Bezpečnost cloud computingu ve firemním prostředí

Bc. Petr Chalupský

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Petr Chalupský**
Osobní číslo:	**A14466**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Bezpečnost cloud computingu ve firemním prostředí**
Téma anglicky:	**The Security of Cloud Computing in a Business Environment**

Zásady pro vypracování:

1. **Vypracujte rešerši bezpečnostních a legislativních otázek v cloudu.**
2. **Zpracujte rizika při nakládání s osobními údaji v prostředí cloudu.**
3. **Prozkoumejte a porovnejte cloudová řešení s tradičním ICT z bezpečnostního a legislativního pohledu.**
4. **Navrhněte cloudová řešení u několika modelových společností s různou závislostí na ICT.**
5. **Popište možná řešení při nedostupnosti cloud služeb u navržených společností.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **VELTE, Anthony T, Toby J VELTE a Robert C ELSENPETER. Cloud Computing: praktický průvodce. Vyd. 1. Brno: Computer Press, 2011, 344 s. ISBN 978-80-251-3333-0.**
2. **SIEPMANN, Frank. Managing risk and security in outsourcing IT services: onshore, offshore and the cloud. Boca Raton: CRC Press, 2014, xvii, 226 s. ISBN 978-1-4398-7909-2.**
3. **LACKO, Ľuboslav. Osobní cloud pro domácí podnikání a malé firmy. 1. vyd. Brno: Computer Press, 2012, 270 s. ISBN 978-80-251-3744-4.**
4. **FURHT, Borivoje a Armando ESCALANTE. Handbook of cloud computing. 2010. New York: Springer, 2010, xix, 634 p. ISBN 9781441965240-.**
5. **METHENY, Matthew. Federal cloud computing: the definitive guide for cloud service providers. First edition. Amsterdam: Syngress, is an imprint of Elsevier, 2013, xxi,437 pages. ISBN 9781620819890.**
6. **KENNETH P. BIRMAN. Guide to reliable distributed systems: building high-assurance applications and cloud-hosted services. [new. ed.]. London: Springer, 2012. ISBN 9781447124153.**
7. **PROCHÁZKA, Jaroslav a Cyril KLIMEŠ. Provozujte IT jinak: agilní a štíhlý provoz, podpora a údržba informačních systémů a IT služeb. 1. vyd. Praha: Grada, 2011, 288 s. Průvodce (Grada). ISBN 978-80-247-4137-6.**

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

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **20. května 2016**

Ve Zlíně dne 5. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 17.5.2016

.....
podpis diplomanta

ABSTRAKT

Tato diplomová práce je zaměřena na hlubší porozumění podstaty cloud computingu. V teoretické části bude čtenář seznámen s bezpečnostními a legislativními otázkami, se kterými se můžeme při využití cloudových služeb setkat. Zejména v prostředí firmy nás totiž zajímá způsob nakládání s osobními údaji. Zdali jsou na všech úrovních adekvátně chráněna a zdali je s nimi zacházeno dle legislativních požadavků. V teoretické části práce budou také srovnána on-premise a cloud řešení v důležitých oblastech a přiblíženy smluvní podmínky užívání služby Windows Azure. V části praktické jsou navrženy tři rozdílné společnosti s využitím cloud služeb, které jsou rozděleny z pohledu závislosti výkonu své činnosti na ICT. Jsou popsána možná řešení při nedostupnosti užívaných služeb a také jsou stanoveny míry závažnosti při jejich nedostupnosti v kontextu navržených společností.

Klíčová slova: Cloud, bezpečnost, legislativa, osobní údaje, SLA, zálohování, šifrování, ICT, Windows Azure

ABSTRACT

This Master's thesis is focused on a deeper understanding of the nature of cloud computing. In the theoretical part, the reader will be familiar with security and legislative issues, which we can meet during use of cloud services. Handling of personal data is our main interest especially in business environment. Whether it is adequately protected at all levels and whether the handling meets legislative requirements. In the theoretical part will be also compared on-premise and cloud solution in important areas and Windows Azure terms of use will be closely described. In the practical part of this thesis are designed tree different companies using cloud services. Those model companies are divided in terms of dependence its activities on ICT. Within the unavailability of used cloud services are described possible solutions and determined levels of severity in the context of proposed companies.

Keywords: Cloud, security, legislation, personal data, SLA, backup, encryption, ICT, Windows Azure

Tímto bych chtěl poděkovat panu Ing. Davidu Malaníkovi, Ph.D. za ochotu, věnovaný čas a věcné připomínky, které mi pomohly při vypracování této diplomové práce. Dále bych chtěl poděkovat rodině a zaměstnavateli za všeobecnou podporu v průběhu studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Nacházíme se v době, kdy jsou data pro mnoho firem až existenčně důležitým faktorem. Podniková aktiva je zapotřebí adekvátně chránit a u dat samotných to platí dvojnásob. Spojení podnikových dat a cloudu je pro mnoho lidí zatím nepředstavitelné, jelikož citlivá data na internet nepatří. Databázi zaměstnanců, obchodních partnerů, účetní záznamy a další kriticky důležité informace také nenecháme jen tak někde pohozené na veřejném místě.

Cloud ale není jen informační dálnice, kde se může pohybovat kdokoliv a s trochou umu manipulovat prakticky s čímkoliv. Se správně nastavenými a implementovanými nástroji a procesy se mohou tato řešení těm klasickým rovnat nebo je i převyšovat. [1]

Při jakékoliv manipulaci s firemními informacemi je nutné dbát na jejich bezpečnost. Zvláště pokud se jedná o digitální informace umístěné mimo danou organizaci, a to datová centra cloudových služeb bezesporu jsou. Mohou se vyskytovat prakticky kdekoliv na planetě. Vzhledem k legislativním požadavkům, nejen domácí země dané organizace, musíme při výběru poskytovatele cloud služeb legislativu a povahu našich dat brát v potaz.

Tradiční řešení ICT prostředků má mnoho společných úskalí s cloudovým řešeními a cloud samotný se může už jen z principu jevit jako rizikové řešení. Dnes jsou však poskytovatelé schopni dodat kvalitní, mnohdy i lepší a bezpečnější řešení, než jsou některé organizace schopny realizovat vlastními prostředky. Právě díky cloudu mohou podniky dosáhnout na ty nejmodernější technologie a postupy, které by si samy nemohli dovolit z finančních důvodů či kvůli absenci kvalifikovaných zaměstnanců ba dokonce vhodných prostor.

Nejen pro nové podniky je tak zde možnost dosáhnout na vlastní infrastrukturu s možností flexibilního přizpůsobení dle aktivních potřeb, a to bez velkých počátečních investic.

Myslíme-li to s cloudem vážně, je výběr správného poskytovatele služeb velmi důležitý. Vzniká tak strategické partnerství, které zásadně ovlivní budoucnost daného subjektu a chybná volba může naše záměry zkomplikovat. Tato stránka však není výsadou cloudu. Své zásadní obchodní partnery a dodavatele máme i bez těchto služeb, ale vzhledem k různým sporným oblastem nabývá správný výběr v tomto případě ještě většího významu.

Každé řešení má svá pro a proti a v této práci se budeme zabývat nejenom bezpečnostními a legislativními aspekty cloudových řešení. Porovnáme tradiční on-premise firemní ICT s možnostmi cloudového přístupu. U navržených společností budou využity dostupné cloud služby a následně rozebrány možnosti při nedostupnosti těchto služeb.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ A LEGISLATIVNÍ OTÁZKY CLOUDU

Pokud se rozhodujeme o migraci do cloudu, zajisté si kromě otázky „Vyplatí se to?“ položíme otázku „Jaká jsou rizika?“. Na druhou otázku nelze jednoduše odpovědět, jelikož zde není pouze otázka bezpečnosti samotné. V dnešní době je důležité držet krok nejenom s dobou, ale hlavně s konkurencí. Nejlepší varianta je samozřejmě být o krok na před a k tomu nám mohou dopomoci flexibilní IT prostředky. Cloud ale není jen hezký mráček v diagramu znázorňující princip cloudu (viz Obrázek 1), ale pokud nebudeme dostatečně obezřetní při realizaci cloudového řešení, mohou se nad našimi obchodními záměry stáhnout temná mračna.

Obrázek 1 - Znázornění cloud computingu[1]

Při outsourcingu IT prostředků pomocí cloudu přistupujeme na SLA[2] daného poskytovatele. V dnešní době jsou již velmi rozsáhlá a je důležité je důkladně prostudovat a nepřehlédnout na první pohled nedůležitý aspekt, který může naše snažení velmi zkomplikovat. Zásadní je tedy SLA neignorovat, jelikož to může být zásadní bod při rozhodování zdali outscourcing ano či ne. Někomu může nabízené SLA padnout jako ručně šitý oblek a dosáhnout tak přirozenějšího IT prostředí za nižší cenu, ale většina zájemců o outsourcing tohoto pocitu přesně sedícího obleku nemusí dosáhnout. [2]

Při outsourcingu IT nebo obchodních procesů je bezpečnost ovlivňována na různých úrovních. Veškerá data, podléhající různému stupni důvěrnosti, byla dříve v námi řízeném pro-

[1] http://cloud-storage-services-comparison.com
[2] viz 1.2.2

středí, a to fyzické i logické stránce. Nyní pro nás kritická data byla svěřena třetí straně, která musí zajistit adekvátní ochranu svěřené informace proti neoprávněnému přístupu či poškození, a to jak poškození úmyslnému i neúmyslnému. Nedílnou součástí je samozřejmě dostupnost svěřených informací kdykoli je to pro obchodní účely zapotřebí.

Velmi důležitá je důvěryhodnost poskytovatel těchto služeb, jelikož kromě samotného podepsání smlouvy musí opravdu smluvené oblasti dodržet. Svěřujeme zde kritické informace, databáze zákazníků, naše know-how, atd. a tyto informace mohou být přístupné prakticky komukoli ze zaměstnanců. Některé informace jsou chráněné zákonem a jejich přenos mezi různými zeměmi je přísně regulován, zejména jde-li o osobní údaje zákazníků.

S masivním rozšířením cloud služeb se rozšířil kaskádový outsourcing, kdy poskytovatel může nabízet prostředky a služby, které on sám neprovozuje. Pronajímá si je od jiného poskytovatele ve velkém a sám je poté nabízí koncovým uživatelům jako samostatné služby. Těchto úrovní poskytovatelů může být více. Smlouvu můžeme mít podepsanou s určitým poskytovatelem, ale pokud on není tím primárním článkem, jsou naše informace jako kapka v moři jedniček a nul. Je nepravděpodobné, že námi adoptované a podepsané SLA s poskytovatelem nižší úrovně bude po všech stránkách odpovídat SLA na všech vyšších úrovních. Námi požadované bezpečnostní opatření a prvky pro ochranu osobních údajů nemusí být dodrženy, jelikož v hierarchii poskytovatelů námi využívaných prostředků se ve výsledku nemusí nikdo orientovat. Informace, která měla zůstat pouze v ČR, potažmo v EU, se najednou může fyzicky vyskytovat v Indii, Filipínách, Thajsku či jiných zemích. [2]

Výběr vhodného poskytovatele nemusí být tak jednoduchý, jak se může na první pohled zdát. Vzhledem k výše zmíněnému je vhodné zejména pro obchodní účely využívat služeb přímo z první ruky, kdy víme kdo dané prostředky vlastní, a i kde jsou fyzicky umístěny. Jelikož velmi často dochází ke zpracování citlivých údajů podléhajících regulaci či jsou chráněny zákony, je zapotřebí této části věnovat zvláštní pozornost. Před přechodem do cloudu si musíme odpovědět na naše otázky nejenom ohledně bezpečnosti. [2]

Cloud computingu se podařilo transformovat práci s výpočetními prostředky i se službami které se tímto způsobem realizují. Z jeho samotné podstaty vyplynula nutnost přizpůsobit či spíše vytvořit opatření na vládní úrovni. Cloud tak získává určitou formu a zachovávají se opatření, které již dlouho dobu fungují při klasickém využití ICT. Jen je nutné na tuto problematiku nahlížet doslova z globálního hlediska. [3]

Spolu s rozvojem cloudu, změnami v obchodních praktikách a novými zákony se objevily nové bezpečnostní hrozby, kterým je nutné čelit. Při přechodu z on-premise řešení na formu služeb, je zapotřebí přizpůsobit nejen obchodní postupy ale i naše myšlení. A to zejména při samotném návrhu daného řešení pro využití nového pojetí ICT a aplikací. Cloud se rychle vyvíjí a technologie podporující samotný obchod jsou stále dostupnější a propracovanější, než kdy dříve. Jak bohužel již v IT bývá zvykem, nové věci s sebou přinášejí nové hrozby, u nichž některé přetrvávají i po letech. [3]

Třebaže je realizace podnikového ICT pouze na cloudových technologiích relativně levná, rychlá a efektivnější než běžný model, nesmíme zapomínat na standardní zásady zabezpečení, procesy a osvědčené postupy. Vše za nás řeší „někdo jiný“, a to svádí k vynechání IT oddělení a odborných pracovníků. Stáváme se tedy pouhými uživateli, kteří nerozumí tomu, co používáme. Lze to přirovnat k manažerovi, který vymýšlí a plánuje takzvaně od stolu a přitom nemá zdání o vnitřních souvislostech a hlavně o tom, jak to ve skutečnosti chodí. Pokud budou tyto dlouhodobě osvědčené bezpečnostní prvky chybět, jsme náchylní k narušení bezpečnosti, které nás může o veškerý cloudem získaný náskok připravit. [3][4]

1.1 Bezpečnostní pohled

1.1.1 Klíčové problémy v oblasti bezpečnosti a ochrany osobních údajů

Jelikož cloud computing vznikl ze standardních technologií jako architektura orientovaná na služby, virtualizace, web 2.0 nebo utilitní model, je mnoho bezpečnostních a legislativních otázek již známých z klasického IT modelu. V případě cloudu je na tyto již známé problémy nutné nahlížet v jiném světle. Neměli bychom význam kombinace těchto známých technologií v novém prostřed podceňovat. Cloud computing představuje oproti konvečním modelům značnou transformaci ve způsobu užívání ICT prostředků. [5][6]

Organizace NIST (National Institute of Standards and Technology) ve své publikaci z roku 2011 definovala devět bodů. Dle jejich mínění tyto oblasti budou mít dlouhodobý význam, a to nejen ve veřejném modelu: [6]

Governance

Samotná organizace by měla dohlížet na dodržování stanovených zásad, postupů a standardů při vývoji aplikací i cloudu. Během návrhu, implementaci, testování, užívání a následného monitoringu nasazených služeb. Praktická jednoduchost při zřizování cloudových služeb usnadňuje osvojení nového prostředí, ale i tak by se nemělo na tyto kontrolní mechanismy zapomínat.

Compliance

Za každé situace je dodržování veškerých zákonů, regulací, standardů a různých nařízení zodpovědností samotné organizace. Zákony a nařízení se mohou lišit na národní, státní či lokální úrovni, a to z této oblasti činí potencionální problém pro samotný cloud computing. V zásadě jde zejména o to, kde jsou využívaná datacenta fyzicky umístěna.

Trust

Při přechodu do cloudu organizace přenechává přímou kontrolu nad mnoha oblastmi bezpečnosti a ochrany osobních údajů poskytovateli daných služeb a vkládá tak do něj velkou důvěru. Někdy možná i nevědomě. Je vhodné užitá opatření znát a ujistit, že jsou aplikována správně a v souladu s našimi potřebami.

Architecture

Použitá HW a SW architektura se může mezi různými poskytovateli a modely nasazení značně lišit. Návrh a implementace přerozdělování prostředků, škálovatelnosti a další pou-

žitých logických prvků. Aplikace jsou vyvíjené prostřednictvím webových prostředí, kdy vzájemně komunikuje více komponent prostřednictvím svých programových prostředí. Virtuální stroje slouží pro nasazení IaaS nebo velmi podobně realizovaných cloudových úložišť. Samotné pochopení toho, co se skrývá uvnitř, a je zároveň podstatou nabízených služeb je velmi důležité.

Identity and Access Management

Pro zabránění neautorizovaným přístupům ke službám musí uživatelé ověřit svoji identitu. Komplikací při přechodu do cloudu může být nekompatibilita stávajícího systému pro správu identit a přístupů. Možností jak nekompatibilitu řešit je však více. Hlavní je se ujistit, že použité nástroje pro autentizaci, autorizaci a další procesy spojené se správou identit a přístupů jsou pro naší organizaci vyhovující. Bariéra v této oblasti může samotný přechod či propojení s on-premise řešením prodloužit, prodražit a někdy i znemožnit.

Software Isolation

Jedním ze základních prvků cloud computingu je sdílené prostředí a flexibilní přidělování výpočetních prostředků jednotlivým uživatelům (agl. tenant). Toto prostředí je tvořeno abstrakcí HW prostředků do celků, které jsou následně přerozdělovány. Fyzicky tedy mohou mít různí uživatelé data na stejných pevných discích, využívat stejnou operační paměť, apod. Pro samotnou izolaci jednotlivých zákazníků se využívá velmi důkladná logická izolace. U IaaS například provozem více virtuálních strojů na jednom fyzickém serveru. U PaaS a SaaS je možné sdílet prostředky jiným způsobem. Například u SaaS se často nevyužívají virtuální stroje, ale jedna logická instance dané aplikace, která je schopná obsloužit mnoho uživatelů a přitom se ji přidělují prostředky dle aktuální potřeby.

Je vhodné si osvojit virtualizační a další logické izolační techniky, které poskytovatel využívá a ujistit se, že pro naše záměry to není zásadní problém.

Data Protection

Jak bylo již zmíněno v předchozím bodě, data jsou ve většině případů uložena ve sdíleném prostředí, které využívají další subjekty. Pokud jsou všechna potřebná opatření správně aplikována, neměli bychom tuto situaci vůbec pocítit. Je dobré si ověřit, jsou-li nástroje na správu dat u našeho budoucího CSP pro nás vhodné. Zdali disponuje možnostmi pro správu přístupu, zabezpečení dat při uložení, přenosu, zpracování. Například jaké formy šifrování jsou aplikovány, a to zejména jsou-li naše data citlivého charakteru.

Availability

Dostupnost je často v SLA vyjádřena a garantována v procentech. CSP tím udává, kolik procent času CSP zaručuje funkčnost (dostupnost) svých služeb. Ve většině případů potřebujeme být dostupní neustále a každý výpadek je problém. Výpadky mohou být dočasné či permanentní. DoS útoky, výpadky HW a přírodní katastrofy jsou hrozby, které se týkají nejen cloudu, ale i tradičního on-premise řešení. Pokud si vše řešíme sami, zařizujeme si i zálohy a obnovy dat či plány pro disaster recovery[3]. V cloudu ale většinou pro tyto případy přebíráme již nastavené nástroje a procedury. Je zapotřebí si tyto nástroje a procedury osvojit a ověřit si vhodnost těchto řešení pro nerušený provoz našich služeb.

Incident Reponse

Každý útok může mít následky a jejich rozsah je závislý na nastavených procesech pro zvládnutí těchto incidentů. Aplikace, operační systém, síť, databáze, systém rozložení zátěže, IDS[4] a další části cloud computingu generují protokoly událostí. Ty většinou plně spravuje právě poskytovatel služeb. Při ověřování a analýze útoků, sběru dat z incidentů, nápravě problémů a obnově služeb hraje tedy CSP zásadní roli. Komplexnost cloud služeb vyžaduje mezi CSP a uživatelem jeho služeb pro úspěšné zvládnutí těchto situací co nejužší spolupráci. Nastavené procedury řešení těchto incidentů by měly našim potřebám vyhovovat. Přehled incidentů a jejich řešení by mělo být transparentní a příslušné informace dostupné po celý průběh řešení. Uživatel by měl mít možnost na řešení s poskytovatelem spolupracovat v závislosti na předem stanovených rolích.

1.1.2 Největší hrozby

Jak již bylo řečeno, cloud nám přináší mnohé výhody, se kterými bohužel přichází i druhá strana mince ve formě rizik, kterým musíme čelit. Identifikovat bezpečnostní hrozby je velmi individuální záležitost a proto jsem se rozhodl zpracovat sérii reportů od Cloud Security Alliance (dále CSA)[5], které jsou základem pro tuto část rešerše.

---

[3] Distaster Recovery Plan - Postupy, jak v co nejkratším čase, s minimem výdajů a rizik obnovit chod kritických aplikací.
[4] IDS - Systém pro odhalení průniku
[5] Cloud Security Alliance (CSA) je přední světová organizace věnující se definování a zvyšování povědomí o osvědčených postupech pro zajištění bezpečného prostředí cloud computingu. www.cloudsecurityalliance.org

Účelem těchto reportů je poskytnutí potřebného kontextu řízení rizik při osvojování cloudových strategií. Spolu s těmito dokumenty o rizicích doporučují také využít "Security Guidance for Critical Areas in Cloud Computing" a "Security as a Service Implementation Guidance". Tyto dokumenty se často používají jako katalog nejlepších postupů pro zabezpečení cloud computingu.

Základem pro úspěšné zvládnutí rizik v jakékoli oblasti je pochopení jejich podstaty. Přesně tak k tomu přistupuje CSA nejen „Top Threats" dokumenty, ve kterých se snaží zprostředkovat aktuální informace pro tuto oblast. [3]

První report s názvem Top Threats to Cloud Computing v1.0 byl vydán v roce 2010. Experty z CSA bylo identifikováno 9 hrozeb:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

Zaměřili se na oblasti, které jsou díky samotné povaze cloud computingu velmi specifické, nebo právě klíčovými vlastnostmi cloud computingu mají větší význam.

Členové interní komise CSA sice jednotlivá rizika subjektivně ohodnotili, ale kumulativní hodnocení nebylo považováno za dostatečně přesvědčivé na to, aby toto pořadí mohlo být publikováno. Považovali za nutnost angažovat širokou odbornou veřejnost pro ohodnocení vážnosti jednotlivých rizik. Pomocí interního hodnocení si, alespoň dle jejich slov, ověřili správnost výběru rizik pro současnou situaci v této oblasti. V dalších verzích reportu s nimi budou tedy dále pracovat.

V tomto dokumentu také zmiňují, že výběr vhodných bezpečnostních mechanismů vyžaduje znalost cílového prostředí. Například v případě nasazování aplikace pomocí PaaS je pro nás hlavní starostí zabezpečení příslušného API[6].

[6] Viz 1.1.2.3

Druhý report z roku 2013 nese název The Notorious Nine: Cloud Computing Top Threats in 2013. V tomto případě již seznam rizik nebyl realizován pouze samotnými experty z CSA. Pro získání profesionálního pohledu na nejzranitelnějších oblasti cloud computingu byl proveden průzkum mezi experty v tomto odvětví. Na základě tohoto průzkumu a vlastní expertízy následně v CSA sestavili výsledný „Top Threats“ dokument pro rok 2013. Metodika průzkumu dle CSA zaručuje, že zvolená rizika skutečně odpovídají oblastem, které toto odvětví nejvíce sužují. Byly identifikovány, a dle vážnosti seřazeny, tyto hrozby:

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issue

Šest ze sedmi hrozeb z roku 2010 zůstalo stejných, pouze se u některých položek mírně pozměnil název. V seznamu byl přejmenován bod Uknown Risk Profile na Insufficient Due Diligence a přibyl bod Denial of Service. Hrozba Data Loss or Leakage byla rozdělena na Data Breaches a Data Loss.

