat v uložištích

Řízení lokace uložení dat. Klienti mají možnost určit geografickou oblast, kde budou jejich data uložena.

Šifrování a Key management. Pro uložená data Azure nabízí škálu řešení pro šifrování, aby klient měl možnost zvolit typ a způsob šifrování podle své konkrétní potřeby. Klienti mají možnost své šifrovací klíče generovat, spravovat, určovat, kdo k jednotlivým klíčům má přístup, dokonce i revokovat kopie klíčů určené pro společnost Microsoft.

Izolace dat. Jakožto víceuživatelská služba Azure rozděluje data jednotlivých klientů na virtuální úrovni, ačkoliv můžou být umístěna na stejném hardwaru.

3.1.2 Bezpečnost dat v pohybu

Izolace sítě. Azure zaručuje oddělení jednotlivých klientů pomocí logické izolace jejich virtuálních sítí.

Šifrování komunikace. Šifrována může být komunikace mezi jednotlivými virtuálními sítěmi i mezi privátní a veřejnou částí cloudu, a to pomocí technologií SSL/TLS/IPSec.

3.1.3 Řízení přístupu k datům

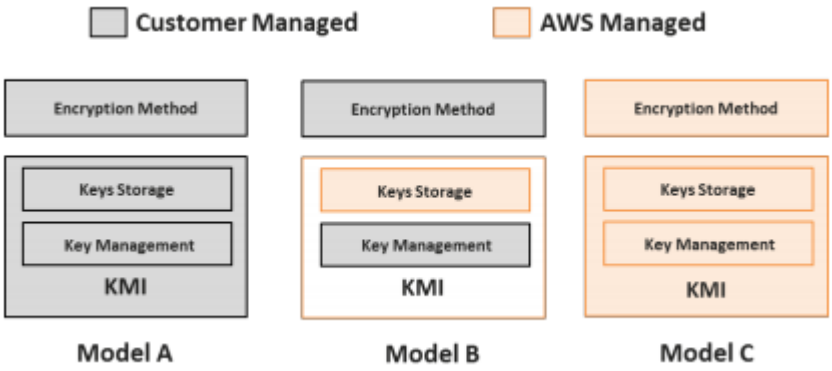
Pro řízení přístupu používá Azure službu Active Directory. Tato služba zajišťuje správu identit, uživatelů a jejich přístupu k aplikacím a datům. Zároveň umožňuje monitorování uživatelských přístupů pro případ nevyžádaných incidentů. Dále Azure nabízí vícefaktorovou autentizaci pro zajištění vysokého zabezpečení.

4.2 Amazon Web Services

AWS řeší potřeby hybridního cloudu pomocí svých veřejných cloudů a pomocí jejich produktu AWS Direct Connect, která zajišťuje soukromé spojení mezi infrastrukturou společnosti klienta a jeho veřejným cloudem v rámci AWS. Jako zdroje byla použita dokumentace [BEER-2014], [AWS-2015] a [TODOROV-2013].

3.2.1 Bezpečnost dat v uložištích

Šifrování a Key Management. Pro potřeby šifrování a správy šifrovacích klíčů nabízí AWS tři modely řešení. Ty jsou rozdílné v tom, kdo ovládá šifrovací metody, ukládání klíčů a spravování klíčů. Jak lze vidět na *Obrázku 6,* AWS nabízí pro své klienty plnou kontrolu nad klíči a šifrovacími metodami, nabízí také, že veškerou správu bude zařizovat samotné AWS, případně rozdělení těchto zodpovědností.



Obrázek 6 - Modely přístupu k šifrování v AWS [BEER-2014]

3.2.2 Bezpečnost dat v pohybu

Šifrování komunikace. Veškerá komunikace mezi všemi službami je šifrována pomocí TLS protokolu.

Izolace sítí. Oddělení sítí je zajištěno vestavěnými firewally a řízením přístupu v jednotlivých sítích.