Třetí a nejaktuálnější dokument typu „Top Threats“ byl publikován koncem února roku 2016 pod názvem „The Treacherous 12 Cloud Computing Top Threats in 2016“. Zpráva reflektuje aktuální názor expertů v CSA komunitě na v současnosti největší hrozby v cloud computingu. Z mnoha bezpečnostních otázek se tento report zaměřuje na 12 specifických oblastí, které vycházejí ze samé povahy cloud computingu. Postup sestavení žebříčku byl stejný jako u dokumentu z roku 2013. Základem je tedy průzkum v tomto odvětví a následná zpracování dat skupinou lidí pro „Top Threats“ z CSA. Na základě provedeného průzkumu byly zkoumané oblasti seřazeny dle závažnosti. StejnouTedy stejná metodika jako v předchozím dokumentu.

Stejnou metodikou, jako v předchozím dokumentu z roku 2013, byly identifikovány a dle závažnosti seřazeny následující hrozby:

1. Data Breaches

2. Insufficient Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues

Z předchozí verze reportu zůstalo všech 9 položek, pouze jedna se přejmenovala. Konkrétně Abuse of Cloud Services (2013) na Abuse and Nefarious Use of Cloud services.

Poslední seznam nezávažnějších hrozeb se rozšířil o 3 položky. Jsou umístěny na 2., 4. a 5. místě.

To by bylo pro základní přehled o hrozbách vše. V následujícím textu se podíváme na použitou metodologii sestavení tohoto reportu a na jednotlivé položky ze seznamu pro rok 2016.

Metodologie tvorby reportu „Top Threats“ pro rok 2016

Výzkum byl proveden ve dvou hlavních fázích, kdy byly jako hlavní nástroje využity ankety a dotazníky.

V první fázi pracovní skupina sestavila seznam 20 bezpečnostních hrozeb. Základem bylo 8 hrozeb identifikovaných v reportu vydaném v roce 2013. Přidali dalších 12 potencionálních rizikových oblastí a vše bylo konzultováno s jednotlivými členy pracovní skupiny. Nejprve uvedli důležitost jednotlivých položek pro jejich organizace a následně mohli také navrhovat další možné položky do připravovaného seznamu. Po analýze a zvážení všech získaných informací sestavila pracovní skupina seznam 13 nejvýznačnějších bezpečnostních obav v cloudu.

V druhé fázi výzkumu bylo hlavním cílem tento užší seznam seřadit dle závažnosti jednotlivých oblastí. Pro zachycení názorů dotazovaných subjektů bylo využito následující Likertovo škálování[7]:

1 - Irelevantní

2 - Mírně relevantní

3 - Relevantní

4 - Velmi relevantní

Každá položka seznamu byla ohodnocena průměrným bodovým ziskem a na základě těchto průměrů byl sestaven žebříček. Oblast na posledním místě byla prakticky ohodnocena jako nejméně závažná a byla ze seznamu tedy vypuštěna. Zbylo tedy 12 nejzávažnějších hrozeb.

Na této studii se v pracovní skupině podílelo 271 lidí, odborníci z praxe. To také dokazuje nejhojnější zastoupení zaměření členů pracovní skupiny (mohli volit více oblastí najednou):

- Bezpečnostní specialista - 87,33 %
- Softwarový specialista - 12,22 %
- Síťový specialista - 9,95 %

Veškeré hrozby z tohoto průzkumu se dotýkají všech modelů nasazení (SaaS, PaaS, IaaS). [4]

1.1.2.1 Data Breaches

Jako nejzávaznější problém byl identifikován únik či narušení integrity dat. V dokumentu Top Threats pro rok 2016 CSA popisuje tento bod jako incident při kterém jsou citlivá, chráněná nebo důvěrná data zveřejněna, prohlížena, ukradena či použita osobou, která k tomu není oprávněna. Data jsou v dnešní době pro firmu jedním z nejcennějších aktiv, a

[7] Likertovo škálování se využívá pro měření postojů a názorů lidí. Pro jednotlivé hrozby z předloženého seznamu dotazovaný subjekt označil na čtyřbodové stupnici míru relevantnosti dané hrozby pro jeho organizaci.

přitom o ně můžeme snadno přijít. A to například cíleným útokem, lidskou chybou nebo nedostatečnými bezpečnostními opatřeními. [4]

Oproti on-premise řešení má cloud svá přirozená specifika, která mohou v některých případech zvýšit riziko odcizení či narušení integrity dat. Zaměstnanci poskytovatele služeb, další subjekty, které poskytovatel využívá nebo samotné sdílené výpočetní prostředky. Jedna z hlavních předností cloudu může být při chybném navržení sdíleného prostředí velkým rizikem. Při kombinaci s chybně navrženou aplikací může útočník získat přístup k datům ostatních účastníku sdílené prostředí nejen v rámci jednoho fyzického serveru. [3]

Nedostatečná autentizace[8], autorizace[9] a zaznamenávání (audit) přístupů. Nekonzistentní použití šifrovacích a softwarových klíčů. Legislativní a politické problémy související s umístěním datacentra s jeho spolehlivost závisející na Disaster Recovery[10] scénářích. To jsou problémy, které sužují nejen cloud. [7]

Samotné šifrování dat může zmírnit dopad v případě úniku dat, ale může zafungovat i jako prevence před útoky. Šifrování, anebo i pouhé hašování[11] kritických údajů snižuje hodnotu dat v očích potencionálního útočníka, jelikož data se nedají tak lehce využít v jeho prospěch. [8]

Dopad na samotnou organizaci při úniku závisí na povaze a citlivosti napadených dat. V mnoha zemích zákony a různé předpisy přímo organizacím nařizují zajistit dostatečnou ochranu citlivých informací proti zneužití. Dojde-li k narušení bezpečnosti dat, mohou firmy čelit velkým finančním pokutám, soudním sporům a mimo jiné velmi utrpí samotné jméno dané organizace. [4]

1.1.2.2 Insufficient Identity, Credential and Access Management

V reálném životě jsou situace, kdy musíme ověřit svou identitu. Na úřadě občanským průkazem, ID kartou pro přístup do omezených prostor či například heslem pro vyzvednutí balíčku. Totéž platí takřka pro každý informační systém, pro který je důležitá i přijatelná

[8] Proces ověření identity subjektu
[9] Proces získání souhlasu k provedení dané operace či povolení přístupu do určité oblasti.
[10] Pojem Disaster Recovery znamená (přinejmenším ve světě IT) obnovu po havárii. Přesněji vyjádřeno, jedná se o předem připravený scénář, který vede k obnově infrastruktury po nastalé havárii - ať již fatální havárii hardware nebo software způsobené lidským faktorem, živelnou katastrofou nebo jiným selháním.
[11] Hašovací funkce - matematická funkce (resp. algoritmus) pro převod vstupních dat do malého čísla (haš).

míra jistoty, že přistupující uživatel je skutečně tím, za koho se vydává. V mnoha oblastech již dávno nestačí pouze jméno a heslo. V případě bankovních aplikací to mohou být certifikáty a v podnikové sféře tuto oblast řeší zejména více-faktorová autentizace. [9]

Klíčovým prvkem při zabezpečení podnikového prostředí je kvalitně řešená správa identit a přístupů[12]. Jde zde o několik úzce provázaných technologií, jejichž prvky se kombinují dle potřeb konkrétního prostředí, a tudíž mají projekty vysokou variability. [10]

Systém se skládá ze 3 základních technologií: [11]

- **Adesářová služba** - Udržuje centrální databázi uživatelů
- **Systém řízení přístupů** - Provádí centrální autentizaci, základní autorizaci, zaznamenávání (audit) přístupů, atd.
- **Provisioning systém** - Zabezpečuje správu uživatelské databáze, synchronizaci, řídí bezpečnostní politiku, atd.

Kromě IAM je velmi důležitá již zmíněná více-faktorová autentizace, jejíž faktory jsou: [9]

- **Znalost** - Informace, kterou uživatel zná, nebo se mu sdělí
  - Přihlašovací jméno a heslo (PIN k platební kartě, PIN k SIM kartě, …)
- **Vlastnictví** - prostředek, který má k dispozici pouze daný uživatel
  - Mobilní telefon, hardwarový token[13] (SIM karta, občanský průkaz, …)
- **Biometrie** - charakteristiky nositele
  - Otisk prstu, autentizace hlasem (CAPTCHA[14], …)

V internetovém bankovnictví, přihlašování do Google účtu[15] nebo Windows Azure[16] služeb se používá dvoufázové ověřování. Kromě standardní procedury se jménem uživatele a hesla je zapotřebí zadat do příslušné aplikace kód, který obdrží uživatel například prostřednictvím SMS nebo telefonátu[17].

---

[12] IAM - Správa uživatelů, rolí a oprávnění
[13] Hardwarový token - jednoúčelový hardware v držení uživatele - data z něj čte, nebo jej zapojí do čtečky.
[14] CAPTCHA - používá se při ověření „jsem člověk“ - odlišení skutečného uživatel od robotů. Řešení je sice jednoduché, ale těžko se algoritmizuje. Přepis kódu z obrázku, „Kolik je 2 + 3?, atd.
[15] https://www.google.cz/ - Ochrana soukromí - Dvoufázové ověření
[16] https://azure.microsoft.com/cs-cz/ - Produkty - Správa identit a přístupů - Multi-Factor Authentication
[17] Během telefonátu je kód reprodukován syntetickým hlasem.

Nezbytná je implementace periodické a automatické výměny šifrovacích klíčů, certifikátů a změna hesel. Samotným základem je však bezpečné heslo. Dostatečná délka, použité znaky (velké, malé písmeno, číslo, speciální znak, interpunkční znaménko, …), atd. Dostatečně silné heslo by mělo být samozřejmostí v případě, kdy jiná opatření nejsou aplikována. Další používanou možností je šifrování pevných disků na uživatelských stanicích. [4][12]

Pokud je některá z výše zmíněných oblastí nedostatečně řešená, pravděpodobnost úniku či narušení integrity dat roste.

Výše zmíněné oblasti platí nejen pro cloud ale samozřejmě i pro on-premise řešení, ve kterém si ale rozdíl od cloudu můžeme konkrétní řešení zvolit sami.[4]

Centralizovaný mechanismus skladování kritických dat (např. hesla, soukromé klíče, databáze zákazníků) je pro útočníky nesmírně lákavý a hlavně hodnotný cíl. Při volbě podobného centralizovaného úložiště je zapotřebí zvážit a porovnat pohodlí oproti potencionálnímu riziku, které toto řešení může přinést.

V závěru k tomuto bodu v reportu „Top Threats“ pro rok 2016 uvádějí, že podvratní uživatelé s legitimním přístupem (oprávněním) uživatelů, administrátorů či vývojářů mohou napáchat zásadní a nevratné škody. Dle úrovně oprávnění mohou číst, upravovat, mazat nebo vynést informace. Manipulovat s nastavením systémů, odposlouchávat přenášená data či nasazovat škodlivý software, který se tváří jako legitimní součást systému. [4]

Každý pro nás hodnotný majetek si chráníme, jak nejlépe umíme, a proto bychom měli i zde věnovat velkou pozornost klíčovým systémům, jimiž správa identit a přístupů bezesporu je. Selhání v této oblasti může mít katastrofální následky.

1.1.2.3 Insecure Interfaces and APIs

Pro správu a přístup ke cloudových službám nabízejí jejich poskytovatelé sadu uživatelských rozhraní (UI) nebo rozhraní pro programování aplikací (API). Prostřednictvím těchto nástrojů se realizuje provisioning, správa, orchestrace a monitoring. [4]

Právě na zabezpečení těchto základních API závisí dostupnost a bezpečnost samotných koncových služeb. Tato prostředí musí být navržena tak, aby odolala náhodným i úmyslným pokusům o obcházení bezpečnostních opatření.

UI a API patří do částí sytému, které jsou vystaveny externím vlivům, jelikož jsou přístupné i mimo důvěryhodné prostředí. Adekvátní bezpečnostní opatření jsou tedy namístě, jeli-

kož jsou tyto části systémů v první linii obrany. Spoléháním se na nedostatečně navržená prostředí a API se organizace vystavují bezpečnostním problémům souvisejících s důvěryhodností, integritou, dostupností a odpovědností. [4]

Zatímco zajištění implementace těchto opatření je na straně poskytovatele, je velmi důležité, aby uživatelé na straně zákazníka těmto nástrojům porozuměli a uměli je správně používat.

1.1.2.4 System and Application Vulnerabilities

Systémové a aplikační chyby[18] oslabují systém a dávají útočníkům příležitost k proniknutí za účelem získání dat, ovládnutí samotného systému nebo narušení činnosti služeb. Pokud se tyto chyby týkají samotných komponent operačního systému, tedy kernelu, systémových knihoven a aplikačních nástrojů, týká se hrozba všech dat a služeb souvisejících s tímto operačním systém.

Musíme si ale uvědomit, že tento typ hrozeb nesouvisí pouze s cloudem. Bugy jsou tu s námi od vynalezení počítačů, ale s příchodem sdílení zdrojů a jejich využívání různými organizacemi vnikly nové formy hrozeb. Data více organizací mohou být fyzicky umístěna na stejném disku a využívat stejnou sdílenou paměť a další zdroje.

Důsledky útoků na tato zranitelná místa mohou být značné, ale pravděpodobnost jejich nastání lze zmírnit již základními opařeními. Pravidelné monitorování systémů, sledování aktuálních hrozeb a včasné aplikování aktualizací a záplat pro zavření bezpečnostních mezer. Rizika je samozřejmě nejlepší eliminovat již v zárodku. Kladen by tak měl být kladen velký důraz na kvalitní návrh a architekturu základních částí cloudu a přístupových oprávnění.

Pokud nebudeme ze systému odstraňovat chyby, může být dopad takto nezáplatovaného systému velký a také nákladný. Přitom na rozdíl od nákladů vzniklých po úspěšných útocích je nákladová stránka samotných oprav chyb zanedbatelná. V případě vysoce regulované organizace (např. vládní a finanční instituce) je důležité rychlé zvládnutí záplatování

[18]V angličtině využíván výraz „bug“

objevených chyb. Vhodné je také zavedení krizových scénářů pro eliminaci nebezpečí pro období od doby objevení chyby (známo jako „zero-day“[19]), do chvíle nasazení řešení.

Dále je vhodné stavit si priority pro jednotlivé části systému a samozřejmě přednostně řešit ty kritické. Vše by mělo být důkladně zdokumentováno pro pozdější analýzy a možnost, se podobným situacím v budoucnu vyvarovat.

1.1.2.5 Account Hijacking

Při neoprávněné vniknutí do účtu mohl získat útočník informace pro přístup vícero způsoby. Nejčastěji se pro proces přihlášení používá pouze uživatelské jméno nebo e-mail a heslo. Uživatelské jméno může být dostupné v rámci organizace nebo veřejně a tedy jediným bezpečnostním prvkem je samotné heslo, jehož sílu si může poskytovatel dané služby i částečně vynutit. Mělo by však být zájmu samotného uživatele, aby do účtu neměl přístup nikdo jiný. V případě vniknutí do účtu může dojít k jeho zneužití ke škodlivým aktivitám s „podpisem“ původního uživatele.

Heslo lze získat například pomocí prostého hádání, podvodem, phishingem[20] nebo cíleným útokem na databáze uživatelů s využitím chyb v systému. Pokud jsou hesla uložena v čitelné podobě, je tu problém. Totožné přihlašovací údaje jsou uživateli často používána napříč různými službami, což zvyšuje negativní dopad v případě jejich odcizení. [4]

Někdy si uživatelé hesla zapisují, aby je nezapomněli, lepí na lístečcích na počítač a podobně. V tomto případě sebelepší heslo nepomůže. Podobně někteří řeší PIN k platební kartě a lísteček s tímto kódem nosí společně s kartou v peněžence. Více nahrát zloději již nemůžeme.

Neoprávněná vniknutí do účtů jsou běžná, avšak s příchodem cloudu se objevila nová forma hrozeb. Pokud útočník získá naše přístupové údaje, může odposlouchat naše aktivity a transakce, manipulovat s daty či přesměrovat klienty na nelegitimní místa. Z našeho účtu se může stát pro útočníka základna, ze které může vést následné útoky. Samotné organizace by si měly být těchto možných útoků vědomy stejně tak jako ochranných strategií zná-

[19] Zero-day attack je útok zneužívající chyby v SW, jenž není všeobecně známá a zatím pro ni neexistuje záplata.
[20] Phishing - podvodná technika používaná k získávání citlivých údajů v prostředí internetu.

mých jako „Defense in depth“[21]. To zejména proto, aby zabránili možným škodám a soudním sporům vyplívajících z průniku do systému. [4][13]

Ačkoli je tato doba a cloud o sdílení, přístupové údaje k účtům bychom neměli ostatními sdílet. Účet v IT vyjadřuje naši identitu jako občanský průkaz v reálném světě.

Všude kde je to možné zavádět více-faktorovou autentizaci. Veškeré aktivity na účtech a účty samotné by měli být monitorovány, aby byly jednotlivé aktivity vysledovatelné k daným osobám.

Na závěr ve svém dokumentu CSA zmiňuje, že zneužití účtu je stále významná hrozba. S odcizenými přístupovými údaji se mohou útočníci často dostat ke kritickým částem cloudových služeb, a tím ohrozit důvěryhodnost, integritu a jejich dostupnost. Nesmíme opomenout fakt, že tímto způsobem mohou být odcizena data, poškozeny služby, systém a také pověst samotné společnost. [4]

1.1.2.6 Malicious Insiders

Pojem Malicious Insider lze definovat následovně:

> „A malicious insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.“
>
> [14]

Dále v knize zmiňují tři identifikované modely vnitřních hrozeb:

- **IT sabotáž** - Využití IT prostředků pro přímé poškození organizace nebo osoby.
- **Krádež duševního vlastnictví** - Využití IT prostředků ke krádeži duševního vlastnictví. Lze sem zařadit průmyslovou špionáž realizovanou vlastními lidmi.

[21] Defense in depth - vícevrstvé bezpečnostní mechanismy zvyšují bezpečnost systému jako celku.

- **Podvod** - Využití IT prostředků pro neoprávněnou úpravu, doplnění nebo smazání firemních dat pro osobní zisk či krádež informace vedoucí k trestné činnosti s identitou (krádež identity, podvod s platební kartou, …).

Výše zmíněné případy jsou zajisté prováděny úmyslně, avšak v některých případech to může být provedeno neúmyslně. Lidé s dostatečným oprávněním mohou ovlivnit důvěryhodnost, dostupnost a integritu podnikových dat. [14]

Správa identit a přístupů je velmi důležitá, avšak pokud je onou černou ovcí například systémový administrátor, jsou potenciálně ohrožena citlivá data. Čím blíže má daná osoba k základu cloudové infrastruktury (od SaaS, přes PaS až samotnému IaaS), tím je větší šance, že bude mít přístup k důvěrným informacím a možnost výrazně uškodit.

Samotná implementace šifrování nemusí být proti těmto útokům dostatečným opatřením, pokud jej realizuje poskytovatel cloud služeb (CSP). To platí i tehdy, jsou-li klíčové systémy pro správu těchto zabezpečení mimo datové úložiště organizace, tedy na separátním úložišti CSP. Dále v dokumentu „Top Treats“ pro rok 2016 zmiňují, že zásadní je také monitoring a záznam veškerých procedur realizovaných samotným CSP. Černou ovcí může být právě zaměstnanec poskytovatele služeb a měla by zde být tedy realizována dostatečná opatření jako segregace povinností, omezení přístupů dle rolí a dostatečný monitoring a záznam aktivit.

Jako nejčastější důvody pro tyto sabotáže byly při průzkumu společnosti Verizon identifikovány finanční zisk a podvod. Zejména díky zneužití svěřených pravomocí (55 % ze všech incidentů). Tedy ani správně realizovaný systém pro přístupy a oprávnění nemusí všemu zabránit. [15]

Samotná „hrozba zevnitř“ nemusí být vždy úmyslná a zaměstnanec může například nahrát důvěrné informace týkající se zákazníků na veřejné úložiště s fyzickým umístěním datacentra v jiné zemi, které podléhá odlišné právní úpravě ochrany osobních údajů.

1.1.2.7 Advanced Persistent Threats

Jako sedmá hrozba je v seznamu APT, což lze volně přeložit jako *přetrvávající pokročilé hrozby*, které vyjadřují přesně cílené útoky proti konkrétní organizaci nebo osobě. Rozdíl oproti běžným útokům popsal na svém webu Bruce Schneier. Dle něj se tradiční hacker příliš nezajímá o konkrétní cíl, ale jde mu pouze o dosažení svého prvoplánového cíle. Například získání velkého množství čísel a dalších informací k platebním kartám pro finanční

podvod, apod. Bezpečnost vůči těmto druhům útoků je relativní. Dokud je daná organizace zabezpečena lépe než ostatní, tím spíše se jí hacker vyhne a bude se zabývat ostatními. V případě APT je útok cílený a i ta nejlepší úroveň zabezpečení nemusí útočníka od samotného činu odradit. Hlavní je, jestli všechna implementovaná bezpečnostní opatření dovedou pokusy o útok odrazit. Tyto osoby bývají více motivované, zkušenější, dobře financované a mají větší trpělivost. Tím spíše uspějí. [16][17]

Prostřednictvím těchto parazitických forem útoků infiltrují cílový systém a zřídí si opěrný bod v cloudové infrastruktuře, ze které pak mohou vynášet potřebná data. Probíhají po delší dobu, nenápadně a přizpůsobují se napadenému systému tak, aby nedošlo k odhalení.

Popis **APT**:

Advanced techniques - Pro průnik do systému se využívá mnoho pokročilých technik.

Persistent access - Cílem APT je zajistit si trvalý přístup do systému dané organizace.

Do cílového systému musí ale nejdříve hacker prorazit, překonat zabezpečení. Nejlepší cesta je přes potencionálně nejslabší články. V dokumentu „Top Threats“ pro rok 2016 zmiňují například spearphishing[22], přímé hackování, nezabezpečené AP[23] či doručení škodlivého kódu prostřednictvím USB zařízení. Také špatně zabezpečené sítě obchodních partnerů napojené na sítě dané organizace mohou být pro hackera vstupní branou. Jakmile je APT na místě může splynout s běžnou síťovou aktivitou a dosáhnout svých cílů. [4]

APT úzce souvisí s modelem útoku o třech fázích: [18]

V první fázi se shromažďují informace. Pasivně, polo-pasivně a aktivně.

- V pasivním mód se může podařit vyhledat nějaké veřejné i neveřejné informace.
- V módu polo-pasivní může být generován nějaký síťový provoz, ale bez vzbuzení podezření.
- V posledním, aktivním módu může útočník provádět i odvážnější průzkumy (např. skenování portů) pro zmapování cílové sítě.

[22] Spearphishing - Podobné jako phishing, ale útok je zaměřen na konkrétní organizaci pro získání neautorizovaného přístupu k důvěrným informacím.
[23] Access Point - Přístupový bod

V druhé fázi se modelují hrozby, které útočníkovi hrozí a mohly by ho odhalit. Mapuje se cílová síť a hledají se nevhodnější způsoby a techniky pro infiltraci cíle. Poslední fáze je ve znamení provedení samotného útoku s využitím nalezených zranitelností.

IT oddělení by měla sledovat aktuální dění na poli kyberbezpečnosti a mít přehled o aktuálních hrozbách. Tyto formy útoků může být těžké identifikovat, ale lze jim předcházet proaktivním přístupem k bezpečnostním opatřením.

V „Top Threats" dokumentu pro rok 2016 také zdůrazňují, že za většinou útoků stojí chyba uživatele. Prvotní obranou je tedy osvěta samotných zaměstnanců a přidružených osob v této oblasti. Boj proti APT je však komplexní záležitost, která vyžaduje pokročilé bezpečnostní opatření, správu procesů, plán reakcí na různé incidenty a samozřejmě školení IT personálu. To vše sice může vést ke zvýšení nákladů na bezpečnost, avšak v porovnání s možnými ekonomickými důsledky úspěšného APT je to zanedbatelná položka.