3.2.3 Řízení přístupu k datům

AWS nabízí schopnost definovat, udržovat a spravovat zásady uživatelského přístupu. Mezi služby v rámci řízení přístupu řadí správu identit a uživatelů, vícefaktorovou autorizaci a integraci s již zavedenými modely řízení ve společnosti klienta.

4.3 VMWare

Společnost VMWare nabízí podnikům produkt vCloud Air, který umožňuje přesun části klientova data centra a aplikací do cloudu. Jako zdroje byla použita dokumentace [VMWare] a [VMWare-1].

3.3.1 Bezpečnost dat v uložišti

Izolace dat. Uložiště dat jsou logicky rozdělena tak, aby každý uživatel měl přístup pouze ke svým datům.

Šifrování a Key Management. VMWare umožňuje klientům šifrovat svá data v uložištích a zároveň k tomu využít jejich existující řešení pro správu šifrovacích klíčů, a to za pomocí služeb partnerské společnosti CloudLink.

3.3.2 Bezpečnost dat v pohybu

Šifrování komunikace. VMWare vyžaduje po svých klientech zajištění šifrování komunikace pomocí SSL, TLS či IPSec protokolem pro zabezpečení komunikace mezi podnikovou infrastrukturou a cloudem.

Izolace sítí. Sítě jednotlivých klientů jsou logicky rozděleny pomocí virtualizace. Klienti mají možnost nastavení vlastních firewallů a pravidel v rámci svojí sítě.

3.3.3 Řízení přístupu k datům

VMWare ve své veřejné dokumentaci neuvádí žádnou podporu v oblasti řízení přístupu. Naopak spíše vyzývá své klienty, aby se touto oblastí zabývali a řešili svými silami.

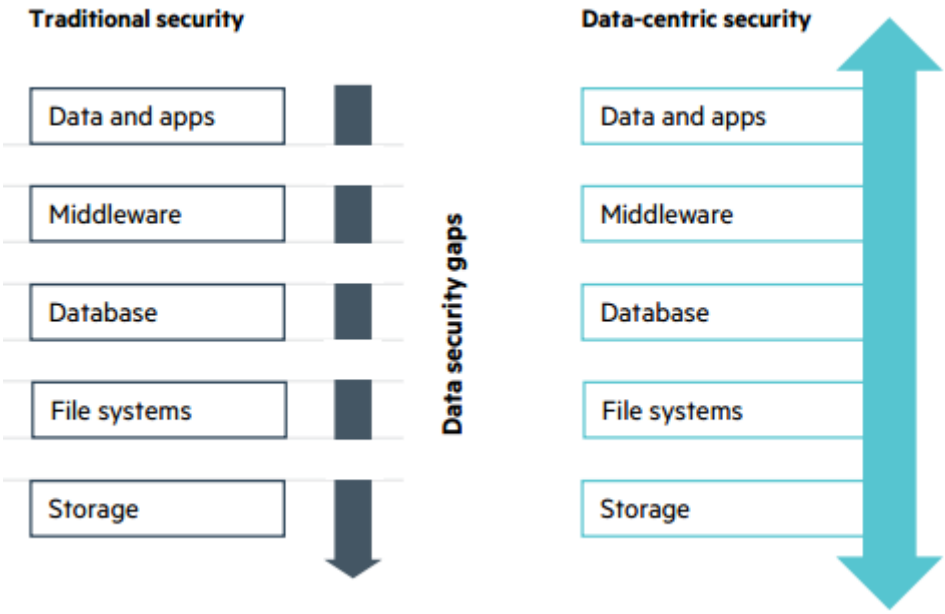
4.4 Hewlett-Packard

Jako zdroje byla použita dokumentace [HP-2016] a [HP-2015].

3.4.1 Bezpečnost dat

Společnost HP přichází v ohledu bezpečnosti dat s inovativním přístupem. Oproti běžnému postupu, kdy jsou data šifrována a dešifrována během jejich životního

cyklu. To podle společnost HP představuje bezpečnostní mezery, a proto přichází s data-centrickým přístupem, kdy data zůstávají zašifrovaná po celou dobu jejich využívání, viz *Obrázek 8*.

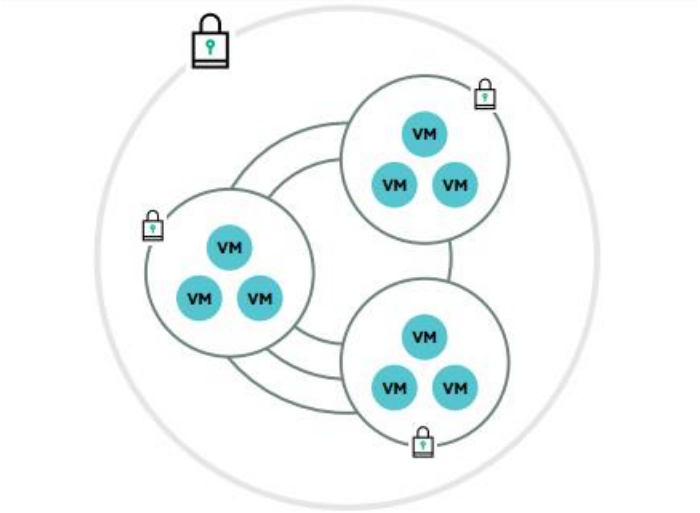


Obrázek 7 - Šifrování dat podle HP [HP-2016]

HPE Helion nabízí také nástroje pro škálovatelnou správu šifrovacích klíčů.

3.4.2 Izolace sítí

HP ve svém cloudovém řešení používá separaci sítí na fyzické i logické úrovni a vytváří podsítě v rámci jednoho klienta. Tyto podsítě jsou navrženy jako bezpečnostní zóny, a v případě úspěšného útoku na jednu podsíť útočník nedostane přístup k celé infrastruktuře a všem službám a datům. Logika tohoto přístupu je zřejmá z *Obrázku 9.*



Obrázek 9 - Izolace sítí [HP-2016]

3.4.3 Řízení přístupu k datům

Pro řízení přístupu nabízí HPE vlastní nástroje, které umožňují správu uživatelů a jejich přístupu na základě jejich rolí v organizaci. Tyto nástroje by měly také umožnit snadnou integraci s existujícím podnikovým řízením přístupu.

4.5 Shrnutí

V současné době poskytovatelé hybridního cloudu velmi cílí na bezpečnost svých služeb. Není reálné objektivně určit, který z poskytovatelů nabízí největší úroveň zabezpečení v prostředí svých cloudů, protože neuvádějí ve svých veřejných dokumentacích dostatečně podrobné informace, pomocí kterých by toto vyhodnocení mohlo proběhnout. Dalším důvodem je fakt, že každý podnik má

jiné potřeby pro svoje cloudové řešení, a pro každý podnik může být vhodnější jiný poskytovatel.

Můžeme, na druhou stranu, zhodnotit tuto problematiku z jiného úhlu pohledu. Pokud budeme hodnotit úroveň nabízených služeb, nástrojů pro řízení bezpečnosti a podrobnosti dokumentace, pak můžeme porovnání vyjádřit následující tabulkou, která uvádí pokrytí jednotlivých služeb nástroji nabízenými poskytovatelem.

Tabulka 2: *Srovnání bezpečnosti poskytovatelů*

	Microsoft	AWS	VMWare	HP
Zabezpečení dat v uložištích	Ano	Ano	Ano	Ano
Zabezpečení dat v pohybu	Ano	Ano	Ano	Ano
Řízení přístupu	Ano	Ano	Ne	Ano
Podrobnost dokumentace	4	3	2	2
Kontrola lokace dat	Ano	Ne	Ne	Ne

Pro hodnocení podrobnosti nabízené dokumentace bylo použito hodnocení 1-5, kdy 1 je nejhorší a 5 je nejlepší.