1.1.2.8 Data Loss

Data jsou v dnešní době pro moderní společnosti nejhodnotnější aktivem, které mohou vlastnit. V tomto duchu to je popsáno i v knize Principles of Information Security:

> *„Without data an organization loses its record of transactions and/or its ability to deliver value to its customers."*
>
> [19]

A neplatí to je pro velké společnosti, ale i ty malé jsou závislé na datech pro jejich každodenní činnost. Skladový stav, seznamy dodavatelů a zákazníků, objednávky, fakturace, mzdy, finance a mnoho dalšího. Ztráta dat může mít pro organizaci až likvidační následky. Zvláště pokud nejsou zajištěny potřebné nástroje a postupy pro obnovu dat. [4]

Ztráta dat je noční můrou nejen pro zákazníky, ale pro samotné poskytovatele cloudu. Může tak dojít ke ztrátě kreditu poskytovatele a odlivu zákazníků. Tedy ekonomická ztráta až likvidační situace.

Ke ztrátě cenných dat a informací může dojít mnoha způsoby a nemusí být vždy způsobem nějakou formou útoku. Nemusí být vždy cílená. Stačí pár neopatrných klinutí a data mohou

být navždy pryč. Za touto ztrátou není vždy chyba uživatele nebo SW, v horším případě ten důvod může být fyzický.

Havárie HW komponent nebo živelné katastrofy, které postihnou datacentrum hostující příslušné informace. Pokud nebyla přijata adekvátní opatření pro zálohu, zabezpečení kontinuity provozu kritických systémů a připraveny plány pro zotavení po havárii (tzv. Disaster plan), může mít nevinně vyhlížející situace velké následky. Tyto stránky by měl obstarat zejména poskytovatel služeb, ale pokud zákazník ztratí šifrovací klíče, mohou být data ztracena i takto nešťastným způsobem. [4]

Například služba Windows Azure nabízí lokální a „geo" redundanci.[24] V případě lokální redundance jsou data uložena ve třech kopiích v rámci jednoho zařízení. „Geo" redundance obsahuje kromě lokální redundance i další 3 kopie dat v jiné lokaci, v jiné části světa. Možnosti, jak omezit fyzickou ztrátu dat tedy existují, ale nesmíme zapomenout na samotnou lokaci oněch datacenter. Hlavně pokud pracujeme s daty, která podléhají ochraně osobních údajů.

Vzhledem k pravidlům EU o správě a ochraně osobních dat se zničení či poškození těchto dat považuje únik dat. Tyto situace je nutné hlásit úřadům. [4]

1.1.2.9 Insufficient Due Diligence

S příchodem cloud computingu se naskytla nová příležitost jak snížit náklady, zvýšit efektivitu a zesílit současné zabezpečení. Tyto cíle jsou dosažitelné, ale je zapotřebí plně porozumět tomuto prostředí Je zapotřebí ověřit, jestli nabízená možnost je pro nás ideální a zvládne všechny naše potřeby. Pokud tuto část, známou jako Due Diligence („hloubková prověrka") zanedbáme a samotný přechod uspěcháme (prověrka nebude dostatečná), může to mít zásadní následky. [3][20]

V dokumentu „Top Threats" pro rok 2016 zkoumali tyto oblasti Due Diligence: [4]

- **Komerční** - Pokud pro správu čí zavádění našich služeb či aplikací musí poskytovatel vyvíjet nové systémy a procesy, měli bychom poohlédnout někde jinde. Pokud si toto nemůžeme realizovat sami, anebo je nutná spolupráce se samotným poskytovatelem služby, bude to pravděpodobně pro nás velká komplikace.

[24] https://azure.microsoft.com/en-us/documentation/articles/backup-azure-dpm-introduction/

- **Technické** - Nejsou-li návrháři a architekti dostatečně obeznámeni s příslušnými cloudovými technologiemi, mohou při přenosu aplikací do nového prostředí nastat neznámé provozní a architektonické problémy.
- **Právní** - Jsou-li zpracovávaná data fyzicky umístěna v nám neznámých lokacích, může dojít k porušení právní ochrany. Pokud s daty takové povahy pracujeme, je vhodné vědět, kde příslušná datacentra jsou. Zvláště chceme-li se vyhnout možným právním sporům.
- **Compliance** - Tento bod lze v tomto případě popsat jako soulad procesů a bezpečnostních opatření našeho současného a budoucího řešení. Je nebezpečné přesouvat aplikaci závisející na interních bezpečnostních opatřeních síťové úrovně, pokud cílové prostředí těmito prvky nedisponuje.

Před přechodem na tuto platformu je záhodné se pomocí rozsáhlého Due Diligence důvěrně seznámit s nabízenými možnostmi a pochopit je.

1.1.2.10 Abuse and Nefarious Use of Cloud Services

Díky cloud computingu se i malé firmy mohou dostat k „neomezenému“ objemu výpočetních prostředků, aniž by bylo nutné budovat vlastní drahou infrastrukturu. Bohužel ne každý tuto „sílu“ využije pro ty správné účely. S těmito prostředky je mnohem snazší rozluštit hesla či použité šifrování, provést masivní DDoS útok, hostovat nelegální data či realizovat farmy na luštění CAPTCHA. [3][7]

K těmto službám není těžké se dostat a to i prakticky anonymně. Postačí validní platební karta a v řádu pár minut můžeme služby využívat. V některých případech jsou dostupné i tzv. trial verze zdarma. Někdy jsou limitovány časem, někdy spotřebou výpočetních prostředků. Možností je mnoho. Samotná registrace do podobné služby není podmíněna ověřením identity registrující se osoby, tedy anonymita internetu vlastní je samozřejmostí. [3]

Samotné zneužití cloud služeb je spíše problém poskytovatelů, ale pokud je útok veden ze stejného datacentra, může nadměrné využití výpočetních prostředků ohrozit ostatní uživatele. Bude pro ně tak méně dostupných prostředků. Pokud jsou navíc bezpečnostní opatření nedostatečná, nemusí na nekalé jednání poskytovatel přijít včas.

1.1.2.11 Denial of Service

Je-li obchod zavřený, nevydělává. Je-li webová služba nedostupná, nevydělává. V našem zájmu je tedy udržovat naše služby nabízené prostřednictvím internetu neustále online.

Nezáleží na tom, jestli služby běží na firemním serveru v prostorách firmy, nebo kdesi v datacentru na druhém konci světa. Hlavním cílem je být dostupný. Pokud tomu tak není, přicházíme o zákazníky a reputaci. Snažíme se tedy udržovat naše služby nestále dostupné, ale vše může zhatit DoS či DDoS útok.[25] Další možnou variantou je DoS útok na aplikační úrovni, kdy je využito samotné logiky aplikace, aby například upadla do nekonečného zacyklení, nebo využívala enormní množství výpočetních prostředků. [21]

Pomocí této formy útoku lze samozřejmě zpomalit až vyřadit z provozu i běžné on-premise řešení, ale útok cloud s sebou přináší i další možné negativní dopady.

V případě on-premise řešení máme omezené výpočetní prostředky a v případě jejich vyčerpání dojde k pádu serveru a úplné nedostupnosti služby. V případě cloudu k tomu nemusí dojít tak snadno. Jednou ze základních výhod je flexibilní přidělování výpočetních prostředků a nemusí tak útok službu vyřadit úplně. Může však dojít k extrémní konzumaci procesorového času, operační paměti, diskového prostoru, apod. Pokud platíme právě dle spotřebovaných výpočetních prostředků, mohou se škody po takovém útoku vyšplhat velmi vysoko.

V případě různých forem nejen DoS útoků ale není postižen pouze cíl. Mohou být postiženi uživatelé tohoto sdíleného prostředí. [2]

1.1.2.12 Shared Technology Vulnerabilities

Služby založené na cloud computingu jsou dodávány flexibilně za pomoci sdílené infrastruktury, platforem a aplikací. Za tím vším stojí komponenty (např. CPU, GPU, HDD), které nemusí být navrženy pro potřebu silných izolačních vlastností mezi jednotlivými uživateli takto sdílené prostředí. Tato zranitelnost se týká všech modelů nasazení (IaaS, PaaS, SaaS). Tento nedostatek kompenzuje virtualizační hypervisor tím, že zprostředkovává komunikaci mezi hostovanými operačními systémy a fyzickými výpočetními prostředky. Naneštěstí i toto řešení není plně spolehlivé a i tak je vhodné implemetovat strategie Defense in depth. Musí být zajištěno silné rozčlenění prostředků, aby se uživatelé svými operacemi neovlivňovali navzájem. [4][7]

[25] DoS vs DDoS - Při DoS útoku je využíván jeden počítač a jedno internetové připojení. Naopak při DDoS je skupinový útok realizován mnoha počítači, většinou s fyzickým umístěním po celém světě.

Ohrožení byť jen jedné části této sdílené technologie může ohrozit celé sdílené prostředí a ovlivnit tak všechny zúčastněné uživatele. Už jen toto je pádný důvod zamezit nepovolaným osobám v přístupu do těchto systémů. Například již dříve zmíněnou více-faktorovu autentizací u všech zúčastněných subjektů, implementací HIDS[26]a NIDS[27](pro aplikaci minimálního nutného oprávnění, segmentaci a monitoring na interních sítích). [4]

1.1.2.13 Vývoj jednotlivých hrozeb v čase

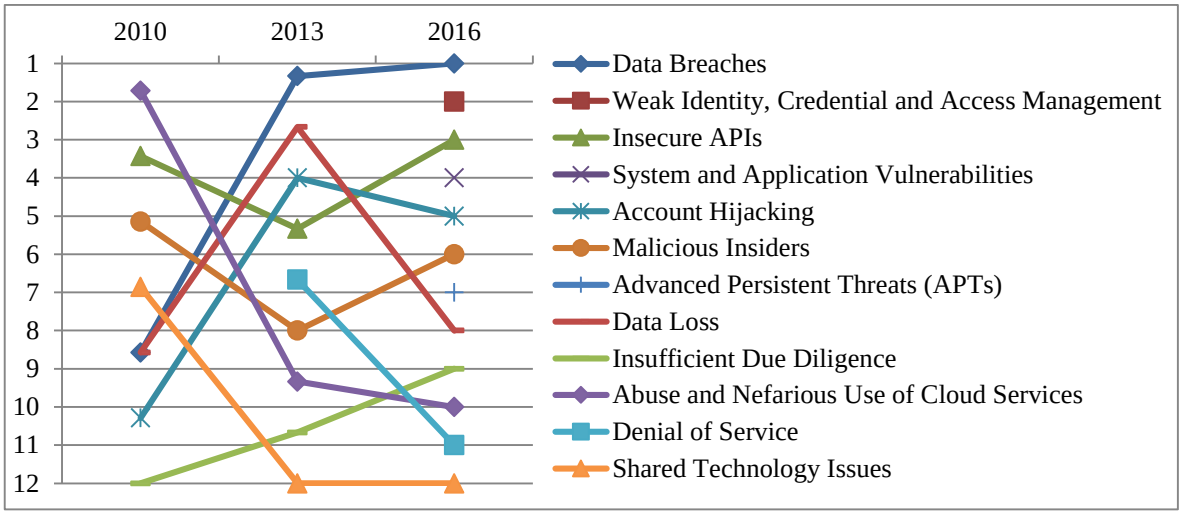
Jak již bylo dříve zmíněno, pro identifikaci bezpečnostních hrozeb bylo využito tří reportů typu „Top Threats“ od CSA. A to konkrétně rok 2010, 2013 a 2016. Aktuální verze byla publikována koncem února roku 2016.

Naneštěstí samotný vývoj v žebříčku nelze jednoduše zachytit, jelikož v každém vydání je počet sledovaných oblastí jiný. Přesto jsem s úpravou zobrazil vývoj v tabulce 1 a grafu 1.

Pořadí	Hrozba	2010	2013	2016
1	**Data Breaches**	5	1	1
2	**Weak Identity, Credential and Access Management**			2
3	**Insecure APIs**	2	4	3
4	**System and Application Vulnerabilities**			4
5	**Account Hijacking**	6	3	5
6	**Malicious Insiders**	3	6	6
7	**Advanced Persistent Threats (APTs)**			7
8	**Data Loss**	5	2	8
9	**Insufficient Due Diligence**	7	8	9
10	**Abuse and Nefarious Use of Cloud Services**	1	7	10
11	**Denial of Service**		5	11
12	**Shared Technology Issues**	4	9	12

Tabulka 1 - Vývoj identifikovaných hrozeb v čase

[26] HIDS - Host-based intrusion detection sytem
[27] NIDS - Network Intrusion Detection Systems



Graf 1 - Vývoj identifikovaných hrozeb v čase

Výchozí počet položek byl 12, dle reportu pro rok 2016. Pro srovnání ostatní reportů bylo provedeno následující:

Počet položek pro rok 2016 byl vydělen počtem pro příslušný rok. Po získání koeficientů pro oba předchozí ročníky byly příslušné pozice vynásobeny a získány pozice vyobrazené na grafu 1. (viz Tabulka 2)

Rok	Počet hrozeb	Rok 2016		Koeficient
2010	7	12	12/7	1,7142857
2013	9		12/9	1,3333333

Tabulka 2 - Výpočet koeficientů

1.1.3 Šifrování

Již z principu cloud computingu dochází k přenosu dat mezi poskytovatelem a zákazníkem prostřednictvím internetu. Prakticky při jakémkoli přenosu dat skrze nezabezpečenou síť by mělo docházet k šifrování. Tento přenos je nutné řádně zabezpečit, aby nedocházelo k odposlechu, změně či poškození dat. Autentizace u webových služeb standardně probíhá pomocí HTTP mechanismů a pro zajištění šifrované komunikace se používá nejčastěji SSL/TLS (např. využití silného algoritmu AES-256, využití proprietárních řešení se nedoporučuje). [22]

V rámci různorodosti uchovávaných dat by se mělo stanovit, je-li nutné šifrovat všechna data. Některá lze chránit jinými způsoby a některá není třeba šifrovat vůbec. Při stanovení

míry zabezpečení je nutné brát zejména v úvahu to, co by se stalo v případě úniku jednotlivých typů dat či co přikazuje zákon. Někdy může postačit v cloudu pouze omezit k některým datům přístup - pro zabránění přístupu neoprávněných uživatelů nebo pro splnění zákonných nařízení.

Šifrování je za cenu komplexnosti a výkonu. Plné šifrování dat, která se zpracovávají, není jednoduché a nabízejí se tak jiné varianty ochrany dat. Zmíněné omezení přístupů nebo například ukládání pouhého hash z důvěrných dat. K ověření správných hodnot postačující a samotná data jsou schována. Spolu se šifrováním přichází i správa šifrovacích klíčů. Klíče by měly být uchovávány v rámci interní sítě a do cloudu pouze odesílány bezpečnou cestou.[28]

Pokud by byla data cloudu šifrována během celého pobytu v prostředí, byl by vyřešen problém bezpečnosti a ochrany údajů. Samozřejmě za předpokladu bezpečně spravovaných šifrovacích klíčů. V tom by ale mohlo v budoucnu pomoci Homomorfní šifrování: []

> *„Budoucnost nám v tomto směru slibuje řešení - tzv. homomorfní šifrování, při kterém se využívá určitých vlastností abstraktní algebry (homomorfismu grup). Zjednodušeně jde o ekvivalenci dvou matematických struktur z hlediska prováděných operací, tj. pokud se povede vytvoření zašifrovaného ekvivalentu nešifrovaných dat tak, aby aritmeticko-logické operace jak nad nešifrovanými, tak nad šifrovanými daty dávaly stejný výsledek, nemusí aplikace a procesor při své práci datům „rozumět" - zdroj data zašifruje, data se přenáší, ukládají i „počítají" zašifrovaně a cíl si data dešifruje. Teoreticky vše funguje, problém je zatím v enormní výpočetní náročnosti.„*
>
> [23]

Výpočetní možnosti se každým rokem zvyšují a homomorfní šifrování může být časem pro cloud praktickou realitou.

[28] https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

1.2 Legislativní a regulační pohled

Při využití vlastních hardwarových prostředků v prostředí organizace nebylo zapotřebí upravovat vnitřní vztahy interními smlouvami. Z přirozené vazby aplikační logiky na hardware a infrastrukturu automaticky vyplývala odpovědnost za provoz aplikace nebo řešení otázek vlastnictví dat. Příslušné servery a samotnou infrastrukturu lze snadno identifikovat. [24]

Cloud computing a virtualizace toto zásadně mění. Data jsou uložena v datacentru na virtualizované infrastruktuře někde na planetě. U většiny významných poskytovatelů s vlastní infrastrukturou není zásadní problém fyzické umístění serverů zjistit a u některých si i můžeme vybrat, v jaké části světa chceme data uchovávat a zálohovat.

Každá smlouva by měla také upravovat předávání dat od zákazníka poskytovateli a naopak. Mělo by být jasně stanoveno, kdo je vlastníkem dat a jak se bude postupovat a nakládat s daty v případě ukončení smluvního vztahu. [2]

Právě kvůli předávání dat do „rukou“ jiného subjektu a případně i do právního prostředí cizího státu, je nutné myslet na legislativní otázky. Jednotlivé aktéry v problematice ochrany osobních údajů popisuje zákon č. 101/2000 Sb. následovně:

- **Subjekt** - Fyzická osoba, ke které se osobní daje vztahují.
- **Správce** - Určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj.
- **Zpracovatel** - Na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje.
- **Příjemce** - Subjekt, kterému jsou osobní údaje zpřístupněny.

Zákon primárně upravuje vztahy mezi různými subjekty a v tomto případě se smluvní strany označují následovně: [29]

- Poskytovatel údajů/uživatel cloudu = správce
- Poskytovatel cloudu = zpracovatel

Z pohledu bezpečnosti je nejčastěji řešeným tématem právě fyzické umístění zpracovávaných dat. Před migrací musíme znát legislativní a regulační požadavky námi zpracováva-

[29] zákon č. 101/2000 Sb. - Zákon o ochraně osobních údajů

ných dat, a na základě toho vybírat poskytovatele, který naše požadavky splňuje. Naštěstí většina významných hráčů na trhu všemi potřebnými opatřeními a zabezpečeními disponují a prokazují to řadou certifikací a auditů. Data bývají často ukládána v několika replikách a někdy v několika různých geografických lokalitách. [22][25]

1.2.1 Smlouva o poskytování cloudu

Cloud computing lze také popsat jako poskytnutí licence a hostingu, kde hosting zahrnuje popis rozsahu služby, SLA a ochranu dat. [27]

Pro licenční smlouvu lze použít tuto definici:

> *„Licenční smlouva je smluvní typ upravený občanským zákoníkem, na jehož základě poskytovatel, který je majitelem práva duševního vlastnictví, poskytuje oprávnění k výkonu tohoto práva nabyvateli, jenž se zavazuje poskytovateli poskytnout poskytovateli odměnu.“*
>
> [26]

Cloudové licence se od běžné licenční smlouvy značně liší a pro základní přehled obou typů je využita následující tabulka:

Běžná licenční smlouva	**Cloudová licence**
Jednorázové poskytnutí licence	Možnost průběžné platby (pay as you go)
Pevný počet licencí (uživatelů, produktů)	Škálovatelnost založená na změně počtu uživatelů a produktů
Většinou nezahrnuje další služby	Zahrnuje služby hostingu - SLA, úprava bezpečnosti a právního režimu nakládání s údaji

Tabulka 3 - Srovnání běžného a cloudového licencování [27]

Rozsah hostingových služeb, neboli distribuční modely, se dělí dle SPI modelu.[30] [31]

- Software jako služba (SaaS)
- Platforma jako služba (PaaS)
- Infrastruktura jako služba (IaaS)

> *„Model SPI se zabývá tím, co je v rámci služby nabízeno. Obvykle je to software nebo hardware, případně jejich kombinace. Každá kategorie řeší jinou problematiku a zpravidla uspokojuje potřeby různých uživatelů.“*
>
> [5]

Základní smluvní záruky v tomto vztahu mezi správcem a zpracovatelem lze popsat následovně:

> *„Smlouva musí přinejmenším stanovovat to, že se zpracovatel řídí pokyny správce a že zpracovatel musí přijmout technická a organizační opatření k náležité ochraně osobních údajů.*
>
> [28]

V dokumentu „Stanovisko č. 05/2012 ke cloud computingu“ uvedla pracovní skupina doporučení pro smlouvy o poskytování služeb cloud computingu. V zájmu právní jistoty by následující doporučení měla smlouva obsahovat (zjednodušeno): [28]

1. Rozsah a podmínky pokynů zákazníka určených poskytovateli, zejména smlouvy o úrovni poskytovaných služeb (SLA) a smluvní pokuty za poskytování služeb v rozporu se SLA.
2. Bezpečnostní opatření, jež musí poskytovatel cloudových služeb dodržovat.

---

[30] Pro rozdělení služeb se nejčastěji používá SPI model, definovaný organizací NIST (National Institute of Standards and Technology) [5]

[31] Pro bližší popis těchto modelů lze použít například mou bakalářskou práci, viz [5]

3. Časový rozvrh a samotný předmět sjednané cloud služby. Rozsah, způsob a účel zpracovávání osobních údajů realizovaného poskytovatelem cloudových služeb, a to včetně typů zpracovávaných údajů.
4. Podmínky navrácení zákaznických dat nebo jejich bezpečné vymazání v případě ukončení smlouvy.
5. Závazek o důvěrném zacházení s daty zákazníka uložených v cloudu.
6. Závazek poskytovatel vůči zákazníkovi (správci) při usnadňování výkonu práv subjektů údajů na přístup ke svým údajům, na jejich opravu a smazání.
7. Závazek poskytovatele služeb, že nepředá údaje třetím stranám, není-li ve smlouvě ustavení o subdodavatelích. Subdodavatelé musí splňovat stejnou úroveň ochrany jako poskytovatel a správce musí být o subdodavatelích dostatečně informován a souhlasit s jejich využitím.
8. Definovat oznamovací povinnosti poskytovatele vůči zákazníkovi v případě jakéhokoliv narušení ochrany údajů, které může mít dopad na údaje zákazníka.
9. Povinnost poskytovatele služeb poskytovat seznam možných lokalit pro zpracování dat zákazníka.
10. Právo správce dohlížet a povinnost poskytovatele v této věci spolupracovat.
11. Povinnost poskytovatele podávat informace o změnách služeb zákazníkovi.
12. Řešit evidenci a kontrolu příslušného zpracovávání osobních údajů prováděného poskytovatelem nebo jeho subdodavateli.
13. Povinnost poskytovatele uvědomit zákazníka, vyžadují-li státní orgány přístup k uloženým datům, není-li to zakázáno například trestním právem. A to z důvodu zajištění důvěrnosti vyšetřování v rámci výkonu práva.
14. Poskytovatel je povinen zaručit, že jeho interní procesy zajišťují dostatečné zabezpečení dat a jsou plně v souladu s použitelnými vnitrostátními a mezinárodními předpisy.

Pokud jsou zákazníci cloud služeb správci údajů musí si v rámci čl. 17 odst. 2 směrnice 94/46/ES vybrat poskytovatele s vhodnými technickými a organizačními opatřeními na ochranu osobních údajů.