Z tabulky je zřejmé, že společnost Microsoft a její služba Microsoft Azure poskytuje nejlepší přístup k řízení bezpečnosti hybridního cloudu. Jako jednu z rozhodujících služeb bych u Azure zmínil Kontrolu lokace dat, která není běžnou záležitostí u cloudových poskytovatelů. Dokumentace je zároveň dostatečná, a

proto označil společnost Microsoft za nejlepšího poskytovatele hybridního cloudu v oblasti bezpečnosti dat, v určených kritériích.

5 Závěr

V této práci jsem se věnoval konceptu hybridního cloudu. V rámci teoretické části jsem zhodnotil charakteristiky cloud computingu, modely nasazení a služeb. Dále se práce věnovala bezpečnostními riziky v cloudovém prostředí, a tyto rizika byly specifikovány pro prostředí hybridního cloudu.

V rámci praktické části byly analyzovány a srovnány bezpečnostní výzvy a rizika hybridního cloudu oproti dalším modelům nasazení, jimiž jsou cloud privátní a veřejný. Na konec jsem analyzoval a pomocí syntézy srovnal čtyři známé poskytovatele hybridního cloudu na základě přístupu k řízení bezpečnosti dat a tím jsem naplnil všechny cíle práce.

Za největší přínos práce považuji charakterizování bezpečnostních rizik specifických pro cloudové prostředí, na základě čehož mohou potenciální uživatelé hybridního cloudu uvažovat o bezpečnostní strategii. Dalším přínosem je analýza poskytovatelů, která čtenářům poskytuje základní představu o přístupu poskytovatelů k bezpečnosti dat.

6 Terminologický slovník

Termín	Zkratka	Význam
Application Programming Interface	API	Rozhraní implementované v rámci aplikací, které umožňuje programátorský přístup ke službám daného informačního systému. [CHRISTENSSON]
Firewall		Hardwarový a softwarový prostředek s vlstní bezpečnostní politikou, autentizačními metodami, aplikační bránou a filtrem paketů, který logicky a fyzicky odděluje důvěryhodnou síť od nebezpečné sítě [GÁLA-2009]
Service level agreement	SLA	Smlouva mezi poskytovatelem služby a uživatelem, která stanovuje práva a povinnosti obou stran. [PATEL, AJITH, RANABAHU-2009]
Service level objective	SLO	Cíle, které se poskytovatel zavazuje, že služba splní. [PATEL, AJITH, RANABAHU-2009]
Single Sign-On	SSO	Přístup k více odděleným službám pomocí jedné autentizační metody. [PŘIBYL]
Cloud bursting		Dočasné zvýšení výpočetních zdrojů pomocí přenesení do veřejného cloudu. [NAIR-2010]
Security Assertion Markup Language	SAML	Standard založený na XML, který umožňuje výměnu autentizačních dat. [HALLAM-BAKER-2001]
eXtensible Access Control Markup Language	XACML	Standard, který definuje jazyk pro řízení přístupu. [MATHER-2009]
Secure hash algorithm	SHA	Hashovací funkce, která ze vstupních dat vytváří řetězec fixní délky [HAJNÝ-2009]
Advanced encryption standard	AES	Bloková symetrická šifra, která se používá k šifrování dat [ASPNET]
Rivest, Shamir, Adleman	RSA	Algoritmus pro asymetrické šifrování, používaný i pro podepisování [ROUSE-2014]

Secure socket layer	SSL	Protokol vložený mezi aplikační a transportní vrstvu, zajišťující bezpečnou komunikaci. [RESCORLA, MODADUGU-2012]
Transport layer security	TLS	Nástupce SSL. [RESCORLA, MODADUGU-2012]
Internet protocol security	IPSec	Bezpečnostní rozšíření protokolu IP, které je založené na šifrování a autentizaci každého IP datagramu. [ROUSE-2010]
SQL Injection		Typ útoku, kdy útočník vloží do webového formuláře SQL kód a pokouší se zpřístupnit utajovaná data. [ROUSE-2010-1]
Cross-site scripting	XSS	Typ útoku, kdy se na základě injekce javascriptového kódu útočník snaží znepřístupnit službu, zpřístupnit utajovaná data a obcházet bezpečnostní opatření. [ROUSE-2015]

7 Seznam použité literatury

[ARMBRUST-2010] Armbrust, Michael, et al. "A view of cloud computing." *Communications of the ACM* 53.4 (2010): 50-58.

[ASPNET] „Symetrické šifrování AES/Rijndael v .NET", *ASPNET.CZ*. [Online]. Dostupné z: http://www.aspnet.cz/articles/147-symetricke-sifrovani-aes-rijndael-v-net.aspx. [Viděno: 02-kvě-2016].

[ASSUNCAO] A. E. Assuncao, „Cloud Computing Basics for Business | YODspicaTM [Online]. Dostupné z: http://www.yodspica.info/2011/12/cloud-computing-basics-for-business.html. [Viděno: 18-dub-2016]

[AWS-2015] "Introduction to AWS Security" Amazon Web Services, 2015

[BEER-2014] Ken Beer, Ryan Holland "Encrypting Data at Rest" Amazon Web Services, 2014

[BRIGHTHUB-2008] „How Phishing happens: Know Your Enemy (Man in the Middle Attacks)". [Online]. Dostupné z: http://www.brighthub.com/computing/windows-platform/articles/4781.aspx. [Viděno: 22-dub-2016].

[BURROWS-1989] Burrows, Michael, Martin Abadi, and Roger M. Needham. "A logic of authentication." *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. Vol. 426. No. 1871. The Royal Society, 1989.

[CARLIN, CURRAN-2011] Carlin, Sean, and Kevin Curran. "Cloud computing security." (2011).

[CHEN-2012] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*. Vol. 1. IEEE, 2012.

[CloudSecurityAlliance-2011] Cloud Security Alliance. SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0. USA 2011. Dostupné z: https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf

[CRHISTENSSON] Christensson, Per. "API Definition." TechTerms. 2006. [Online]. Dostupné z: http://techterms.com/definition/api [Viděno 02-kvě-2016]

[CSCC] Cloud Standards Customer Council „A practical guide to hybrid cloud computing" 2016

[DAWOUD-2010] Dawoud, Wesam, Ibrahim Takouna, and Christoph Meinel. "Infrastructure as a service security: Challenges and solutions." *Informatics and Systems (INFOS), 2010 The 7th International Conference on*. IEEE, 2010.

[DIOGENES, SHINDER, STEVENS-2016] Yuri Diogenes, Tom Shinder, Anthony Stevens, „Private Cloud Security Considerations Guide-Security Challenges". 2014 [Online] Dostupné z: https://blogs.technet.microsoft.com/privatecloud/2014/11/09/private-cloud-security-considerations-guide-security-challenges/ [Viděno: 30-dub-2016]

[GÁLA-2009] Pour, Jan, Libor Gála, and Zuzana Šedivá. "Podniková informatika." (2009).

[GOYAL-2014] Goyal, Sumit. "Public vs private vs hybrid vs community-cloud computing: A critical review." *International Journal of Computer Network and Information Security* 6.3 (2014): 20.

[GROSSMA-2009] Grossman, Robert L. "The case for cloud computing." *IT professional* 11.2 (2009): 23-27.

[HAJNÝ-2009] Piller, I., and JAN HAJNÝ. "Hashovací funkce a jejich využití při autentizaci." (2009).

[HALLAM-BAKER-2001] Hallam-Baker, Phillip. "Security assertions markup language." *May* 14 (2001): 1-24.