1.2.2 Smlouva o úrovni poskytovaných služeb

Pro porozumění SLA lze použít například tuto definici:

> „SLA představuje formalizovaný popis služby, kterou poskytuje dodavatel zákazníkovi. SLA definuje rozsah, úroveň a kvalitu služby.“
>
> [29]

Tato smlouva vznikla potřebou co nejlépe a nepřesněji definovat rozsah, úroveň a kvalitu služeb poskytovaných CSP zákazníkovi. SLA je v tomto prostředí nezbytným nástrojem pro stanovení práv a povinností obou stran a vybudování dlouhodobé spolupráce, ze které by měl nejlépe vzniknout silný partnerský vztah. [30]

Cloudové smlouvy a SLA vychází ze zásady smluvní volnosti, nemají tedy určitý právní rámec. SLA je většinou definována čistě na straně poskytovatele a platí pro všechny uživatele. Ostatní smlouvy se mohou obsahově lišit, dle dohody obou smluvních stran. [27]

Ve studii vyhotovené v roce 2015 pro Evropskou komisi se kromě modelové SLA určené jako vzor pro sestavení tohoto typu smluv na konci dokumentu zabývají body, které by měla již existující SLA upravovat pro soulad s modelovým řešením. Je to spíše vodítko pro potencionálního zákazníka, jaké oblasti mají být v SLA řešeny. [31]

SLA Checklist: [31]

- Identifikuje SLA dostatečně jasně služby, ke kterým se váže?
- Je jasně uvedeno, je-li SLA právně závazné nebo je to pouhé nezávazné prohlášení?
- Jsou zde jasně uvedeny výjimky aplikovatelnosti SLA jako například postup při plánované odstávce, neplánovanému výpadku nebo při útocích (např. DoS útok)?
- Jsou kompenzace při nedodržení SLA jasně definovány?
- Jsou závazky vůči zákazníkovi ze strany poskytovatele jasně definovány?
- Je zde uvedeno, kdo ověřuje dodržování závazků?
- Jsou implementovány nepřetržité kontrolní mechanismy pro ověřování dodržování závazků?
- V případě narušení bezpečnosti dat podniká nápravné kroky zákazník nebo nápravu sjednává proaktivně poskytovatel?

- Je zde mechanismus pro řešení sporů v otázkách dodržování SLA?
- Může CSP jednostranně měnit podmínky stanovené v SLA?
- Je jasně stanoven postup při situaci, kdy současné SLA bylo zrušeno a zároveň má zákazník stále nárok na kompenzaci?
- Jsou závazky stanovené v SLA kompatibilní se závazky spojenými s námi dále poskytovanými službami?

1.2.3 Ochrana osobních údajů

Osobní údaje jsou klíčem k našemu soukromí a právo jejich ochrany je základním lidským právem.[32] Jde o jakýkoliv údaj, který se vztahuje k nějaké fyzické osobě a současně je možné ji na základě tohoto údaje identifikovat. [32]

V dnešní době je ochrana osobních údajů zásadním objektem ochrany zájmů jednotlivce a je i tímto způsobem prosazována ze strany státu.

> *„Ochranu osobních údajů upravuje zejména zákon o ochraně osobních údajů č. 101/2000 Sb. v platném znění. Pozornost je věnována především zpracování osobních údajů, citlivým údajům, právům a povinnostem subjektů zpracovávajících informace, Úřadu pro ochranu osobních údajů, kontrolní činnosti a problematice předávání osobních údajů do zahraničí.“*
>
> [33]

Osobní údaje jsou předmětem zájmu komerčních společností a také pachatelů různých trestných činů a je tedy nutné zabezpečit jejich adekvátní ochranu. V případě cloud computingu jsou data předávána mimo firemní prostředí se známým zabezpečením, které je pod naší kontrolou. Data jsou často předávána pro zpracování na území jiných států s jinou právní úpravou a pro dodržení všech právních nařízení a norem musíme být při výběru poskytovatele obezřetní.

---

[32] Viz článek 5, Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb.

1.2.3.1 Předávání osobních údajů

Fyzické umístění datových center, ve kterých jsou data zpracovávána, hrají tedy při výběru poskytovatele zásadní roli. U některých typů dat legislativa nařizuje konkrétní parametry umístění zpracovávaných dat. Toto nařízení může být ve formě lokality, podmínky (např. ISO) či prověrky NBÚ. Umístění je nutné přesně znát a počítat s tím při předávání zákaznických dat do cloudu. [34]

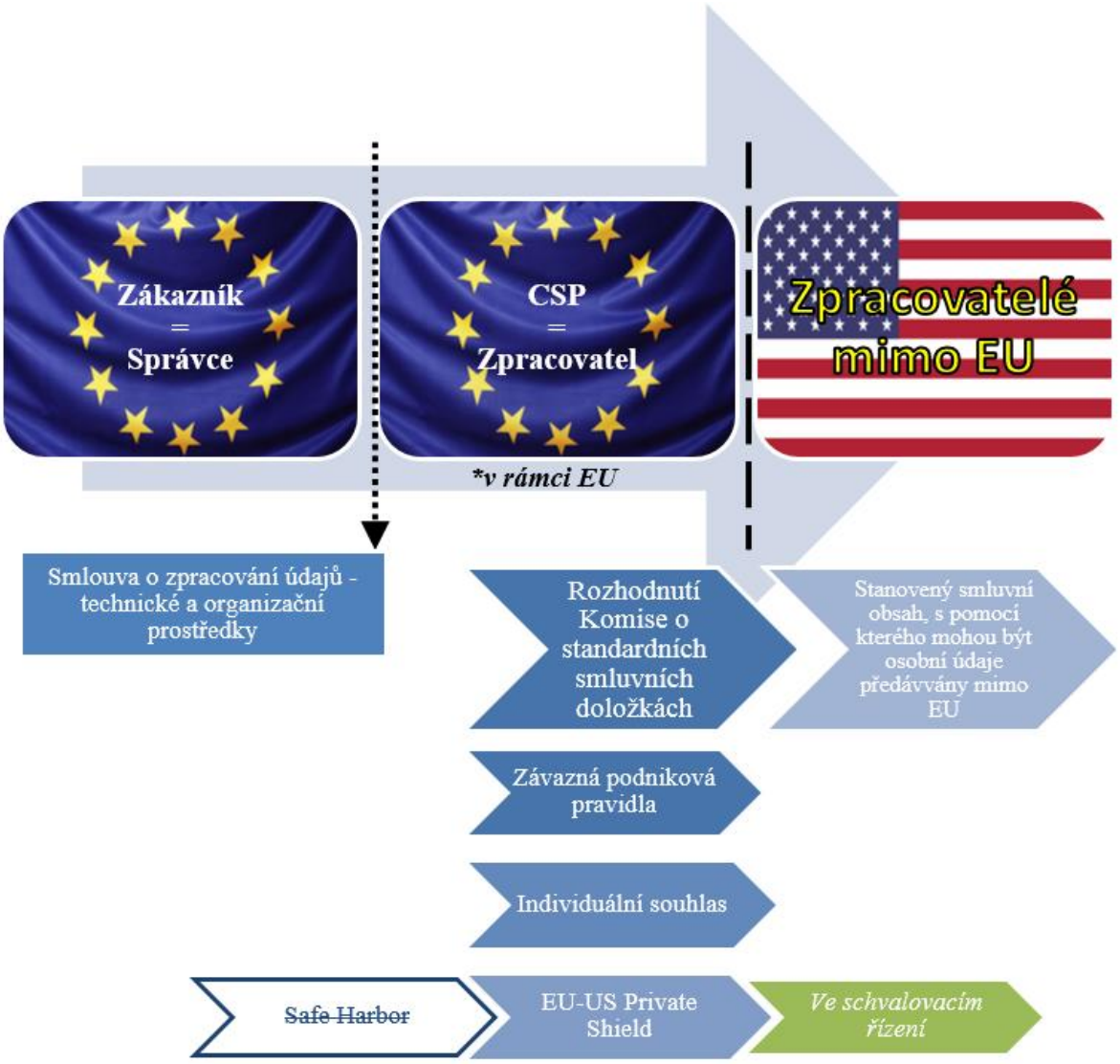
Na území České republiky (ČR) je úmluva o ochraně osob implementována zákonem č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů. V případě zkoumaného cloud computingu je zde důležitý §3 odst. 5. Říká, že každý správce zpracovávající osobní údaje s jejich fyzickým umístěním na území České republiky musí s daty pracovat dle příslušných zákonů ČR. Dále se v tomto zákonu v §27 ustanovuje, že volný pohyb osobních údajů nemůže být omezován, nepřesáhne-li jejich předání hranice členských států Evropské unie.[33]

Jednotlivé členské státy přijímají a implementují přijaté Směrnice[34] do své národní legislativy. Na evropské úrovni je ochrana osobních údajů řešena hlavně Směrnicí č. 95/46/ES[35]. Byla přijata pro podporu jednotného trhu, jelikož rozdíly v legislativách jednotlivých členských států neumožňovaly volný pohyb osobních údajů mezi těmito státy. Vzniklo tak mezinárodní společenství, ve kterém lze volně předávat data.

Evropská unie má díky přijatým směrnicím o ochraně dat přísnější pravidla na ochranu osobních údajů než většina zemí, včetně USA. Jsou-li data předávána do zemí mimo EU, vyžaduje Směrnice 95/46/ES, aby příslušná třetí země[36] „zajistila odpovídající stupeň ochrany“. Bez zajištění tohoto požadavku je přenos dat do takové země zakázán.[37] Tyto přenosy jsou však legitimní, jsou-li realizovány na základě uznávaného mechanismu. (viz Obrázek 2)

---

[33] Evropská unie je ekonomická a politická unie, ve které jednotlivé členské státy přijímají a implementují Směrnice do své národní legislativy. Vzniká tak mezinárodní společenství, ve kterém lze volně předávat data.
[34] Směrnice je právní akt stanovující cíl, který musejí všechny země EU splnit. Je však na jednotlivých zemích, jak formulují příslušné vnitrostátní zákony a jak těchto cílů dosáhnou.
[35] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Platné od 24. října 1995
[36] Třetí země - dle směrnice 95/46/ES jsou to země mimo EU a EHS s nedostatečnou úrovní ochrany osobních údajů.
[37] odst. 57 Směrnice 95/46/ES



Obrázek 2 - Transfer osobních údajů mimo EU [25]

Safe Harbor

Pro umožnění kontinuální toku informací, jenž je nutný pro mezinárodní obchod, dospěla Evropská komise k dohodě s Ministerstvem obchodu USA. Na jejím základě se mohli organizace samy certifikovat a potvrdit tak, že splňuji „bezpečný přístav“. Od roku 2000 byl tedy pro přenos dat mezi EU a USA užíván Safe Harbor. Pokud chtěla nějaká organizace legálně přenášet a následně zpracovávat data z EU do USA, musela se veřejně zaručit, že bude dodržovat zásady Safe Harbor. Ano, stačilo pouhé prohlášení o dodržování Safe Harbor, avšak jeho nedodržování bylo úřady sankcionováno.

Soudní dvůr Evropské unie dne 6. října 2015 prohlásil Safe Harbor za neplatný.[38] Následně byly zahájeny diskuze s americkými úřady za účelem nalezení právního, politického a technického řešení pro pokračování v předávání dat z EU do USA. V mezidobí přijetí alternativy po konci „bezpečného přístavu" je nutné užívat jiné nástroje, které zajistí odpovídající úroveň ochrany osobních údajů ve třetích zemích. Jako nejvhodnější se jeví standardní smluvní doložky[39] nebo závazná podniková pravidla. [40] [28][35][36]

Standardní smluvní doložky

> *„Standardní smluvní doložky představují vzorový text smlouvy mezi správcem osobních údajů, který hodlá předat osobní údaje do třetí země mimo Evropskou unii, resp. mimo EHP, a příjemcem osobních údajů v této třetí zemi. Jedná se o tzv. samoregulační nástroj pro předání osobních údajů do třetích zemí, přičemž správce sám přijímá přímou odpovědnost za zajištění bezpečnosti předávaných údajů."*
>
> Úřad pro ochranu osobních údajů[41]

Tyto vzorové texty byly vytvořeny jako efektivní a jednoduchý nástroj k zajištění odpovídající úrovně ochrany osobních údajů v rámci jejich předávání zpracovatelům ve třetích zemích. Obsahují detailní popis práv a povinností správce a zpracovatele osobních údajů.

Závazná podniková pravidla

Další zmíněnou možností jsou závazná podniková pravidla[42]. Jde o seznam principů, které zajišťují odpovídající úroveň ochrany při předávání osobních údajů v rámci koncernu. Oproti standardním smluvním doložkám platí smlouva o zpracování osobních údajů pro každou pobočku a není nutné uzavírat smlouvy jednotlivě. Tato možnost není vhodná pro každý subjekt a nevýhodou je náročný administrativní schvalovací proces. [37]

---

[38] Rozsudek ve věci C-362/14 Maximillian Schrems v. Data Protection Commissioner
[39] Viz 1.2.3.1 - Stadardní smluvní doložky
[40] Viz 1.2.3.1 - Závazná podniková pravidla
[41] www.uoou.cz
[42] Binding Corporate Rules, BCR

„Závazná vnitropodniková pravidla představují schválený souhrn zásad zpracování osobních údajů v rámci skupiny, který naplňuje požadavky evropské úpravy ochrany osobních údajů a který je právně závazný pro všechny pobočky skupiny, včetně poboček umístěných ve třetích zemích s nedostatečnou úrovní ochrany osobních údajů.“

Úřad pro ochranu osobních údajů[43]

V současné době[44] má schválená podniková pravidla 86 společností, mezi které patří například AXA, BMW, e-Bay, Intel Corporation a Siemens Group.[45]

EU-US Privacy Shield

Nová dohoda, a zároveň nástupce zrušeného Safe Harbor byla mezi EU a USA schválena sborem komisařů 2. února 2016. Stejně jako Safe Harbor bude tento rámec chránit základní práva Evropanů při předávání osobních údajů do Spojených států a také zajistí právní jistotu pro podniky.

„Nový štít mezi EU a USA *pro ochranu osobních údajů bude chránit základní práva občanů v případech, kdy jsou jejich údaje předávány společnostem v USA. Je to poprvé, co Spojené státy poskytly EU závazná ujištění, že přístup veřejných orgánů k údajům pro účely národní bezpečnosti bude podléhat jasným omezením, ochranným opatřením a mechanismům dohledu. Je to rovněž historicky poprvé, co budou moci občané EU v této oblasti využívat mechanismy nápravy. USA nás v rámci jednání o této dohodě ujistily, že neprovádí žádné hromadné či plošné sledování evropských občanů. Zavedli jsme společný roční přezkum za účelem důkladné kontroly plnění těchto závazků.“*

Evropská komisařka Věra Jourová[46]

[43] www.uoou.cz
[44] Duben 2016
[45] http://ec.europa.eu/justice/index_cs.htm
[46] Evropská komisařka pro spravedlnost, ochranu spotřebitelů a otázky rovnosti pohlaví

Na konci února roku 2016 byly zveřejněny právní texty, na základě kterých vznikne tzv. štít mezi EU a USA pro ochranu údajů. Zatím se právní texty konzultují v rámci výboru, složeného ze zástupců členských států a také musí vydat stanovisko pracovní skupina orgánů EU pro ochranu údajů[47]. USA zatím provede nezbytné přípravy pro zavedení nového rámce, monitorovacích mechanismů a nové funkce veřejného ochránce práv. Konečné rozhodnutí zatím nebylo přijato, ale předpokládá se termín do konce roku 2016. [27][38]

1.2.4 Certifikace a audity

Při snaze přesvědčit potenciální klienty o vhodnosti právě jejich řešení, je v zájmu samotných poskytovatelů cloud služeb být v souladu s mezinárodně uznávanými standardy a právními normami. Zavádí procesy a implementují mechanismy pro vyhovění náročným požadavkům pro získání osvědčujících certifikací auditů.

Na základě těchto certifikátů a auditů si může zákazník předem ověřit, jestli daný poskytovatel pokrývá jeho potřeby zabezpečení, ochrany osobních údajů, atd. Příklady:

ISO/IEC 27001

- Tento standard poskytuje model pro zavedení efektivního systému řízení bezpečnosti informací (ISMS[48]) a je jednou z nejlepších měřítek bezpečnosti cloudových služeb (důvěrnost, integrita, dostupnost služeb). Je součástí řady standardů ISO/IEC 27000, které řeší otázky ochrany osobních údajů, technického zabezpečení a důvěrnosti. „Zavádějí pokyny a obecné zásady pro zahájení, realizaci, udržování a zlepšování řízení zabezpečení informací v rámci organizace“. Dohromady popisují stovky možných kontrolních prvků a mechanismů. [39]

SSAE 16[49]/ISAE 3402[50]

- Tyto auditní standardy jsou zaměřené na organizace poskytující služby. Outsourcingové služby, a to cloudové služby samozřejmě jsou, mají dopad na prostředí

[47] Zřízená podle článku 29 směrnice 95/46/ES
[48] ISMS - Information Security Management System - Systém řízení bezpečnosti informací
[49] Statement on Standards for Attestation Engagements No. 16
[50] International Standards for Attestation Engagement No. 3402

kontroly na straně zákazníků. Tyto standardy umožňují zákazníkům nahlížet do procesů, udávají kvalitu a efektivnost řízení u poskytovaných služeb. [2]

HIPAA/HITECH

- Udává postupy, zásady a pokyny pro zpracování zdravotních informací za současného a zachování soukromí a bezpečnosti těchto informací. V případě cloudu jde o přenos elektronické informace.

EU Model Clauses

- Standardní smluvní doložky jsou v současné době používány jako náhrada za zneplatněný Safe Harbor v případě přenosu a zpracování osobních údajů z EU do USA či dalších třetích.

1.2.5 Sektorová regulace

V hospodářství probíhá mnoho různých činností, které lze dělit dle odvětví. Jednotlivé sektory vznikají na základě podobných znaků odvětví a i v případě cloud computingu lze na tyto sektory aplikovat sady opatření, které je zapotřebí dodržet. Z toho vyplývá tzv. sektorová regulace. Pro příklad dva sektory: [27]

Finanční sektor

Údaje jsou chráněny specifickou právní úpravou bankovním tajemstvím. Outsourcing dat z této oblasti je možná při dodržení standardů uznávaných ČNB. Regulaci na úrovni EU upravují směrnice MIFID I & II, CRD IV, CRR, Solvency II. Česká právní úprava řeší outsourcing těchto dat vyhláškou ČNB č. 163/2014 SB, příl. č. 7.

Zdravotnický sektor

Pro citlivé údaje v ČR nejsou žádné dodatečné legislativní požadavky pro outsourcing. Lze tedy cloud využít při zachování standardních ochrany osobních údajů. Pro zpracování údajů v zdravotní dokumentaci mají zdravotnická zařízení souhlas pacienta ze zákona. Samotný režim outsourcingu není výslovně upraven.

2 RIZIKA PŘI NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI V PROSTŘEDÍ CLOUDU

Správce osobních údajů by měl vědět kdo, kde a jakým způsobem zpracovává jím spravované data. A to zejména v případě osobních údajů. Měl by znát implementovaná zabezpečení a mít nad těmito daty zaručenu co nejvyšší míru kontroly. Pro zajištění těchto aspektů správy by měl správce vyžadovat od poskytovatele služeb potřebné informace pro posouzení rizik nabízeného řešení.

Zpracování osobních údajů v cloudu přináší vyšší úroveň rizika, než běžné zpracování lokálními prostředky správce či zpracovatele. Většina rizik s tímto spojených spadá do dvou hlavních kategorií: [28]

- Nedostatek kontroly nad údaji
- Nedostatečné informace o samotném zpracování = netransparentnost

2.1 Nedostatek kontroly

Při správě osobních údajů lokálními prostředky, má správce v případě přímého vlastnictví těchto prostředků výlučnou kontrolu nad těmito údaji. Může aktivovat nezbytná technická a organizační opatření pro zajištění stěžejních prvků, kterými jsou dostupnost, integrita, důvěrnost, transparentnost, izolovanost, schopnost intervence a přenositelnost údajů. Předá-li správce spravované osobní údaje do systémů poskytovatele cloud služeb, může o tyto prvky díky ztrátě výlučné kontroly přijít.

Nedostatečná kontrola se může projevit následujícími způsoby:

Nedostatečná dostupnost kvůli chybějící interoperabilitě[51] - Přenese-li zákazník data do prostředí s proprietární[52] technologií, může dojít k tzv. lock-in efektu. Pro zákazníka tak bude obtížné přemisťovat data mezi různými cloudovými/lokáními systémy (přenositelnost) nebo si vyměňovat informace se subjekty s jinými řešeními ICT (interoperabilita).

[51] Lock-in efekt způsobuje závislost na poskytovateli.
[52] Specifická, jedinečná a uzavřená technologie, kterou využívá velmi omezené množství poskytovatelů. Nebo jen jediný.

Nedostatečná integrita způsobená sdílením zdrojů - Ve virtualizovaném prostředí cloudu sdílejí zákazníci prostředky pocházející ze stejné infrastruktury. Při zpracování dat z různých zdrojů tak může dojít ke střetu zájmů, anebo zpracování může sloužit rozdílným cílům.

Nedostatek důvěrnosti ve smyslu žádostí o vymáhání práva adresovaných přímo poskytovateli cloudových služeb - Donucovací orgány členských zemi EU nebo třetích zemí mohou vymáhat právo na datech uložených v cloudu. Tyto požadavky na zpřístupnění dat se předně adresují přímo poskytovateli cloud služeb a existuje tak možné riziko vydání cizím donucovaným orgánům bez platného právního základu EU. Tím by došlo k porušení právních předpisů Evropské unie pro ochranu osobních údajů.

Neschopnost intervence kvůli komplikovanosti a dynamice řetězce v rámci externího zajišťování služby - Cloudové smlouvy bývají velmi komplexní a obsažené služby nemusí být vždy dodávaný jedním původním poskytovatel. Služby lze dynamicky přidávat a odstraňovat v průběhu platnosti zákaznické smlouvy a může docházet k řetězení poskytovatelů. Prolínají se tak různé obchodní záruky a procesy pro ochranu osobních údajů. Soulad všech článků řetězce by měl zajistit původní poskytovatel.

Neschopnost intervence - V některých případech nemusí být zajištěna potřebná opatření a nástroje pro správu osobních údajů. Správce tak nemůže plně aplikovat práva subjektů osobních údajů, jako např. přístup k údajům, výmaz či jejich oprava.

Chybějící izolovanost - Ve sdíleném cloudovém prostředí jsou data různých zákazníků na fyzické úrovni „vedle sebe“. Jsou prakticky oddělena „pouze“ SW bariérami, které zajišťují individuální prostředí pro jednotlivé zákazníky. S pomocí fyzického přístupu k prostředkům uložení dat nebo zneužitím přístupů s vysokou úrovní (high-risk roles) mohou být tyto bariéry prolomeny.

2.2 Nedostatek informací o zpracování (transparentnost)

Poskytovatel služeb by měl o svých službách uvádět dostatečné informace a zákazník by se měl o tyto informace dostatečně zajímat. Při nedostatku v informovanosti o operacích zpracování údajů vyplývají rizika nejen pro správce, ale i pro subjekty zpracovávaných osobních údajů.

Není-li správce dostatečně obeznámen s některými z následujících skutečností, vystavuje sebe i subjekty osobních údajů různým hrozbám:

- Poskytovatel využívá k dodání služeb i subdodavatele
- Ke zpracování osobních údajů dochází v různých zemích EHP. To může mít přímý dopad na použité právní předpisy pro ochranu osobních údajů a případné spory s tímto spojené, k nimž může dojít mezi uživatelem a poskytovatelem.
- Ke zpracování osobních údajů dochází mimo země EHP a jsou tak předávány do třetích zemí. Tyto třetí země musí zajišťovat odpovídající úroveň ochrany a předávání dat do těchto zemí musí být spojeno s vhodnými ochrannými opatřeními, jinak by toto předávání osobních údajů bylo nezákonné. Možná opatření jsou např. standardní smluvní doložky, závazná podniková pravidla, individuální souhlas nebo v budoucnu rozpracovaný EU-US Privacy Shield (viz 1.2.3.1).