[HAUGHEY] Duncan Haughey„RACI Matrix", *Project Smart*. [Online]. Dostupné z: https://www.projectsmart.co.uk/raci-matrix.php. [Viděno: 03-kvě-2016].

[HIGASHI-2013] M. Higashi, „Symmetric vs. Asymmetric Encryption", *CipherCloud*, 04-říj-2013. [Online]. Dostupné z: https://www.ciphercloud.com/blog/cloud-information-protection-symmetric-vs-asymmetric-encryption [Viděno: 19-dub-2016]

[HOFMANN, WOODS-2010] Hofmann, Paul, and Dan Woods. "Cloud computing: the limits of public clouds for business applications." *Internet Computing, IEEE* 14.6 (2010): 90-93.¨

[HOSCH] William L. Hosch „zombie computer", *Encyclopedia Britannica*. [Online]. Dostupné z: http://www.britannica.com/technology/zombie-computer. [Viděno: 02-kvě-2016].

[HP-2015] „Critical Security and Compliance Considerations for Hybrid Cloud Deployments“ Hewlett-Packard, 451 Research, 2015

[HP-2016] „Embrace risk: secure your hybrid cloud“ Hewlett-Packard, 2016

[IBM] IBM, „Public clouds, private clouds and your security“ [Online] Dostupné z: https://www.ibm.com/ibm/files/Z702257B23536P19/15PPCLOUDCOMPUTING_116KB.pdf [Viděno 30-dub-2016]

[IBM-2009] „Cloud computing versus grid computing", 03-bře-2009. [Online]. Dostupné z: http://www.ibm.com/developerworks/library/wa-cloudgrid/. [Viděno: 18-dub-2016].

[JADEJA, MODI-2012] Jadeja, Yaju, and Kavan Modi. "Cloud computing-concepts, architecture and challenges." *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*. IEEE, 2012.

[JANSEN-2011] Jansen, Wayne, and Timothy Grance. "Guidelines on security and privacy in public cloud computing." *NIST special publication* 800.144 (2011): 10-11.

[KELLER-2008] Keller, Eric, and Jennifer Rexford. "The" Platform as a Service" Model for Networking." *INM/WREN*. 2008.

[KUČERA-2044] Radek Kučera. „SLA - co je to a kdy se používá", *Bigdrobek*, 18-bře-2014. [Online]. Dostupné z: http://bigdrobek.com/sla-service-level-agreement/. [Viděno: 18-dub-2016].

[KULKARNI-2012] Kulkarni, Gaurav, et al. "A security aspects in cloud computing." *Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on*. IEEE, 2012.

[LEAVITT-2013] Leavitt, Neal. "Hybrid clouds move to the forefront." *Computer* 5 (2013): 15-18.

[LI, JIN-2010] Li, Jin, et al. "Fine-grained data access control systems with user accountability in cloud computing." *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*. IEEE, 2010.

[LI, JIN-2015] Li, Jin, et al. "A hybrid cloud approach for secure authorized deduplication."*Parallel and Distributed Systems, IEEE Transactions on* 26.5 (2015): 1206-1216.

[MARINO, BRISCOE-2009] Marinos, Alexandros, and Gerard Briscoe. "Community cloud computing."*Cloud Computing*. Springer Berlin Heidelberg, 2009. 472-484.

[MATHER-2009] Mather, Tim, Subra Kumaraswamy, and Shahed Latif. *Cloud security and privacy: an enterprise perspective on risks and compliance*. " O'Reilly Media, Inc.", 2009.

[McDOWELL-2013] Mindi McDowell,„Understanding Denial-of-Service Attacks | US-CERT". 2013 [Online]. Dostupné z: https://www.us-cert.gov/ncas/tips/ST04-015. [Viděno: 02-kvě-2016].

[MELL-2011] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011): 20-23.