Pokud správce zpracovává osobní údaje svými lokálními prostředky, řídí se zákony dané země a procesy zpracování dat si stanovuje a implementuje vlastními silami. Rozhodne-li se pro outsourcing a s tím i zpracování osobních údajů třetí stranou v cloudu, musí být velmi obezřetný, jakého poskytovatele a službu si zvolí. Vše co si dříve mohl nastavit dle svých potřeb, nyní nastavuje někdo jiný a ne vždy to bude v souladu s veškerými požadavky pro adekvátní zpracování osobních údajů v rámci platných právních předpisů a regulací.

3 POROVNÁNÍ CLOUDOVÝCH ŘEŠENÍ S TRADIČNÍM ŘEŠENÍM Z BEZPEČNOSTNÍHO A LEGISLATIVNÍHO POHLEDU

Při rozhodování mezi vlastním řešením ICT a cloudovými službami je zapotřebí zvážit mnoho stránek. Najít důvěryhodného poskytovatele, který bude suplovat pozitiva lokálního řešení a splňovat všechny naše požadavky může nějaký čas zabrat. Tato fáze by se však neměla podceňovat a jednou z možností je položit si obě varianty vedle sebe a jednotlivé oblasti porovnat.

3.1 Aktualizovaný software

Aktualizace softwaru a záplatování bezpečnostních trhlin je velmi důležitá část správy. Je-li řešena rychle a dostatečně, přispívá to k větší míře zabezpečení a obraně proti nežádoucím aktivitám.

- **On-premise** - Zajišťuje sama organizace. Rychlost a kvalita řešení bezpečnostních trhlin závisí na IT oddělení.
- **Cloud** - Zajišťuje poskytovatel služby. Zákazník má automaticky dostupné nejnovější verze softwaru. Jelikož je poskytovatel služby finančně odměňován za funkční službu, měl by tak přistupovat i při prevenci.

3.2 Správa identit a přístupů

Způsob zabezpečení přístupů do systémů s rozdělení rolí zásadně ovlivňuje celkovou bezpečnost již v samotném počátku, při přístupu do systému. Důsledky ukradených přístupových údaje či zlé úmysly některého ze zaměstnanců může správně řešený IAM utlumit.

- **On-premise** - Celé řešení si volí organizace dle svých potřeb a může ho kdykoliv upravit a přizpůsobit konkrétní situaci.
- **Cloud** - Přebírám IAM dle implementace poskytovatele. Problém může nastat v případě, kdy budeme chtít provést vylepšení. Systém platí pro všechny zákazníka daného poskytovatele a customizace většinou není možná.

3.3 Přístupová prostředí

Ať jde o cloud nebo tradiční lokální řešení, využíváme pro přístup do systému a služeb UI/API.

- **On-premise** - Při lokálním řešení nemusí přístupová prostředí vůbec opustit interní síť a nevystavují se tak negativním vlivům internetu. Drobné programové chyby nemusí mít tak zásadní následky.
- **Cloud** - Do služeb se přistupuje prostřednictvím internetu, a tak na rozdíl od lokálních řešení mohou čelit cíleným útokům. Přístupová prostředí musí být odolná proti neautorizovaným přístupům.

3.4 Šifrování

Velmi často používaným způsobem zabezpečení dat je jejich šifrování. Lze toho docílit více způsoby a u dat záleží na jejich povaze, způsobu a místu zpracování.

- **On-premise** - Při lokálním řešení si volíme vlastní způsob ochrany a šifrování řešíme pouze v rámci interní sítě či uživatelských stanic. Data ve známem a důvěryhodném prostředí by měla být vnějších vlivů ušetřena ostatními bezpečnostními prvky.
- **Cloud** - Kromě zabezpečení uživatelských stanic, je zásadní bezpečný přenos dat mezi zákazníkem a poskytovatelem. Data nesmí být během přenosu čitelná. Spolu s tím se nachází v cizím, „nedůvěryhodném“ prostředí a určitá data by měla být vhodným způsobem šifrována.

3.5 Přenos dat

Zpracovávaná data je zapotřebí přenášet v rámci infrastruktury a ke koncovému uživateli.

- **On-premise** - Je-li dostatečně zabezpečená a izolovaná vnitřní síť organizace od okolního světa, mohou data putovat v rámci celé infrastruktury.
- **Cloud** - Data jsou zpracovávána na serverech mimo infrastrukturu organizace. Přenos dat přes internet je realizován nejen ke koncovému zákazníkovi, ale může být realizován i v rámci infrastruktury poskytovatele. Tento přenos musí být dostatečně zabezpečen - šifrován.

3.6 Fyzický přístup

Přímý přístup osob k serverům dává možnost se dostat k informacím v surovém stavu. Není-li aplikováno šifrování, mohou být odcizená data použitelná.

- **On-premise** - Standardně více věříme vlastním zaměstnancům, ale i zde se mohou objevit zlé úmysly. Pro příklad stále více aktuálnější sociální inženýrství a zavlečení malware do organizace zaměstnanci.
- **Cloud** - Zaměstnanci poskytovatele se zákazníky bližší a neznámí lidé mají fyzický přístup k serverům, kde jsou uložena data. Ve sdíleném prostředí, kdy nevíme, na jakých fyzických discích se data nacházejí, se data konkrétního uživatel hůře lokalizují.

3.7 Útoky

Ať již je cílem toku získání citlivých dat nebo vyřazení služby z provozu, jsou napadení zvenčí velmi častým a nevítaným jevem. Díky sociálnímu inženýrství se i do velmi dobře zabezpečené řešení může útočník dostat a napáchat velké škody.

- **On-premise** - Napadení je cílené a zaměřené na krádež, modifikaci, výmaz dat nebo vyřazení serverů z provozu.
- **Cloud** - Navíc od výše uvedeného sem spadají i útoky na ostatní uživatele sdíleného prostředí. Dochází-li během útoku k přetěžování infrastruktury, mohou být kromě cíle zasaženi další uživatelé. Důsledkem útoku mlže být i mnohonásobné zvýšení spotřeby výpočetních prostředků a tím i účet za služby.

3.8 Ochrana osobních údajů

Jak již bylo řečeno, osobní údaje jsou klíčem k našemu soukromí a tak jsou kromě know how a duševního vlastnictví jedním z nejcennějších artiklů. Ochrana osobních údajů je dána ze zákona a je tak nejvíce řešena a striktně vyžadována.

- **On-premise** - Pro splnění požadavků na ochranu většinou stačí dodržovat zákony země, kde organizace sídlí a data zpracovává.
- **Cloud** - Poskytovatel může data zpracovávat v různých zemích světa a je tedy nutné se ujistit, že zajišťuje dostatečnou úroveň zabezpečení osobních údajů pro pře-

nos a zpracování. Zákazník se musí ujistit, že jsou implementována a dodržována potřebná opatření a procesy.

V rámci sektorové regulace může docházet k různým legislativním úpravám v rámci různých sektorů. Některá odvětví (sektory) však nemusí být právně upraveny. Jelikož ale cloud patří do režimu outsourcingu, je nutné dodržovat i opatření právě pro outsourcing.

Dodržování potřebných norem a procesů ze strany poskytovatele si lze ověřit provedenými certifikacemi a audity. [53]

Systémy v cloudu se více zaměřují na bezpečnost, jelikož jsou neustále pod tlakem vlivů otevřeného internetu a investují do těchto opatření velké částky. Organizace s vlastním lokálním řešením mohou žit v pocitu bezpečnosti vlastní infrastruktury schovaná na firewallem a jejich řešení nebo prevence mohou být nedostatečná. Rázné odmítání této technologie tedy není na místě. Pokud budeme postupovat s rozmyslem, například cestou hybridní cloudu, přineseme při správné realizaci do své organizace to nejlepší z obou světů. [40]

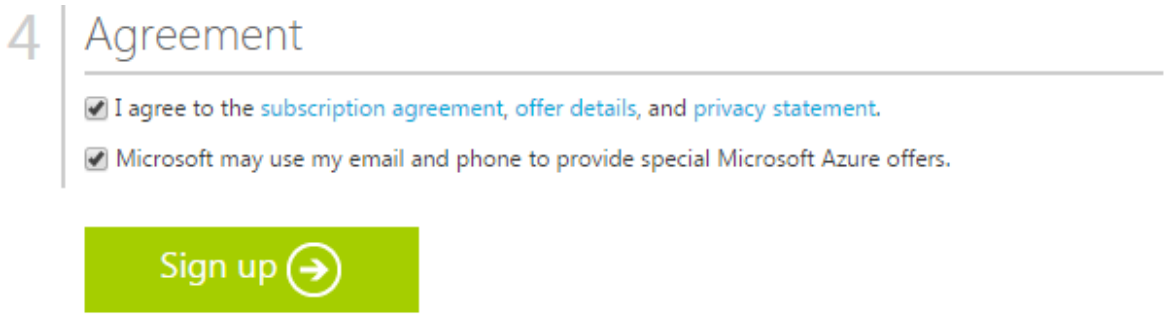
[53] Viz sektorová regulace, 1.2.5

4 CLOUDOVÉ SMLOUVY U WINDOWS AZURE

Gartner označil Microsoft Azure jako lídra PaaS ve svém „Magic Quadrant for Enterprise Application Platform as a Service“ třetí rok po sobě a je jednou z nejpoužívanějších cloud platforem[54]. Proto jsem se ji rozhodl použít jako vzorový příklad pro řešení cloudové smlouvy.

4.1 Smlouva a podmínky poskytování služeb

Využívání služeb Azure od společnosti Microsoft se řídí podmínkami a ujednáními smlouvy Microsoft Online Subscription Agreement[55]. S touto smlouvu souhlasíme a její podmínky přijímáme při založení účtu na Azure, viz „subscription agreement“ na Obrázku 3.



Obrázek 3 - Souhlasy při zřízení služby Windows Azure

Její součástí jsou Obchodní podmínky, Podmínky používání služeb Online Services[56], SLA[57] a Detaily nabídky[58]. Na vše se lze proklikem dostat z přehledové stránky[59].

Se vším souhlasíme jednoduchým zatržením a stisknutím tlačítka „Sign up“ a také kvůli tomu, jsou veškeré potřebné informace kdykoliv dostupné. Zatržení potřebných bodů a stisk zmíněného tlačítka při tvorbě účtu nahrazuje podpis standardní papírové smlouvy.

[54] Report si lze zdarma stáhnout po vyplnění formuláře například zde: https://azure.microsoft.com/cs-cz/resources/gartner-apaas-magic-quadrant/
[55] https://azure.microsoft.com/cs-cz/ ; dále Podpora - Právní informace - Smlouva o předplatném
[56] https://azure.microsoft.com/cs-cz/ ; dále Podpora - Právní informace - Podmínky použití služeb
[57] https://azure.microsoft.com/cs-cz/ ; dále Podpora - Právní informace - Smlouvy o úrovni služeb
[58] Liší se dle sjednaných služeb
[59] https://azure.microsoft.com/cs-cz/ ; dále Podpora - Právní informace - Přehled

Tak to ale prakticky funguje u jakékoliv webové služby či e-shopu a neplatí to tedy pouze pro Azure.

4.2 Smlouva o úrovni poskytovaných služeb (SLA)

Nejčastějšími prvkem SLA je dostupnost. Například Microsoft garantuje pro každou službu platformy Azure v separátních SLA dostupnost pro danou službu. Pokud není tato garance dodržena, obdrží zákazník jako odškodnění kredit na slevu z dané služby.[60]

V žebříčku 25 nejpopulárnější SaaS aplikací a služeb realizovaném společností Okta se na prvním místě umístil Office365 od společnosti Microsoft. Pro příklad tedy použijeme tuto webovou službu. V SLA má garantovánu procentuální dobu fungování v měsíci více než 99,9 %. Při 30 dnech v měsíci je tedy garantována maximální nedostupnost 43,2 minut[61]. Pokud tato hranice nebude dodržena, uplatňuje se kompenzace ve formě slevy pro danou službu za dané fakturační období, viz tabulka 4. [41]

Procentuální doba fungování v měsíci	Kredit služby
< 99,9 %	10%
< 99 %	20%
< 95 %	100%

Tabulka 4 - Dostupnost služby vs kompenzace za nedostupnost[62]

4.3 Podmínky používání služeb Online Services

V toto dokumentu Microsoft sepsal sadu závazků vůči zákazníkům, podrobné podmínky ochrany dat a standardní smluvní doložky EU[63] pro všechny online služby určené pro podniky. V části „Podmínky ochrany osobních údajů a zabezpečení“ jsou uvedeny informace týkající se všech služeb a v části „Podmínky zpracování dat“ informace o zpracování dat a závazky pro určité, blíže specifikované služby.

[60] https://azure.microsoft.com/cs-cz/support/legal/sla/
[61] 43,2 minut = (30dní * 24 hodin) * 0,001 nedostupnost * 60 (převod na minuty)
[62] Office365 SLA
[63] Standardně jsou připojeny jako příloha dokumentu

V následujícím textu budou důležité body stručně popsány.

4.3.1 Obecné podmínky ochrany osobních údajů a zabezpečení

- **Použití zákaznických dat**

  Zákaznická data budou použita pouze pro poskytování služeb online zákazníkovi, včetně účelů souvisejících s poskytováním těchto služeb. Tato data nebudou ze strany poskytovatele služeb využívána a zákazník si zachovává veškerá práva s daty spojená.

- **Zveřejnění zákaznických dat**

  Při standardní situaci se poskytovatel zavazuje, že data nezveřejní mimo společnost, ovládané dceřiné společnosti a afilace[64]. Výjimkami je přímý požadavek zákazníka, případy uvedené v podmínkách služeb online nebo podle požadavků zákona. Při jakémkoli požadavku na data zákazníka je zákazník informován.

- **Vzdělávací instituce**

  Pokud zákazníkem se vzdělávací organizace, kterou se vztahují předpisy v rámci zákona FERPA[65], nebude poskytovatel vlastnit žádné nebo jen omezené kontaktní údaje studentů. Pro použití spravovaných služeb budou muset mít koncoví uživatele souhlas rodičů. Tento bod se prakticky týká vzdělávacích institucí pouze v USA. U takto chráněných subjektů například neprochází e-maily pro reklamní účely.

- **Komerční spolupracovník HIPAA**

  Má-li zákazník ve svých datech zahrnuty „chráněné informace o zdravotním stavu“ zahrnuje smlouva se zákazníkem i smlouvu HIPAA BAA.

  V České republice nejsou žádné dodatečné požadavky pro zpracování citlivých údajů při outsourcingu, ale například v Německu jsou významná omezení pro předávání citlivých údajů do zahraničí. U zdravotní dokumentace není v ČR režim outsourcingu výslovně upraven. [27]

[64] Afilace je pobočka nebo samostatný, ale podřízený (ovládaný) subjekt, podnik
[65] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g

- **Oznámení incidentu zabezpečení**

  Zjistí-li poskytovatel jakýkoli nezákonný přístup k datům zákazníka, jehož následkem bude ztráta, zveřejnění nebo změna zákaznických dat, bude zákazník poskytovatelem o incidentu informován. Dále bude incident prošetřen a poskytovatel provede kroky pro zmírnění účinků a minimalizaci škod z incidentu vyplývajících.

  V případě možnosti zneužití zákaznických účtů, ověřovacích údajů a dalších narušení bezpečnosti ve vztahu k online službám musí zákazník informovat poskytovatele.

- **Místo zpracování dat**

  S některými výjimkami mohou být zpracovávaná data zákazníka přenesena, uchovávána a zpracovávána ve Spojených státech amerických nebo jiné zemi, ve které poskytovatel či subdodavatel provozují zařízení. Poskytovatel se zároveň zavazuje, že se budě řídit požadavky EHP a švýcarského zákona o ochraně dat[66].

- **Použití dodavatelů**

  Poskytovatel si může najmout subdodavatele za účelem poskytování služeb jeho jménem a tito subdodavatelé získávají zákaznická data pouze za účelem poskytování služeb. Samotný poskytovatel je odpovědný za dodržování svých povinností při nakládání s daty zákazníka na straně subdodavatele.

4.3.2 Podmínky zpracování dat

Podmínky zpracování údajů zahrnují také smluvní doložky pro předávání osobních údajů[67] zpracovatelům usazeným ve třetích zemích podle směrnice EU o ochraně osobních údajů.

Tato část podmínek se vztahuje jen na určité služby, v dokumentu blíže specifikované.

Nejdůležitější části stručně popsány v následujících bodech:

[66] Švýcarský zákon o ochraně dat
[67] V souladu s rozhodnutím Evropské komise ze dne 5. února 2010 o standardních smluvních doložkách

Ochrana osobních údajů

- **Vymazání nebo vrácení zákaznických dat**

  Zákazník do 180 dnů od ukončení používání služeb odstraní svá data a účet deaktivuje.

- **Předávání zákaznických dat**

  Během období platnosti smlouvy je garantována certifikace v rámci programů na ochranu osobních údajů EU a Švýcarska, a to za předpokladu, že jsou udržovány vládou USA. Zpracování osobních údajů je řešeno standardními smluvními doložkami připojenými v příloze smlouvy.

- **Pracovníci společnosti Microsoft**

  Bez svolení zákazníka nebudou zákaznická data pracovníci poskytovatele zpracovávat. K datům musí přistupovat dle podmínek o zpracování údajů v průběhu i po ukončení trvání všech závazků.

- **Předávání subdodavatelům**

  Poskytovatel může najmout subdodavatele za čelem poskytování určitých omezených nebo pomocným služeb jeho jménem. Tito subdodavatelé musí poskytovat stejnou úroveň zabezpečení jako samotný poskytovatel a pokud s novým subdodavatelem nesouhlasí, může za stanovených podmínek odmítnout a službu bez postihu ukončit.

- **Další podmínky pro Evropu**

  Tyto a další podmínky pro Evropu platí, má-li zákazník koncové uživatele v EHP nebo Švýcarsku. Pro užívání a konfiguraci funkcí služeb online představují „Podmínky pro služby online“ úplné a konečné pokyny pro zpracování dat poskytovatelem. Jakékoli další pokyny musí být dohodnuty v souladu s procesem doplnění multilicenční smlouvy zákazníka.

  Poskytovatel dle směrnice o ochraně osobních údajů EU, s použitím článku 12(b):

  - Umožní zákazníkovi svá zákaznická data opravit, odstranit nebo zablokovat.

  Nebo

  - Bude takové opravy, odstranění nebo blokování provádět jeho jménem.

- **Zabezpečení**

  V obecných postupech poskytovatel (Microsoft) uvádí implementaci zabezpečení uvedených v tomto dokumentu. Zavazuje se udržovat a dodržovat bezpečnostní opatření, která představují jedinou odpovědnost na zabezpečení zákaznických dat ze strany poskytovatele služeb. V tabulce zde popisuje realizovaná bezpečnostní opatření pro jednotlivé domény.

- **Zásady zabezpečení informací služeb online**

  Každá poskytovaná služba se řídí písemnými zásadami a zabezpečení dat, které odpovídají standardům a rámcům řízení, viz následující tabulka 5.

Služba online	**ISO 27001**	**ISO 27002 Postupy**	**ISO 27018 Postupy**	**SSAE 16 SOC 1, typ II**	**SSAE 16 SOC 2, typ II**
Služby Office365	Ano	Ano	Ano	Ano	Ano
Microsoft Dynamics Online Services	Ano	Ano	Ano	Ano	Ano
Služby Microsoft Azure Core	Ano	Ano	Ano	Liší se	Liší se
Online služby Microsoft Intune	Ano	Ano	Ano	Ano	Ano
Služby Microsoft Power BI	Ano	Ano	Ano	Ne	Ne

Tabulka 5 - Certifikace a audity[68]

Nové oborové nebo vládní standardy mohou být kdykoli poskytovatelem přidány a odebrány mohou být v případě, nejsou-li již používány a byly nahrazeny jinými.

Jednotlivé standardy a rámce řízení byly rozebrány v části 1.2.4.

- **Audity služeb online společnosti Microsoft**

  Pro každou službu online provádí poskytovatel audity zabezpečení počítačů, výpočetního prostředí a fyzických datových center, které jsou používány pro zpracování zákaznických dat.

[68] Windows Azure - Podmínky pro služby online

Postup je v dokumentu popsán následovně:

- Pokud audity podléhají standardu nebo rámci, bude audit podle takového kontrolního standardu nebo rámce proveden pro každou službu online minimálně jednou ročně.
- Každý audit bude proveden v souladu se standardy a pravidly regulatorního nebo akreditačního orgánu pro jednotlivé příslušné kontrolní standardy nebo rámce.
- Každý audit bude proveden kvalifikovanými nezávislými auditory zabezpečení třetí strany dle výběru společnosti Microsoft a na její náklady.

II. PRAKTICKÁ ČÁST

5 NÁVRH CLOUDOVÝCH ŘEŠENÍ

Výpočetní technika je v dnešní době nedílnou součástí života většiny lidí a provozu firem. Jaký vliv bude mít selhání ICT při plnění stanovených cílů, záleží zejména na míře závislosti daného subjektu na těchto prostředcích.

Pro možná využití cloudových služeb jsou stanoveny tři modelové společnosti s různou mírou závislosti právě na ICT:

- Mírná závislost - Truhlářství
- Střední závislost - Personální agentura
- Úplná závislost - Animační studio

Předmět výkonu jednotlivých subjektů je rozdílnou měrou závislý na výpočetní technice. Cílem této části je navrhnout řešení využití technologií cloud computingu pro tyto modelové společnosti a stanovit možnosti, budou-li tyto služby nedostupné. Výběr konkrétních řešení bude realizován s ohledem na bezpečnostní a legislativní aspekty daných subjektů, tedy SLA konkrétních služeb budou samozřejmě brány v potaz. Ekonomická stránka věci zde nebude přímo řešena.

Společným aspektem všech modelových společností bude jejich čerstvé zřízení. Nedisponují tedy žádnými HW ani SW řešeními a nebudeme tedy řešit výměnu či integraci do nového řešení. Půjde pouze o využití technologií cloud computingu při realizaci podnikového ICT.

Při výběru cloudového poskytovatele je dobré zaměřit se na stabilní a silné partnery, u kterých nehrozí zánik. Pro všechny případy je tak vhodné vybírat služby, které nejsou založené na proprietárních technologiích, čímž bychom si znesnadnili případnou migraci k jinému poskytovateli. Zálohy je vhodné mít ve 3 až 4 kopiích, dle důležitosti daných dat.

Na závěr každého řešení bude přiložena tabulka se závažností nedostupnosti jednotlivých cloud služeb pro různé doby výpadku. V následující tabulce 6 je znázorněna legenda:

Závažnost	**Barva**
Nízká	
Střední	
Vysoká	

Tabulka 6 - Legenda pro míry závažnosti

5.1 Využité služby

5.1.1 Office365

5.1.1.1 Funkcionality

Nejznámější kancelářský software je dostupný také formou webových aplikací. Je nabízen v různých variantách, odlišných dle dodávaných aplikací a funckionalit. Tato služba bude využita u všech modelových řešení a bude rozebrána podrobněji, jelikož její cloudová podstata je zdrojem a zároveň i řešením potencionálních problémů.[69]

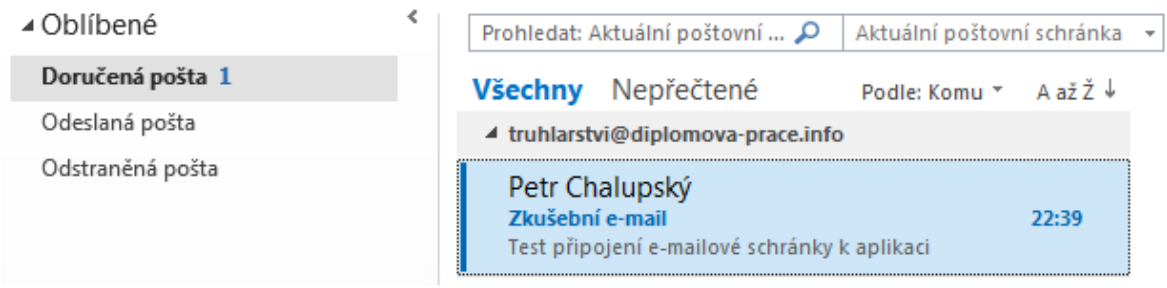
Zásadní věcí je, že k dispozici máme nejen webové verze těchto aplikací[70], ale plnohodnotné desktop verze[71] a také aplikace pro mobilní zařízení[72]. Předplatné na měsíční/roční bázi nám zajišťuje vždy aktuální verze všech aplikací.

Výhodou cloud řešení je dostupnost webové verze odkudkoli. Pro využití služeb Office365 se registrujeme pomocí libovolného účtu Microsoft, pro tento případ účtem „@hotmail.cz“. Pomocí tohoto účtu se připojujeme ke službám i skrze mobilní telefon.

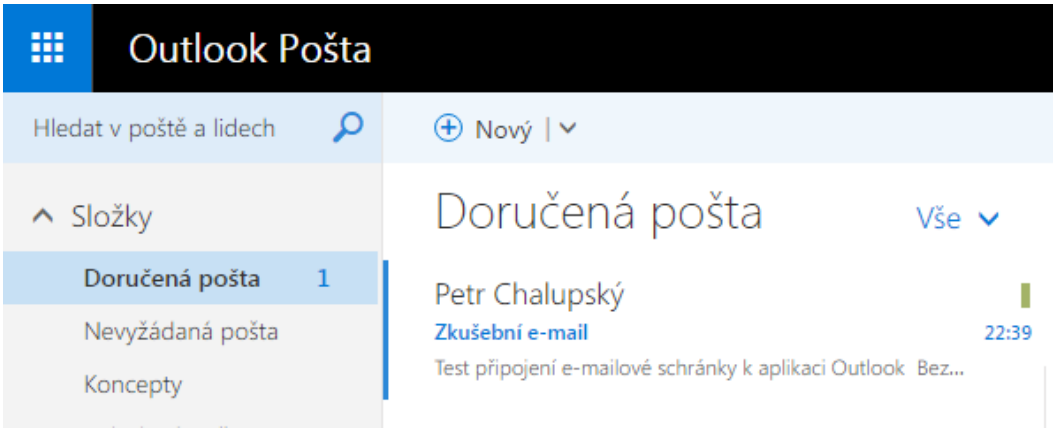
E-mail je pro mnoho firem zásadním komunikačním prostředkem a také možným důkazem v případě sporů, jelikož jde o zaznamenanou komunikaci s prokazatelným původem. Je tedy vhodné mít e-maily zálohované. Pokud budeme využívat poštovní server a všechny varianty aplikace Outlook, můžeme mít až 4 zálohy e-mailů, se kterými můžeme manipulovat (nepočítáme zálohy prováděné samotnými poskytovateli služeb), exportovat (desktop Outlook a poštovní server[73]) a případě dále zálohovat dle svého uvážení.

Jeden e-mail je na následujících obrázcích vyobrazen na třech platformách v aplikaci Outlook (Obrázek 4 - 6).

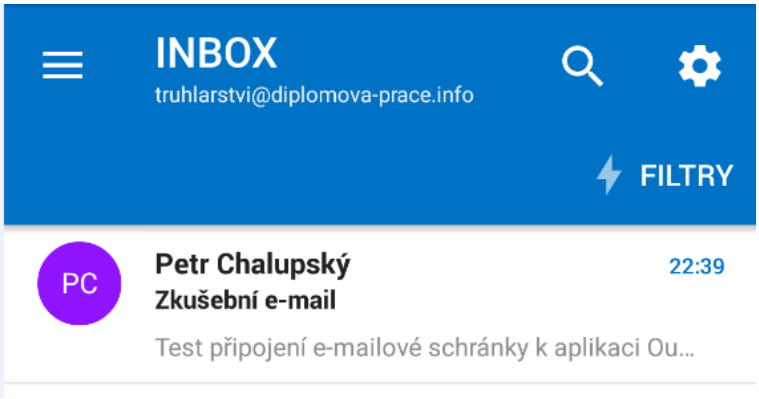
[69] https://products.office.com/cs-CZ/
[70] Kombinace aplikací dle zvolené varianty služby
[71] Office 2016, k měsíci duben 2016
[72] Android, Windows Phone, iOS
[73] Dle možností poštovního serveru



Obrázek 4 - Office 2016 - Outlook Desktop



Obrázek 5 - Office365 - Outlook - WEB

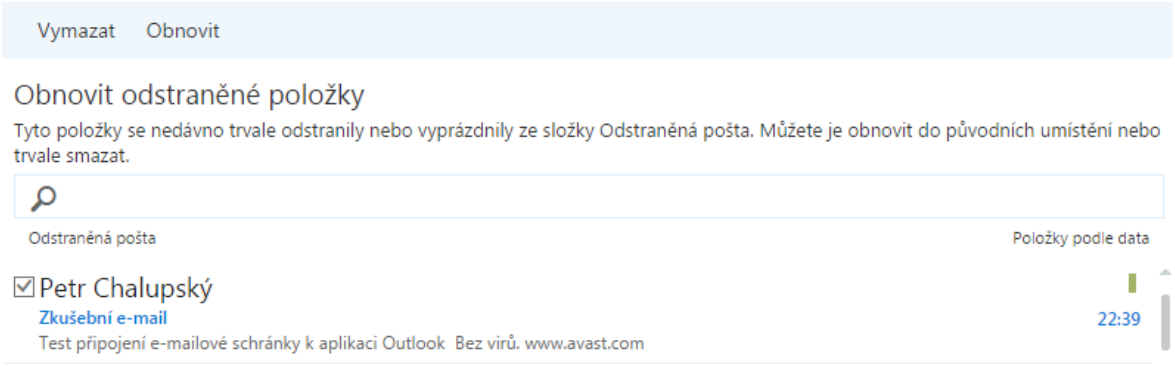


Obrázek 6 - Outlook - Mobile

E-mailové zprávy chodí na poštovní server a do Outlooku je pouze stahujeme. Při takovéto správě máme e-maily uloženy až na čtyřech místech najednou (dle aktualizace schránek v jednotlivých aplikacích Outlook). Dle nastavení se práce s e-maily může chovat následovně:

- Při smazání e-mailu v Outlooku se zpráva smaže také na poštovním serveru
- Při smazání e-mailu v Outlooku se zpráva nesmaže také na poštovním serveru

Pokud zvolíme druhou možnost, jsou e-maily na poštovním serveru uložené pro případ smazání. Webový Outlook uchovává odstraněné e-maily standardně po 30 dní a standardně se nadále po 14 dní dají ještě obnovit (Obrázek 7).



Obrázek 7 - Outlook - WEB - možnost obnovy smazaných e-mailů

Pro někoho je zajímavou možností i funkce kalendáře, který můžeme používat v rámci více zařízení díky účtům podporujících Exchange ActiveSync (EAS). Pokud si do desktop Outlooku přidáme i dříve zmíněný Hotmail účet, máme sdílený kalendář pro více zařízení (web, PC, mobilní telefon). Na chytrém telefonu se přihlašujeme přes Microsoft účet jako do webové aplikace a kalendář je zde dostupný automaticky.

K Office365 také patří úložiště OneDrive, na kterém jsou dokumenty zpracovávané na webu uloženy. S dokumenty v rámci OneDrive je možné po přihlášení k danému Microsoft účtu pracovat napříč všemi platformami. V rámci předplatného Office365 je momentálně k dispozici desktop verze Office 2016.

V rámci Office365 může více uživatelů spolupracovat na tvorbě stejného dokumentu (Word, Excel, Powerpoint, OneNote) i z více zařízení najednou. Pro nejlepší synchronizaci a okamžité změny je vhodné používat zejména webové verze aplikací. To funguje bez problémů u všech zmíněných aplikací. Word v desktop verzi pracuje s online alternativou docela dobře. Powerpoint lze editovat zároveň ve web a desktop aplikaci, avšak synchronizace zde pokulhává. Při editaci souboru Excel je spolupráce umožněna pouze v online apli-

kaci, na ostatních platformách může pracovat pouze jeden uživatel - dokument je blokován - pouze pro čtení. U OneNote lze aplikovat stejné doporučení jako u Powerpoint.

Pokud je připojení k internetu stabilní, projevují se změny v aplikacích Word tak, jak je píšeme. Zároveň díky štítkům vidíme autora dané části, která je blokována pro změny ostatními uživateli, dokud není dokončena. Pokud dojde k přerušení spojení a nastane konflikt, např. úprava stejné části textu, zobrazí se v aplikaci nástroj pro řešení konfliktů, kde vybereme tu změnu, kterou chceme ponechat.

Může nastat situace, kdy pracujeme například na notebooku bez připojení k internetu na sdíleném dokumentu Word a zároveň dojde k jeho editaci druhým uživatelem v rámci sdíleného prostoru OneDrive (PC, web, telefon, …). Po připojení zařízení na internet se provede synchronizace. Dojde zde ke konfliktu, při kterém se vytvoří 2 kopie dokumentu, které si kromě původního názvu souboru ponesou v názvu jméno uživatele. Dále je to již na straně uživatelů, jak se s tímto vypořádají a zpracují změny zaznamenané v dokumentech. S tím je zapotřebí počítat.

Ostatní aplikace je pro spolupráci více uživatelů lepší využívat v online verzi.

Kancelářský software Office od společnosti Microsoft je nepoužívanější komerční kancelářský software. Kompatibilita aplikací s dokumenty z různých zdrojů by neměla být problémem. Bezplatnou desktop alternativou může být OpenOffice, který je také některými poskytovateli v cloudu nabízen, ale většinou za určitý poplatek

5.1.1.2 Zálohování

Microsoft u Office365 nabízí, jako u svých ostatních služeb, odolnou infrastrukturu zaručující vysokou úroveň dostupnosti. Data jsou uložena redundantně na discích v rámci serveru, na více serverech v rámci datacentra a také jsou neustále replikována v rámci geograficky oddělených datacentrech. Již na úrovni poskytovatele jsou data uložena na více místech najednou, což nám v případě HW či SW selhání zajišťuje možnost rychlé obnovy dat, kterou zajišťuje poskytovatel automatickými nástroji pro zajištění kontinuity provozu. Datacentra jsou rozmístěna prakticky po celém světě.

Smazané schránky v rámci Exchange Online jsou uchovány po 30 dní, než jsou zcela vymazány. Obnovit je lze z administrátorského účtu Office365.

Na desktopovém Outlooku můžeme provádět ruční zálohu exportem do PST souboru a pro zálohu samotného Office365 existují různé placené cloud služby (např. CloudAlly).

Pro cloudové úložiště OneDrive jsou poskytovány synchronizační aplikace pro PC, mobilní telefon, atd. Cílem je udržovat obsah úložiště OneDrive aktuální na všech zařízeních a webu. Po připojení zařízení na internet dojde automaticky k synchronizaci s cloudem, avšak mobilní verze v rámci úspory datových přenosů pouze nahlíží na dostupné soubory. Je možné si je stáhnout do zařízení, nebo nahrát do cloudu nové soubory. Při využívání těchto možností máme opět několik kopií dat na různých místech a můžeme s nimi manipulovat a případně dál zálohovat dle uvážení.

5.1.1.3 Bezpečnost

Zabezpečení začíná na fyzické úrovni omezením fyzického přístupu do prostor datacenter (využití biometrie) a také interní sítě jsou odděleny od těch externích. Za další fyzickou ochranu by se dal považovat užívaný BitLocker. Data uložená na fyzických discích v serveru jsou šifrována klíči, které jsou uloženy v šifrovacím procesoru (TPM[74]). Disk je tedy spjatý s daným HW a data na disku nelze jednoduše přečíst. Zejména ochrana proti fyzickému odcizení pevného disku. Užívá se zde algoritmus AES-256bit. Pokud stroj běží lze teoreticky klíče získat. Pokud stroj neběží, zbývá jedině dešifrování hrubou silou. U Business verze OneDrive a Sharepoint jsou dále šifrovány i jednotlivé soubory[75]. Pro správu identit a přístupů je užíván Windows Azure Active Directory. Od jednotlivých uživatelů lze vyžadovat silná hesla či případně využít vícefaktorovou autentizaci (mobilní telefon).

Pro přenos dat z Exchange serveru je využíváno šifrované spojení pomocí TLS. Pro příjem a odesílání e-mailů z Outlooku je dostupné SSL/TLS a přenos dat do webových aplikací je chráněn TLS 1.2 (AES-256bit).

5.1.1.4 Legislativa

Z pohledu ochrany osobních údajů jsou jako u Windows Azure (viz 4.3) aplikována různá opatření pro zajištění ochrany osobních údajů. Datacentra jsou rozmístěna v různých lokalitách po světě a i když jsou data primárně uchovávána v regionu jejich vytvoření (pro nás EU), mohou v některých případech fyzicky překročit hranice EU/EHS. Pro zpracování dat v rámci datacenter společnosti Microsoft jsou všechny procesy v souladu s náročnou evropskou legislativou (viz 1.2.3.1 a 4.3).

---

[74] Trusted Platform Module - zabezpečený šifrovací procesor, na který lze ukládat šifrovací klíče.
[75] Více na https://technet.microsoft.com/en-us/library/dn905447.aspx

5.1.1.5 SLA

viz bod 4.2 pro všechny části Office365

5.1.2 Forpsi webhosting

5.1.2.1 Funkcionality

E-mailová a webová adresa na doméně bezplatné služby nepůsobí příliš reprezentativně a prezentace je v dnešní době velmi důležitá. Ve všech navrhovaných řešeních bude užita samostatná doména pro danou společnost. Výběr registrátora záleží pouze na nás a našich konkrétních potřebách, tj. například konkrétní doména nejvyššího řádu[76]. V rámci možnosti praktické testu služeb jsem pro tuto práci zvolil registrátora INTERNET CZ, a.s. (dále Forpsi) a zaregistroval doménu „diplomova-prace.info“. Zřízení proběhlo rychle, od objednání přes uhrazení až po aktivaci domény neuběhla ani jedna hodina. Pod touto zřízenou doménou budou v navrhovaných řešeních teoreticky provozovány webové stránky a vlastní e-mail.

Forpsi nabízí kromě registrací domén další služby, jako webhosting (včetně možnosti poštovního serveru), flexibilní virtuální servery, dedikované servery a nebo housing[77]. Právě virtuální servery jsou ideální variantou, pokud standardní webhosting nestačí a dedikované servery jsou příliš naddimenzované. [78]

5.1.2.2 Zálohování

Zálohování je prováděno na denní bázi a zálohy jsou dostupné 7 až 14 dní zpětně dle jednotlivých služeb. Lze si také zřídit doplňkovou službu pro přístup k zálohám přes FTP pro přístup k historickým datům bez nutnosti přímého kontaktu s poskytovatelem. Případně při požadavku nahrají za poplatek vybranou zálohu na námi vybraný FTP server. V rámci webmail aplikace lze e-maily exportovat hromadně (mbox) nebo jednotlivě (eml). DNS severy jsou umístěny v oddělených geografických lokalitách a při výpadku je zde přímá

[76] TLD - Top Level Domain - CZ, SK, EU, COM, atd.
[77] Housing - umístění vlastního severu do datacentra poskytovatele
[78] https://www.forpsi.com/

náhrada pro zajištění kontinuity provozu. Také tento poskytovatel zajišťuje uložení ve více datacentrech v rámci České republiky. Data jsou i zde uložena redundantně.

5.1.2.3 Bezpečnost

Webmail obsahuje kontroly síly zadávaného hesla, které jsou prováděny při přihlášení nebo změně hesla. Uživatelské jméno, název domény nebo jejich části a kombinace nemohou být použity jako heslo. Dále jsou zakázány číselné/abecední posloupnosti nebo opakování jednoho znaku. Kromě těchto hlavních omezení jsou při volbě hesla aplikovány standardní doporučení - viz lit. [12].

Přenos dat z/do poštovního serveru je chráněn protokolem SSL/TLS. Pro přístup k e-mailu přes webmail je užito TLS 1.0 (AES-256bit) a samotná webová správa účtu na Forpsi užívá TLS 1.2 (AES-256bit).

5.1.2.4 Legislativa

Servery pro zpracování a uchování dat jsou umístěny ve dvou lokalitách v rámci české republiky. Konkrétně v Praze a v obci Ktiše. Pro zpracování osobních údajů jsou dodržována všechna bezpečnostní nařízení stanovená zákony a právními předpisy platnými v České republice a v rámci Evropské unie.

5.1.2.5 SLA

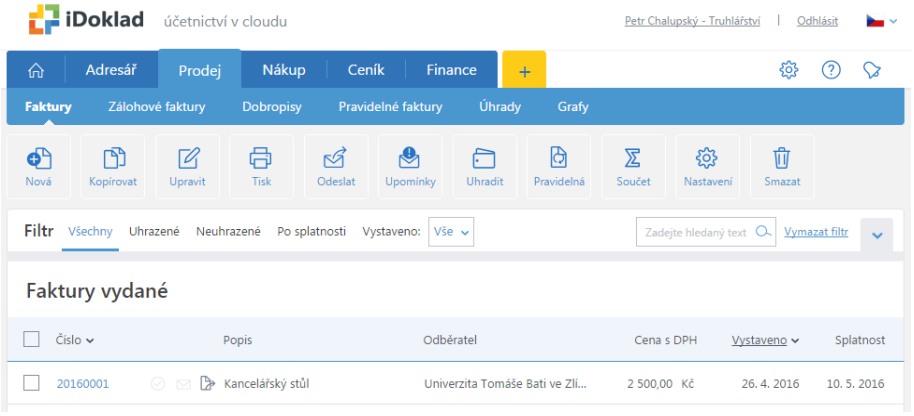
Dostupnost služeb prostřednictvím sítě internet je vypočítán na roční bázi jako 99,95 %. Při přepočtu jde maximálně o 216 minut (3h 36min) nedostupnosti služeb ročně a při nedodržení této garantované dostupnosti je forma kompenzace ve formě kreditu (slevy) z nákladů na službu. Každých 15 minut nedostupnosti služeb nad limit zmíněný výše je kompenzováno slevou 5 %. Maximální limit pro započítání kreditu je 300 minut nedostupnosti, což poté činí 100 % slevu z nákladů na službu (20 * 15 minut = 20 * 5 %) za jedno měsíční období dle typu fakturace. Přesné podmínky nároku na kredit jsou uvedeny v SLA.

5.1.3 iDoklad - účetnictví v cloudu

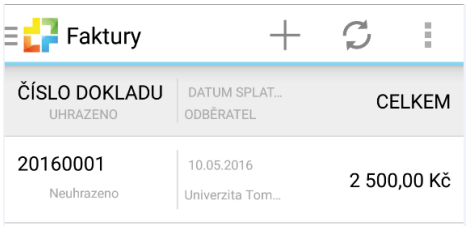
5.1.3.1 Funkcionality

Pro potřeby fakturace můžeme využít mnoho nástrojů od tužky a papíru přes excelovské tabulky až po specializovaný software. Máme-li software cloudu a na ověřené platformě

(Windows Azure), můžeme standardní fakturaci a práci s papíry povznést na vyšší úroveň. Aplikace iDoklad umožňuje vystavovat a tisknout faktury z webového prohlížeče (viz Obrázek 8) nebo v aplikaci na mobilním zařízení (viz Obrázek 9)[79].



Obrázek 8 - iDoklad - WEB



Obrázek 9 - iDoklad - Android

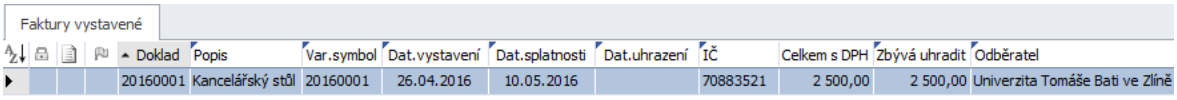
Nejsme závislí na konkrétním počítači, kde by byl standardně software instalován a data uchována. Je možné si vést databázi už pořízených dokladů, kontaktů a ceníkových položek. Navíc se nám dostává:

- Přehled o všech operacích
- Automatické načítání dat z ARES[80]
- Kontrola bezdlužnosti klientů
- Odeslání faktur účetní firmě

[79] Aplikace je dostupná pro zařízení s OS: Android, Windows Phone, iOS
[80] ARES - Administrativní registr ekonomických subjektů

- Pohledové sestavy na vystavené faktury
- Upomínky partnerům za neuhrazené faktury
- Párování úhrad s bankou
- A další…

iDoklad je zdarma a od vývojářů účetního softwaru Money. Velkou výhodou této aplikace je možnost propojení s účetním softwarem kdy je možné nahrávat vystavené faktury do zvolného softwaru[81], kde je stačí pouze zaúčtovat (viz Obrázek 10). A to ať si účetnictví vedeme sami nebo máme svého účetního.[82]



Obrázek 10 - Money S3

5.1.3.2 Zálohování

O možnostech ochrany dat před ztrátou a zálohovacích mechanismech platformy Windows Azure již bylo psáno dříve (např. viz 5.1.1.2). To samé platí i pro iDoklad, který z důvodu redundantnosti dat a dostupnosti provozován paralelně minimálně na dvou virtuálních serverech (dle zátěže) v různých hostingových centrech. V případě výpadku se automaticky provádí synchronizace do třetího datacentra. Data v cloudu jsou umístěna redundantně v rámci serveru, datacentra a zároveň v různých geografických lokalitách dle samotné podstaty platformy Azure. Navíc provádí poskytovatel služby iDoklad zálohování veškerých dat automaticky na záložní média jedenkrát denně (v nočních hodinách). Je možné také provést export dat například do formátů xls a pdf.

5.1.3.3 Bezpečnost

O mechanismech zabezpečení platformy Windows Azure již bylo psáno (např. viz 5.1.1.3). Komunikace mezi serverem služby a klientským zařízením je chráněna protokolem TLS 1.2 (AES-256bit).

---

[81] Momentálně je možné propojení s Money (S3, S4, S5), Pohoda a Altus Vario - více na www.money.cz
[82] https://www.idoklad.cz/

5.1.3.4 Legislativa

Služby běží paralelně ve dvou hostingových centrech cloudu Windows Azure v EU. Již samotná platforma Azure splňuje požadavky na ochranu osobních údajů (viz 4.3) a fyzické umístění dat v EU není nutné, ale zvyšuje pocit jistoty. Samotná aplikace je pravidelně aktualizována pro soulad s aktuální legislativou. Osobní údaje předané při registraci do služby jsou používány výhradně pro správnou funkčnost aplikace, potřeby fakturace a klientskou podporu. V rámci služby je možné pracovat také s digitálním podpisem.

5.1.3.5 SLA

Jelikož je služba nabízena zdarma, není zde standardní SLA uvedeno. Provoz je však realizován na platformě Azure a prostředky k provozu služby podléhají SLA právě této platformy (viz 4.2). Jelikož jde o službu zdarma, provozovatel uvádí výslovné neposkytování žádných záruk na aplikaci. Teoreticky může být služba kdykoliv ukončena či zpoplatněna, ale vzhledem k záměrnému napojení na účetní software od stejného vývojáře je v jeho zájmu službu tuto službu provozovat.