[MICROSOFT-2015-2] „Microsoft Azure Network Security“, Microsoft, 2015

[MICROSOFT-2015-4] “Trusted Cloud: Microsoft Azure Security, Privacy, and Compliance”, Microsoft, 2015

[MURPHY-2014] Gina Murphy „What to consider when negotiating a hybrid cloud SLA", *Network World*, 26-lis-2014. [Online]. Dostupné z: http://www.networkworld.com/article/2851807/hybrid-cloud/what-to-consider-when-negotiating-a-hybrid-cloud-sla.html. [Viděno: 03-kvě-2016].

[NADEEM, JAVED-2005] Nadeem, Aamer, and M. Younus Javed. "A performance comparison of data encryption algorithms." Information and communication technologies, *2005. ICICT 2005. First international conference on*. IEEE, 2005.

[NAIR-2010] Nair, Srijith K., et al. "Towards secure cloud bursting, brokerage and aggregation." *Web services (ecows), 2010 ieee 8th european conference on*. IEEE, 2010.

[O’REILLY-2015] Jim O’Reilly „Managing Data Security In The Hybrid Cloud | Network Computing". 2015 [Online]. Dostupné z: http://www.networkcomputing.com/cloud-infrastructure/managing-data-security-hybrid-cloud/1424680999. [Viděno: 02-kvě-2016].

[OLUDELE, OGU-2014] A. Oludele, E. C. Ogu, K. ‘Shade, a U. Chinecherem, „On the Evolution of Virtualization and Cloud Computing: A Review", *Journal of Computer Sciences and Applications*, roč. 2, č. 3, s. 40–43, lis. 2014.

[ORACLE-2016] Oracle Cloud Computing, *Hybrid Cloud Security with Encryption and Key Management*. 2016 [Online] Dostupné z: https://www.youtube.com/watch?v=ke32mdXhJns [Viděno 02-kvě-2016]

[ORNAGHI, VALLERI-2003] Ornaghi, Alberto, and Marco Valleri. "Man in the middle attacks Demos."*Blackhat [Online Document]* 19 (2003).

[PATEL, AJITH, RANABAHU-2009] Patel, Pankesh, Ajith H. Ranabahu, and Amit P. Sheth. "Service level agreement in cloud computing." (2009).

[PAVLIS] Martin Pavlis, „Možnosti virtualizace, přínosy virtualizace serverů". [Online]. Dostupné z: http://www.systemonline.cz/virtualizace/moznosti-virtualizace-prinosy-virtualizace-serveru.htm. [Viděno: 18-dub-2016].

[PŘIBYL] Tomáš Přibyl „Single-Sign-On a jeho použití v praxi | Odborné články". [Online]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/single-sign-on-a-jeho-pouziti-v-praxi.html. [Viděno: 02-kvě-2016].

[PRIYANKA, SUGATA-2013] Priyanka Naik, Sugata Sanyal, „Increasing Security in Cloud Environment“, 2013

[RAMGOVIND-2010] Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. "The management of security in cloud computing." *Information Security for South Africa (ISSA), 2010*. IEEE, 2010.

[RESCORLA, MODADUGU-2012] Rescorla, Eric, and Nagendra Modadugu. "Datagram transport layer security version 1.2." (2012).

[RODRIGUZ-2011] Thoran Rodriguez | in T. E. Cloud, N. 20, 2011, a 10:00 Pm Pst, „What high availability for cloud services means in the real world", *TechRepublic*. [Online]. Dostupné z: http://www.techrepublic.com/blog/the-enterprise-cloud/what-high-availability-for-cloud-services-means-in-the-real-world/. [Viděno: 18-dub-2016].

[ROUSE-2010] Margaret Rouse „What is IPsec (Internet Protocol Security)? - Definition from WhatIs.com", *SearchMidmarketSecurity*. [Online]. Dostupné z: http://searchmidmarketsecurity.techtarget.com/definition/IPsec. [Viděno: 03-kvě-2016].

[ROUSE-2010-1] Margaret Rouse „What is SQL injection? - Definition from WhatIs.com", *SearchSoftwareQuality*. [Online]. Dostupné z: http://searchsoftwarequality.techtarget.com/definition/SQL-injection. [Viděno: 03-kvě-2016].

[ROUSE-2014] Margaret Rouse „What is RSA algorithm (Rivest-Shamir-Adleman)? - Definition from WhatIs.com", *SearchSecurity*. 2014 [Online]. Dostupné z: http://searchsecurity.techtarget.com/definition/RSA. [Viděno: 02-kvě-2016].

[ROUSE-2015] Margaret Rouse „What is cross-site scripting (XSS)? - Definition from WhatIs.com", *SearchSoftwareQuality*. [Online]. Dostupné z:

http://searchsoftwarequality.techtarget.com/definition/cross-site-scripting. [Viděno: 03-kvě-2016].

[SAVOLAINEN-2012] Savolainen, Eeva. "Cloud service models." *em Seminar--Cloud Computing and Web Services, UNIVERSITY OF HELSINKI, Department of Computer Science, Helsinki*. Vol. 10. 2012.

[SHACKLEFORD-2013] Dave Shackleford„Cloud API security risks: How to assess cloud service provider APIs", *SearchCloudSecurity*. 2013 [Online]. Dostupné z: http://searchcloudsecurity.techtarget.com/tip/Cloud-API-security-risks-How-to-assess-cloud-service-provider-APIs. [Viděno: 02-kvě-2016].

[STATISTA-2016] „Public cloud revenue worldwide 2012-2026 | Statistic", *Statista*. [Online]. Dostupné z: http://www.statista.com/statistics/477702/public-cloud-vendor-revenue-forecast/. [Viděno: 18-dub-2016].

[SUBASHINI-2011] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34.1 (2011): 1-11.

[TODOROV-2013] Dob Todorov, Yinak Ozkan, "AWS Security Best Practices" Amazon Web Services, 2013

[TSAI, XIAOYING, YU-2014] Tsai, WeiTek, XiaoYing Bai, and Yu Huang. "Software-as-a-service (SaaS): perspectives and challenges." *Science China Information Sciences* 57.5 (2014): 1-15.

[VMWare] „VMWare vCloud Air Security" VMWare, Dostupné z: https://www.vmware.com/files/pdf/vcloud-air/vmware-vcloud-air-security-technical-whitepaper.pdf

[VMWare-1] „VMware Product Security - Making Our Products More Secure | United States". [Online]. Dostupné z: https://www.vmware.com/security. [Viděno: 03-kvě-2016].

[VORMETRIC] Vormetric, "2015 Insider Threat Report" 2015, [Online] Dostupné z: http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf [Viděno 30-dub-2016]

[WATERS-2005] Waters, Bret. "Software as a service: A look at the customer benefits." *Journal of Digital Asset Management* 1.1 (2005): 32-39.

[YOKOGAWA] „SCADA Cloud Computing | Yokogawa America". [Online]. Dostupné z: http://www.yokogawa.com/us/technical-library/resources/application-notes/scada-cloud-computing/. [Viděno: 18-dub-2016].

[YOUNG] Young, Bill „Foundations of computer security" [Online]. Dostupné z: https://www.cs.utexas.edu/users/byoung/cs361/lecture44.pdf. [Viděno: 19-dub-2016].

[ZIMORY-2012] Zimory, „High availability in cloud computing". 2012 [Online]. Dostupné z: http://www.zimory.com/fileadmin/zimory/Downloads/Whitepaper/Product-HighAvailabilityinCloudComputing-270813-1611-134.pdf. [Viděno: 18-dub-2016].

[ZOU-2013] Zou, Caifeng, Huifang Deng, and Qunye Qiu. "Design and implementation of hybrid cloud computing architecture based on cloud bus." *Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference on*. IEEE, 2013.

8 Seznam obrázků

9 Seznam tabulek