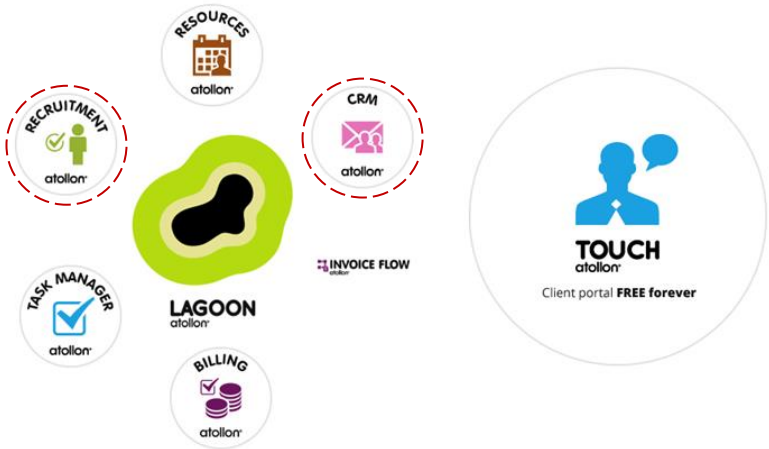
5.1.4 Atollon Lagoon

5.1.4.1 Funkcionality

Řešení Atollon Lagoon je modulární platforma se širokou škálou nástrojů pro řízení procesů celé firmy, dodávané společností Atollon Limited. Platforma Lagoon obsahuje moduly CRM, Recruitment, Billing, Resources, Task Manager, Invoice Flow a modul Touch pro komunikaci s klienty (Obrázek 11). Shrnutí z www.atollon.cz:

- **CRM** - Nástroj ro řízení a automatizaci procesů. Správa klientů včetně historie a jejich životního cyklu, plánování, komunikace v rámci firmy či e-mailový/SMS kontakt přímo ze systému. Automatizace rutinních procesů, katalog zboží a služeb, sdílené kalendáře, správa požadavků, vytváření sestav, centralizace firemních dat, reporting a mnoho dalšího.
- **Recruitment** - Řešení pro automatizaci náborových činností s vyhledávácími a reportovacími nástroji. Databáze uchazečů, import a parsing CV do systému, propojení na web a pracovní portály, tvorba profilů z dat uchazečů, propojení s CRM, atd.

- **Billing** - Systém pro fakturaci a vyúčtování služeb s procesem schvalování faktur. Možnost indvividualizace dle klientů, využití podkladů od ostatních uživatelů, účtování hodin, opakovaná vyúčtování, apod.
- **Resources** - Nástroj pro sledování a řízení alokace lidských zdrojů. Měření úrovně využití lidských zdrojů, přiřazování úkolů či projektů, vykazování odpracovaného času, plánová schůzek, dlouhodobá rezervace pracovníků, atd.
- **Task Manager** - Správa úkolů týmů či celé firmy. Eskalované upomínky termínů, opakované úkoly, kontrolní soupisy k úkolům, konfigurovatelné workflow, apod.
- **Invoice Flow** - Automatizace fakturace pro omezení ručního zpracování dat. Automatický import faktur s využitím OCR, samostatná schránka pro automatizaci zpracování faktur v digitální podobě, zanesení faktur do účetnictví, procesy schvalování, sledování nákladových středisek a jiné.
- **Touch** - Prostředí pro komunikaci s klienty. Správa požadavků klientů a dodavatelů, přehled termínů a obchodních podmínek, přehled vedené komunikace. Toto prostředí je pro všechny účastníky zdarma.



Obrázek 11 - Platforma Atollon Lagoon

Jednotlivé části platformy Lagoon jsou propojeny a funkce celého systému si určujeme dle vybraných modulů. SOA architektura umožňuje využívat služeb systému pomocí vlastních aplikací nebo aplikací třetích stran. Pro uživatelský přístup lze využít tenkého klienta pro MS Windows nebo prostředí webového klienta pro práci z jakéhokoliv prohlížeče a systému. Kalendář, úkoly a kontakty lze synchronizovat s Google Apps či MS Office. Synchronizaci kalendáře lze využít pro účely reportingu v Atollonu, ať již pro vykazování obchodních aktivit nebo výkazy práce

Atollon lze také implementovat s již předkonfigurovanými řešením pro různé obory, např. vývojářské společnosti, účetní společnosti, call centra, konzultační a školící organizace, personální agentury, atd.

5.1.4.2 Zálohování

Veškerá data jsou zálohována na denní bázi. Samotná záloha je umísťována do jiné fyzické lokace, než je hardware, na kterém jsou služby provozovány. Zálohované SQL databáze je možné zpřístupnit pod zaheslovaným přístupem. Tenký klient disponuje reportovacími nástroji, kterými můžeme potřebné informace přenést do CSV formátu a webové prostředí disponuje reportovacími sestavami. Ovšem těmito cestami získáme pouze některé údaje.

5.1.4.3 Bezpečnost

Veškerý tok informací mezi serverem a klientskou stranou je chráněn protokolem TLS 1.2 (AES-128bit). Přístup do služby může být omezen pouze na vybrané lokace (např. firemní kanceláře) využitím integrovaného firewallu. Také je možné si vyžádat vícefaktorovou autentizaci pomocí tokenů. Přístupových oprávnění je využíváno i pro řízení přístupů k důležitým informacím v systému a lze s nimi pracovat v rámci skupin či rolí. Fyzický přístup k serverům v rámci hostingového centra mají pouze jeho zaměstnanci a zaměstnanci firmy Atollon.

5.1.4.4 Legislativa

Atollon využívá služeb jednoho z hostingových center v Praze, data jsou tedy zpracovávána v ČR, potažmo EU. V rámci ochrany osobních údajů jsou dodržována všechna nařízení stanovená zákony a právními předpisy platnými v České republice a zároveň v rámci Evropské unie.

5.1.4.5 SLA

Dostupnost služeb je garantována na úrovni 99 %. Při kalendářním měsíci o 30 dnech jde o potenciální nedostupnost 432 minut (7,2 hodiny). Do tohoto období se započítávají veškeré důvody nedostupnosti, včetně plánové údržby a problémy způsobené vnějšími okolnostmi a vlivy. Plánované údržby se provádí od 1 do 3 hodiny ranní, případně o víkendu.

Neplánovaný výpadek dostupnosti systému je kompenzován při dosažení stanovených podmínek. Pro tyto případy je definována 1 jednotka, která činí 30 minut. Pro započítání jednotky nedostupnosti musí problém trvat více než zmíněných 30 minut a zaručují, že

výpadek služeb nepřekročí 2 jednotky v kalendářním měsíci. Za každou jednotku výpadku bude z vyúčtování sleven 1 den užívání služeb a za 1 kalendářní měsíc může být od vyúčtování odečteno maximálně 7 dní.

5.1.5 Windows Azure

5.1.5.1 Funkcionality

Azure je robustní cloud platforma pro vytváření, hostování a škálování webových aplikací skrze datacentra Microsoftu. Množství nabízených služeb je obrovské, ale pro naše účely bude využito pouze služeb Web Apps, Storage a Batch:[83]

Web Apps - Umožňuje rychlé nasazení webových stránek nebo aplikací/API sestavených v jazycích .NET, Node.js, PHP, Python a Java. Hotové stránky lze pouze nahrát přes FTP, nebo přímo vyvíjet v integrovaném prostředí. Lze také využít již existující API ke službám Azure nebo si sestavit vlastní. Pro zajištění dostupnosti webových stránek je integrováno automatické škálování kapacit a je možné replikovat provoz do více geografických oblastí pro lepší uživatelskou dostupnost.

Storage - Úložiště pro jakékoliv množství a jakoukoliv formu dat, které lze propojit s dalšími službami nejen v rámci Azure. Úložný prostor lze pomocí funkce Data Factory propojit s on-premise stroji a lokálně uložená data synchronizovat do cloud úložiště. Data jsou v jedné oblasti uchována ve třech kopiích a lze si zvolit jinou geografickou lokalitu s dalšími třemi kopiemi pro zajištění vyšší dostupnosti a rychlejší zotavení po havárii.

Batch - Škálování výpočetních úloh na desítky, stovky či tisíce virtuálních počítačů. Počet využitých VM je možné měnit v průběhu zpracování a tím zkracovat dobu zpracování celé úlohy. Tuto výpočetní techniku lze aplikovat prakticky na jakékoliv výpočetní problémy včetně vykreslování animovaných scén pro třetí modelovou společnost. Pomocí integrovaného plánovače lze řadit úkoly do fronty, rozvrhovat či sledovat stav. Při selhání výpočtu úlohy řadí úlohu znovu do fronty. S tím jak se celý úkol postupně dokončuje, jednotlivé VM se vypínají. Po dokončení renderingu se jednotlivé snímky sloučí do výsledného videa, nebo můžeme pracovat s jednotlivými snímky, které jsou uložené na úložišti Storage.

---

[83] https://azure.microsoft.com/cs-cz/

5.1.5.2 Zálohování

Formy zálohování byly již popsány v části 5.1.1.2.

5.1.5.3 Bezpečnost

Bezpečnostní opatření a postupy společné i pro Azure viz 5.1.1.2.

5.1.5.4 Legislativa

Legislativní otázky, zejména ohledně zpracování osobních údajů, byly podrobně rozebrány v části 4.3.

5.1.5.5 SLA

Podrobnosti ohledně SLA pro Azure uvedeny v části 4.2.

5.1.6 YouTube

5.1.6.1 Funkcionality

YouTube je největší internetový server na sdílení videí, který v roce 2006 odkoupila společnost Google a nyní se řadí mezi ostatní aplikace v Google Apps. Pokud chce firma nahrávat videa do této služby, postačí mít vytvořený uživatelský Google účet. Dále je možné vytvářet různé kanály a tak například třídit svá videa do různých kategorií v rámci jednoho účtu. Videa můžeme přehrávat přímo na stránkách služby nebo je vkládat na jiné stránky.[84]

5.1.6.2 Zálohování

Jelikož služba patří pod Google, vztahují se na ní všechny procesy aplikované na jejich služby. Veškerá data jsou rozdělena na menší části zvané „chunks“ a jsou replikována na více serverů a více datancenter zároveň tak, aby při selhání některé z úložných části byla data lehce obnovitelná. Jednotlivé služby jsou provozovány na více serverech a ve více datacentrech zároveň. V případě nedostupnosti jednoho serveru je uživatel automaticky přesměrován na jiný.

[84] https://www.google.com/support/

Na YouTube lze stáhnout námi nahraná videa jednotlivě nebo v kompletním balíku a původní kvalitě.

5.1.6.3 Bezpečnost

Podobně jako u služeb od Microsoftu jsou aplikována bezpečnostní opatření na mnoha úrovních. Samotná videa však na serverech Google nejsou zvláštně šifrována. Pro zabezpečení komunikace mezi servery Google a klientskými aplikacemi je užito protokolu TLS (AES-128bit).

5.1.6.4 Legislativa

Videa ze své podstaty neobsahují citlivé informace, jako osobní údaje, není tedy nutné řešit jejich ochranu. Za obsah samotných videí je zodpovědný jejich autor.

5.1.6.5 SLA

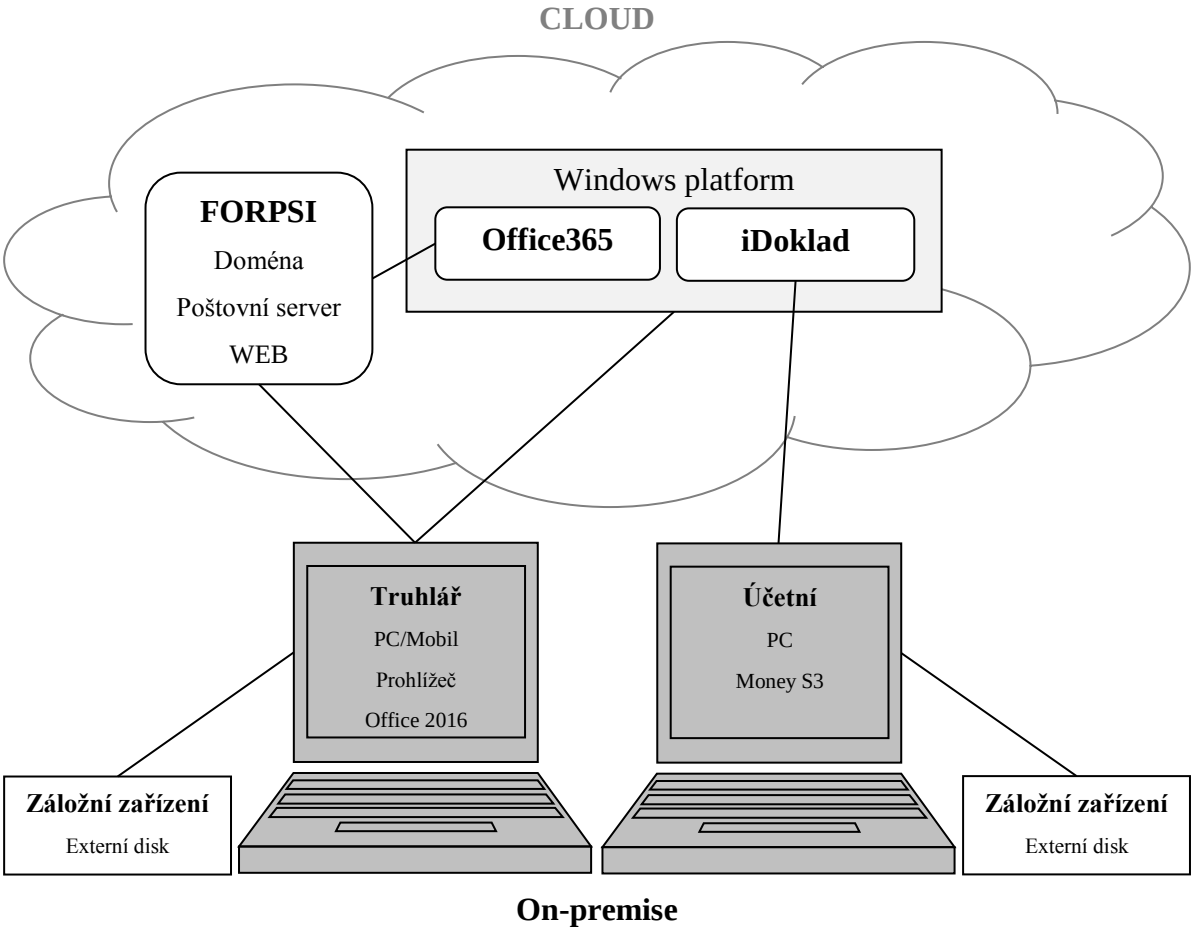
Google garantuje u svých služeb, obdobně jako Microsoft, 99,9 % dostupnost. Využíváme ale bezplatný účet Google a žádné kompenzace se zde v případě nedostupnosti služby neaplikují.

5.2 Společnost s mírnou závislostí na ICT

Pro tuto kategorii bylo zvoleno malé truhlářství, které pro výkon činnosti počítač ani software nepotřebují. Stroje a ruční práce vyžadující pouze samotného člověka. Pro podpůrné činnosti však již počítač potřebný je.

5.2.1 Návrh řešení

Pro prvotní seznámení se strukturou navrhovaného řešení jsem využil nákres, viz Obrázek 12. Office365 a iDoklad využívají cloudové platformy od společnosti Microsoft.



Obrázek 12 - Návrh využití cloud služeb u společnosti s mírnou závislostí na ICT

O důležitosti dobré prezentace v dnešní době velmi dobře ví i náš začínající truhlář a proto si hned na začátku podnikání zaregistruje vlastní doménu. Potřebujeme prostor pro webovou prezentaci a poštovní server, kde využijeme zaregistrovanou doménu. Takto malý subjekt nebude investovat do vlastního poštovního serveru či serveru pro provoz internetových

stránek. Využijeme možností hostingu Forpsi pro provoz webu a pro správu e-mailu. V rámci této práce bylo využito zkušební 18 denní doby.

Možnosti zvolené varianty Easy jsou následující:

- neomezený prostor pro web
- neomezený počet emailových schránek
- PHP 7.0, .NET 4.5
- 1x neomezená databáze (MySQL, MSSQL, PgSQL)
- 5x subdoména, 5x alias - v ceně
- 5x GigaMail (celkem v ceně 25 GB pro e-maily) - min 1 GB na jednu schránku
- zálohování, Business mail

Pro tuto společnost byla vytvořena e-mailová schránka „truhlarstvi@diplomova-prace.info“. Pro samotný přístup do schránky však nebude primárně využíván web-mail.forpsi.com, ale Outlook od společnosti Microsoft.

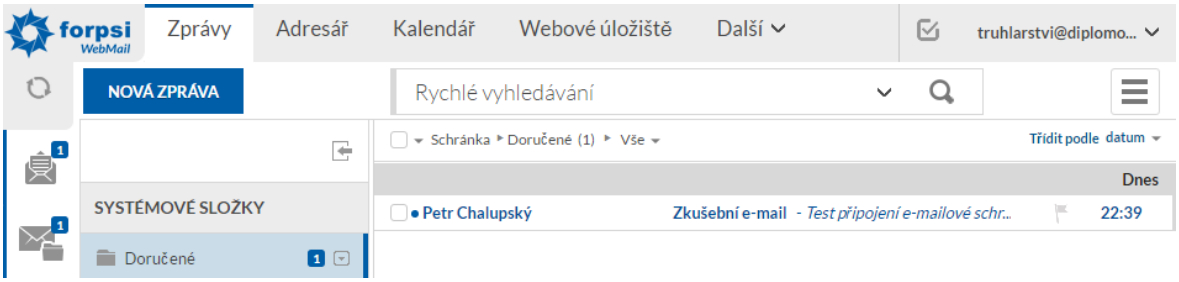
To již prozrazuje volbu kancelářského balíku aplikací - Office365. Konkrétně varianta Business, která obsahuje následující aplikace:

- Outlook
- Word
- Excel
- Powerpoint
- OneNote
- Publisher
- OneDrive s 1 TB pro ukládání a sdílení souborů

Pro představu 2 roky užívání Office365 Business jedním uživatelem je přibližně stejně nákladné jako 1 licence pro desktop verzi Office 2016[85].

E-mailová schránka bude spravována provozovatelem hostingu, zdrojové prostředí vyobrazeno na Obrázku 13.

[85] Údaje k měsíci Duben, roku 2016



Obrázek 13 - Webmail FORPSI

Přistupovat do ní můžeme přímo ze stránek poskytovatele (webmail) nebo z Outlooku (desktop - Obrázek 4, web - Obrázek 5, mobilní zařízení - Obrázek 6), kde schránku připojíme jako další účet. Stačí pouze nastavit POP3/IMAP a SMTP údaje a zahájí se synchronizace s poštovním serverem.

5.2.1.1 Zálohování

Webové stránky a databáze s nimi spojené jsou pravidelně zálohovány poskytovatelem hostingu a zálohy lze zpřístupnit na FTP serveru. Tyto zálohy si lze v případě potřeby stáhnout a uložit na externí disk.

Díky dříve zmíněným možnostem můžeme mít e-maily uloženy na více místech najednou. Servery poskytovatele hostingu, cloud prostředí Office365, desktop verze Outlook. Z PC verze poštovního klienta bude prováděna záloha pošty (do souboru pst) na konci každého pracovního týdne na externí disk.

Dokumenty z OneDrive jsou primárně uloženy na cloud infrastruktuře společnosti Microsoft a automaticky se nahrávají do připojených zařízení. Pokud nějaké zařízení přestane fungovat, máme kopie na ostatních zařízeních. Pro vlastní zálohu lze použít externí disk.

Díky napojení na software Money S3 jenž je spravovaný najatou účetní, se informace potřebné k účtování přenášejí do jejího PC, kde je realizována záloha veškeré účetnictví v její správě na externí disk. Samotné faktury v PDF budou individuálně ukládány na externí disk u podnikatele. Dostupné budou na webu v dané službě a na zmíněném externím disku.

5.2.1.2 Bezpečnost

Pro služby Office365 a iDoklad je využitá silná infrastruktura společnosti Microsoft. Všechny 3 služby mají podporu bezpečného hesla a uživatele nutí nepoužívat primitivní, snadno uhodnutelná, či hrubou silou (Brute Force) prolomitelná hesla. Veškerá komunika-

ce mezi servery jednotlivých služeb a využívanými zařízeními je šifrována TLS protokolem (AES-256bit). Koncový počítač podnikatele bude osazen komplexní ochranou ESET Smart Security.

5.2.1.3 Legislativa

Všechna použitá řešení splňují potřebné mechanismy pro ochranu osobních údajů i pro náročné prostředí, jakým EU bezesporu je. Veškerá komunikace je šifrována a tím je splněna jedna z hlavních zásad při ochraně osobních údajů. Souhlas se zpracováním osobních údajů je u všech služeb poskytován uživatel po dobu nezbytně nutnou, tj. po dobu užívání služeb.

5.2.1.4 SLA

Všechny služby mají vysokou garantovanou dostupnost, avšak teoretickým slabým článkem může být služba iDoklad. Je bezplatná a není zde žádná garance dostupnosti na úrovni samotné aplikace.

5.2.2 Možná řešení při nedostupnosti cloud služeb

Pro samotný výkon předmětu podnikání není ani jedna z využívaných služeb stěžejní a jsme schopni při jejich výpadku pokračovat v produkci nábytku. Objednávky můžeme přijímat telefonicky nebo osobně a samotná výroba zabere většinou více času, takže i celodenní výpadek nemusí chod takto malé a zaměřené firmy ovlivnit.

5.2.2.1 Nedostupnost webových stránek

Webové stránky slouží pro prezentaci firmy jako takové a není zde provozován e-shop. Krátkodobý výpadek může lehce snížit kredit firmy, ale ne zásadně. Pokud by poskytovatel webhostingu nečekaně ukončil činnost, přesuneme poslední zálohu do nového webhostingu. Stránky fungují spíše jako veřejně dostupná vizitka.

5.2.2.2 Nedostupnost e-mailu

E-mail je jedna z možných cest, kterou firma pro komunikaci využívá. Přijímá a provádí objednávky, komunikuje se zákazníky, s úřady a ostatními subjekty. V případě nedostupnosti jsou zde i jiné varianty komunikace. Jelikož je e-mail provozován na několika systémech a zařízeních, může k nedostupnosti dojít na více úrovních. Prvotní úroveň je u posky-

tovatele poštovního serveru, a pokud problém tkví zde, je e-mail na zakoupené doméně mimo dosah. Během výpadku můžeme využít bezplatné e-mailové služby s tím, že se k novým e-mailům na naší doméně dostaneme po zprovoznění příslušného serveru. V případě nedostupnosti cílového severu (ten náš) se zdrojový server pokouší e-mail doručit opakovaně. Samotná zpráva se tedy jen tak neztratí a bude doručena po opětovném spuštění poštovního serveru.

5.2.2.3 Nedostupnost Office365

Zde využíváme poštovního klienta, ostatní standardní kancelářské aplikace (web, PC, mobilní zařízení) a úložiště OneDrive. V rámci Business varianty této služby jsou k dispozici desktop verze aplikací na PC, ve kterých můžeme pracovat na daném PC. Při výpadku samozřejmě přicházíme o možnost použít službu z jakéhokoliv zařízení a o možnost spolupráce. V případě této firmy to ale není stěžejní problém. Po opětovném zprovoznění služby dojde k synchronizaci dokumentů na OneDrive a ke stažení e-mailů z poštovního serveru.

5.2.2.4 Nedostupnost iDoklad

Specifika a množnosti této služby byly již popsány, ale jejím elementárním posláním je tvorba faktur. Ty mají své specifické náležitosti, které je nutné na nich uvést. Nezáleží však na tom, v čem budou vytvořeny, ani jaký budou mít vzhled. V případě výpadku služby a nutnosti fakturovat můžeme zřídit buď jinou cloud službu na fakturování nebo například využít balíku Office (Excel nebo Word) a v provizorní šabloně vytvořit fakturu.

5.2.3 Závažnost nedostupnosti služeb

Služba	1 hodina	4 hodiny	8 hodin	1 den	3 dny	> 1 týden
Webhosting						
Poštovní server						
Office365						
iDoklad						

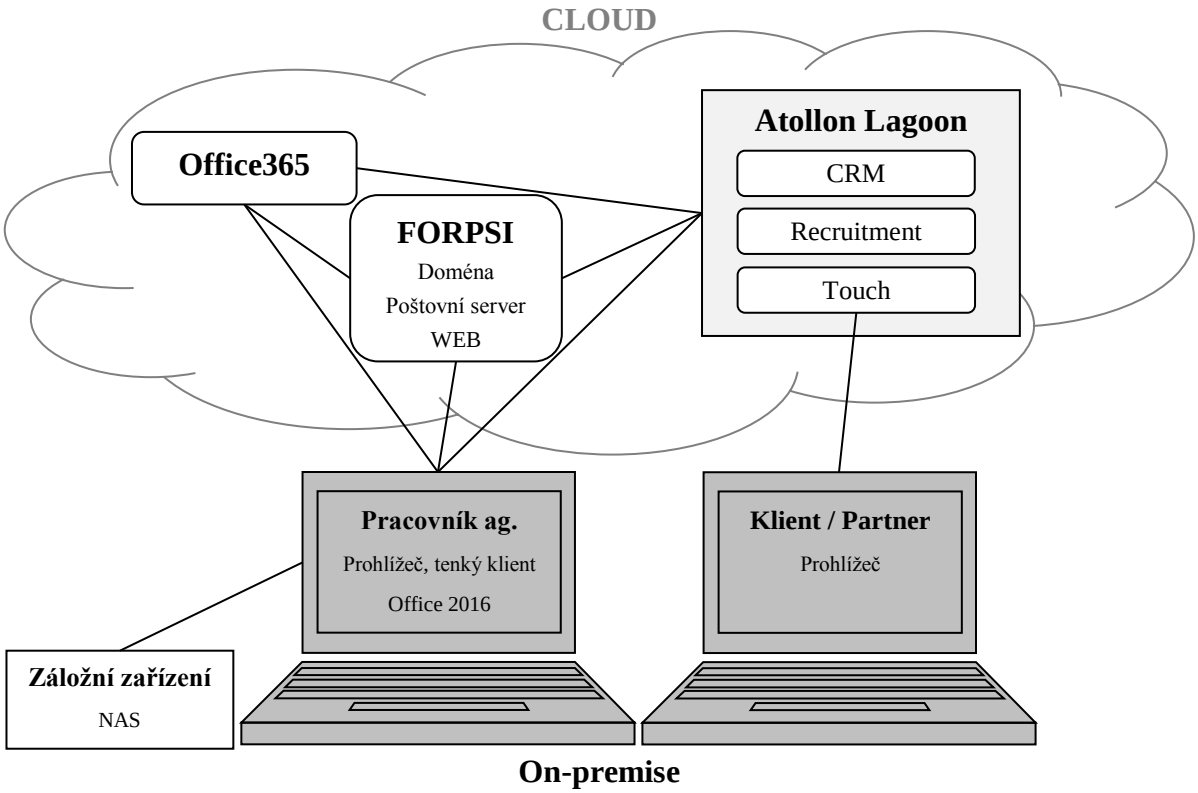
Tabulka 7 - Míry závažnosti nedostupnosti služeb u truhláře živnostníka

5.3 Společnost se střední závislostí na ICT

Druhou kategorii zastupuje personální agentura, která pro své klienty zajišťuje nábor zaměstnanců. V nabídce je také realizace či zprostředkování rekvalifikačních a odborných kurzů pro uchazeče o zaměstnání. Veškerá správa a evidence uchazečů, nabídek práce atd. probíhá elektronicky. Komunikace a výměna dokumentů probíhá elektronickou či fyzickou formou. Samotné pohovory a rekvalifikační kurzy jsou realizovány zejména v prostorách firmy. V rámci všech aktivit nesmíme opomenout možnost telefonického kontaktu.

5.3.1 Návrh řešení

Struktura navrhovaného řešení je vyobrazena na Obrázku 14.



Obrázek 14 - Návrh využití cloud služeb u společnosti se střední závislostí na ICT

Důležitost elektronické prezentace již byla zmíněna v části 5.2.1. Volné pracovní pozice budou nabízeny prostřednictvím pracovních portálů a na webu agentury - správně zvolená doména hraje svou roli. Vše se na web posílá automaticky z modulu Recruitment. V této společnosti nejsou zaměstnáni IT pracovníci pro správu serverů a využijeme tedy služeb Forpsi, jako u předchozí společnosti. Webhosting bude realizován variantou Easy (viz 5.2.1). Hlavní systém Atollon sice nabízí i poštovní server, ale abychom všechny důležité části systému nevsadili na jednu kartu, ponecháme poštovní server u Forpsi. Pokud by-

chom chtěli využít poštovní server v rámci služby Atollon, postačí v administraci domény u Forpsi upravit DNS záznamy, konkrétně záznamy MX.

Pro tuto společnost byla vytvořena e-mailová schránka „personalni-agentura@diplomova-prace.info“. Pro přístup do schránky bude primárně využíván systém Atollon (jako poštovní klient), ale lze využít jakoukoliv aplikaci Outlook.

Jako kancelářský balík je také zvolen Office365 ve verzi Business (viz 5.2.1), která je pro tuto situaci z hlediska obsažených aplikací nejvhodnější. Budou využívány zejména desktop aplikace Office 2016.

Z platformy Atollon Lagoon jsou pro tento návrh zapotřebí 2 moduly, a to CRM a Recruitment (viz Obrázek 11). Pro komunikaci firmy s klienty bude využíváno také prostředí Touch v rámci této platformy. V případě potřeby lze další části této platformy aktivovat.

Jak již bylo zmíněno v části 5.1.4.1, kalendář v Atollon Lagoon lze synchronizovat s kalendářem MS Office a Google Apps. Napojíme tedy do Lagoon kalendáře z MS Office a Google Apps z firemních Android telefonů. Všechna důležitá data budou mít pracovníci automaticky v softwaru Office na všech platformách a také v telefonu na cestách.

5.3.1.1 Zálohování

Pro potřeby zálohování a přístupu k těmto zálohám je pořízen NAS. Bude připojen k firemní síti a zároveň bude dostupný prostřednictvím webového prostředí odkudkoliv.

Webové stránky s nabídkami práce jsou pravidelně zálohovány poskytovatelem hostingu a lze k nim přistupovat skrze FTP. V případě potřeby je lze stáhnout a uložit na NAS.

E-maily můžeme mít uloženy na mnoha místech najednou. Poštovní server, Office365, desktop Outlook, mobile Outlook, Atollon Lagoon. Kromě poštovního serveru jsou to vše klienti, takže pro stažení e-mailu ze serveru musí u aplikace proběhnout synchronizace. Z PC verze poštovního klienta bude každý pracovník dle svého uvážení provádět zálohu pošty (do souboru pst) a bude zálohovat svou poštu na síťový NAS.

Dokumenty uložené na úložišti OneDrive jsou uloženy na mnoha místech najednou (viz 5.2.1.1), v případě potřeby budou uloženy pracovníky na NAS.

V Atollon Lagoon si lze vyžádat zálohu SQL databází a ty si následně uložit na NAS, a to například kvůli vedené databázi kontaktů. Základní výstupy do CSV lze provést v tenkém klientovi i webovém prostředí.

5.3.1.2 Bezpečnost

O bezpečnosti služby Office365a její platformy již bylo psáno například v částech 5.1.1.3 či 5.2.1.2. Veškerý přenos dat skrze internet je chráněn protokolem TLS. Systém od Atollon využívá šifrování v 128bit verzi a ostatní služby 256bit. U Atollon Lagoon si lze vyžádat realizaci vícefaktorové autentizace pomocí tokenů či přístupová omezení na úrovni firewallu. Koncové počítače pracovníků agentury budou osazeny komplexní ochranou ESET v balíku pro firmy ESET Secure Office+.

5.3.1.3 Legislativa

Služby Forpsi a Atollon Lagoon jsou hostovány přímo v ČR. Office365 je sice mezinárodně hostovaná služba, ale disponuje všemi potřebnými nástroji a procesy pro dodržení ochrany osobních údajů pocházejících z EU. Ostatní obecné legislativní prvky jsou shodné s těmi uvedenými v 5.2.1.3.

5.3.1.4 SLA

Všechny využité služby v navrhovaném řešení mají vysokou garantovanou dostupnost a mají nastavenou kompenzaci ve formě slev z vyúčtování při nedodržení garantované dostupnosti. Z pohledu SLA zde nevidím závažnější problém.

5.3.2 Možná řešení při nedostupnosti cloud služeb

Pro výkon činnosti je systém s daty a e-mailové komunikace zásadní, avšak tyto zdroje nejsou nezbytně nutné pro výkon všech činností a po celou pracovní dobu. Krátkodobý či částečný výpadek cloud služeb tedy neochromí celou firmu.

5.3.2.1 Nedostupnost webových stránek

Na webových stránkách agentura sebe sama propaguje a zároveň díky komponentě od Atollo může rovnou z Lagoon prezentovat pozice na svém webu. Dále jsou nabízené pozice odesílány rovnou na vybrané pracovní portály. Při výpadku webhostingu webu sice může jméno firmy utrpět, ale nabízené pozice jsou vystaveny na pracovních portálech, které lidé navštíví spíše, než přímo na web agentury. Pokud budeme chtít změnit webhosting a nebo užívaný hosting ukončil činnost, přesuneme poslední zálohu webu z NAS k jinému poskytovateli webhostingu.

5.3.2.2 Nedostupnost e-mailu

Společnost pro komunikaci používá telefon, osobní kontakt a e-mail. Prostřednictvím e-mailu přijímá od uchazečů životopisy, komunikuje s klienty, úřady a dalšími subjekty. V případě výpadku poštovního serveru bychom mohli postupovat viz druhý odstavec 5.3.2.5, anebo v systému Atollo Lagoon změnit správu pošty modu klient na server. S tím by bylo nutné změnit MX záznamy u správce domény. U dalších e-mailových klientů (Outlook) bychom museli, v případě jejich potřeby, změnit SMTP a IMAP/POP3 údaje pro přesměrování na nový server.

5.3.2.3 Nedostupnost Office365

V této společnosti budou využívány zejména desktop verze Office 2016 na firemních počítačích v prostorách společnosti. Webové kancelářské aplikace a úložiště jsou spíše bonusem, například pro práci z domova, k potřebnému balíku Office. Po opětovném zprovoznění služeb dojde k jejich synchronizaci s ostatními zařízeními.

5.3.2.4 Nedostupnost Atollon Lagoon

V rámci pracovního procesu agentury probíhá většina důležité práce právě v rámci tohoto systému. Při výpadku služby přicházíme o jednoho e-mailového klienta, ale pro to zde máme náhrady v Office365 a přímo u poskytovatele poštovního serveru. Kalendáře jsou synchronizované v MS Office a Google Apps. Důležité dokumenty a SQL databáze ze systému mohou být uloženy na firemním NAS, ale to již záleží na iniciativě samotných uživatelů. Při nedostupnosti tohoto systému přichází agentura o funkce CRM a Recruitment zmíněné v 5.1.4.1. Zásadní denní pracovní oblasti jako osobní pohovory, rekvalifikační kurzy a komunikaci lze bez hlavního systému realizovat. Po obnovení provozu se provede synchronizace a pracovníci doplní nově získaná data vedení v Atollo Lagoon.

5.3.3 Závažnost nedostupnosti služeb

Služba	1 hodina	4 hodiny	8 hodin	1 den	3 dny	> 1 týden
Webhosting						
Poštovní server						
Office365						
Atollon Lagoon						

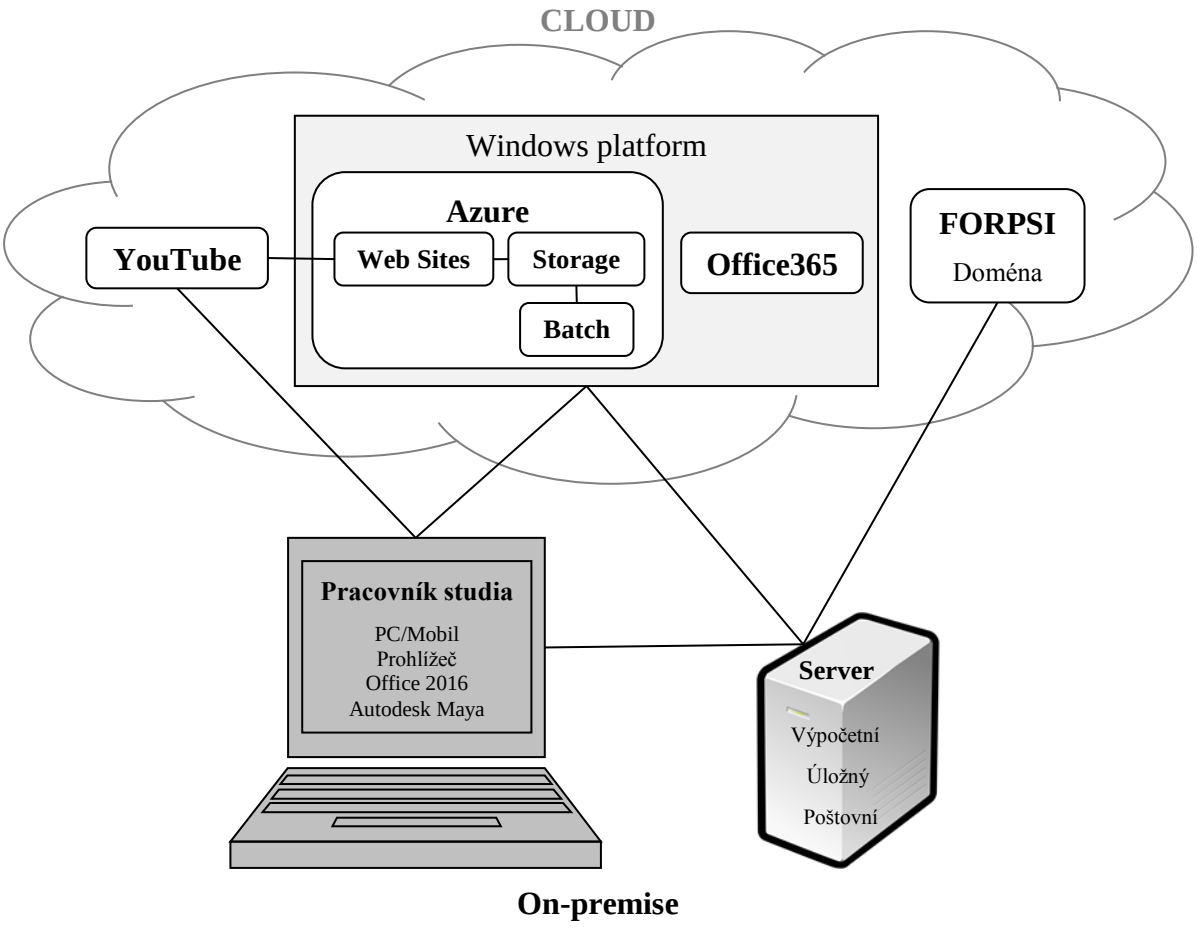
Tabulka 8 - Míry závažnosti nedostupnosti služeb u personální agentury

5.4 Společnost s úplnou závislostí na ICT

Třetí kategorii s nejsilnější závislostí na ICT při výkonu předmětu podnikání reprezentuje animační studio. Hlavní náplní studia je práce v Autodesk Maya, a dalších souvisejících programech, na tvorbě 3D animací či 3D obrázků všeho druhu. Může jít o celovečerní či krátkometrážní animované filmy, vizuální efekty do hraných filmů, 3D modely pro renderování reálně vypadajících obrázků, reklamy, apod. Prakticky vše, kde se dá uplatnit 3D grafická tvorba, jenž je dnes velmi žádaná v mnoha oblastech.

5.4.1 Návrh řešení

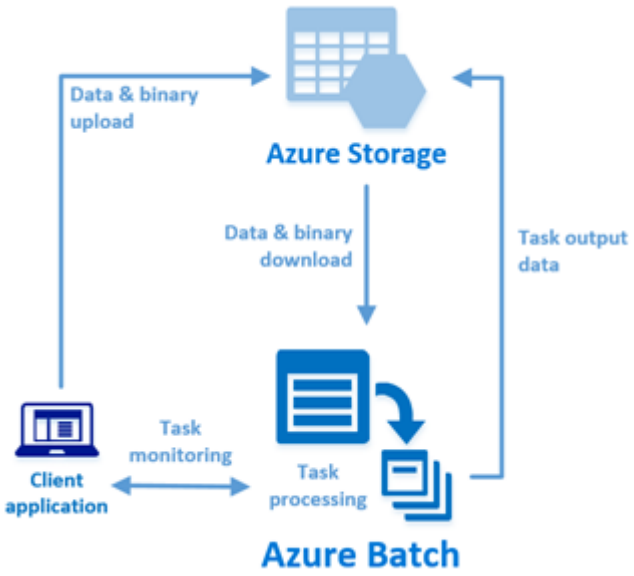
Na Obrázku 15 je graficky znázorněn návrh řešení využití cloud služeb pro animační studio. Tentokrát jsou vybrané služby prakticky pouze z repertoáru firmy Microsoft. To s sebou přináší výhody snadného propojení jednotlivých částí a zároveň nevýhody jednoho poskytovatele.



Obrázek 15 - Návrh využití cloud služeb u společnosti s úplnou závislostí na ICT

Microsoft je však velká a stabilní firma a v tomto případě není zapotřebí obávat se varianty pouze jednoho poskytovatele.

Při renderingu je zapotřebí obrovský výpočetní výkon a výstavba vlastního výpočetního centra je velmi nákladná. Jako nová firma si nemůže investice do potřebného centra dovolit, avšak pro základní výpočetní možnosti je pořízen server. Pro hlavní výpočetní potřeby využijeme možností platformy Azure, a to konkrétně služby Batch. Ve spojení se službou Storage lze renderovat a ukládat výstup z aplikace Autodesk Maya přímo v cloudu (viz Obrázek 16). Rendering videí probíhá po jednotlivých snímcích a ty jsou po dokončení procesu sloučeny do výsledného videa. Velkou výhodou služby Batch je možnost flexibilní volby počtu virtuálních výpočetních strojů (VM), kdy každý VM počítá jeden snímek a najednou může probíhat výpočet mnoha snímků. Účtování probíhá ve výpočetních hodinách. Mezi firmou a renderovací službou bude přenášeno velké množství dat a je nutné zajistit dostatečnou konetktivitu k internetu.



Obrázek 16 - Proces zpracování dat ve službě Batch[86]

Webové stránky na vlastní doméně budou prezentovat nejen firmu samotnou, ale i projekty na kterých pracují. Potřebná videa budou nahrávána na YouTube a následně vkládána na

[86] https://azure.microsoft.com

webové stránky. Při prezentaci nových projektů může být na webové stránky vyvíjen značný nápor návštěvníků a tak budou webové stránky nasazeny ve třech lokacích. Evropa, USA a Asie. Traffic Manager pro návštěvníka vybere nejbližší server a tím docílíme nižší latence a možné náhrady v případě výpadku jednoho ze serverů. Vše řídí integrovaný Traffic Manager.

Poštovní Exchange server si zřídí firma sama. Na Forpsi se pouze změní MX záznamy a využijeme tak vlastní doménu pro elektronickou poštu na vlastním serveru.

Opět využijeme Office365 ve variantě Business. Jako e-mailového klienta budou pracovníci studia využívat zejména desktop verzi Outlook. Webové aplikace a úložiště OneDrive budou využity například při práci z domova, nebo při pracovních cestách.

Azure Storage bude využito i jako úložný prostor pro velké množství dat, které je při projektech zapotřebí. Potřebná velikost úložiště se mění a Azure Storage si přizpůsobíme dle aktuální potřeby. Kromě výpočetního a poštovního serveru je zřízen i server za účelem uložení projektů a dalších potřebných dat. Server bude v režimu RAID10, tedy zrcadlení - veškerá data budou uložena zároveň na dvou discích a disky spojeny do jednoho velkého datového pole. Finančně náročnější, ale odolné vůči havárii jednotlivých disků. Tato data mohou být přesouvána právě do Azure Storage pomocí nástroje Data Factory.

5.4.1.1 Zálohování

Poštovní server máme tentokrát ve své správě a pomocí Windows Server Backup bude server zálohován na úložný server umístěný v prostorách firmy. Záloha bude probíhat v pravidelných intervalech v nočních hodinách.

Webový stránky lze v Azure zálohovat manuálně nebo nastavit automatické zálohování. Zálohy se ukládají do Azure Storage a odtud si můžeme důležité zálohy stáhnout a uložit na firemní server.

Azure Storage využíváme zejména jako podpůrné úložiště pro ostatní služby v rámci platformy Azure, ale lze ho použít i jako zálohu lokálních dat, například zálohy Exchange serveru. Všechna data lze stahovat na firemní server pro lokální uložení.

Azure Batch ukládá výsledky výpočtů na výše zmíněný Storage, odkud můžeme data stáhnout, uložit lokálně a dále s nimi pracovat.

Office365 slouží pouze jako webová kancelář a Outlook používáme jako klienta pro správu pošty. Dokumenty z OneDrive lze v případě potřeby zálohovat na firemní server. O možnostech zálohování Office365 bylo zmíněno v části 5.1.1.2.

Videa nahrána na YouTube jsou zálohována v rámci samotné infrastruktury Google (viz 5.1.6.2) a v případě potřeby je lze stáhnout v původní kvalitě a uložit například na firemní server.

Důležitá data budou zaměstnanci ukládat na interní server.

5.4.1.2 Bezpečnost

Ohledně zabezpečení cloud platforem společnosti Microsoft bylo již psáno v např. v části 5.1.1.3 a 5.2.1.2. To vše se vztahuje i na použité služby Office365 a Azure (Web Sites. Storage, Batch). Pro shrnutí, ochrana dat probíhá od fyzického uložení v „cloudu“ po distribuci do koncového klienta. Veškerá komunikace prostřednictvím otevřeného internetu je chráněna TLS protokolem v 256 bitové verzi, potažmo 128 bitové u YouTube. V této společnosti využijeme pro ochranu koncových stanic řešení od ESET a to konkrétně verzi Secure Business. Obsahuje antivir, firewall a další nástroje pro pracovní stanice, mobilní zařízení, souborové a poštovní servery, včetně vzdálené správy všech zařízení.

5.4.1.3 Legislativa

V tomto návrhu využíváme zejména služby společnosti Microsoft a ochrana osobních údajů v tomto prostředí splňuje veškeré požadavky ČR/EU (část 1.2.3.1). Popsáno například v 4.3, 5.1.1.4 a 5.2.1.3.

Služba YouTube je využita pouze k hostování propagačních videí z produkce dané společnosti a jediné osobní údaje ke zpracování jsou ty, které zadáme při vtvoření profilu. Žádná zákaznická data této službě zpracována nejsou. Samozřejmě v podmínkách užití služby ochrana osobních řešena je a vyhovuje požadavkm ČR/EU.

5.4.1.4 SLA

Garantovaná dostupnost pro služby Azure a Office365 je 99,9 % a při nedodržení této hranice je aplikována kompenzace ve formě kreditu (slevy) z vyúčtování za služby (více 4.2). YouTube jako služba zdarma nemá garantovanou dostupnost, ale placené služby u Google mají garanci dostupnosti taktéž 99,9 %. Vzhledem k důležitosti tohoto projektu, je v nejvyšším zájmu poskytovatele udržovat tuto službu dostupnou nonstop.

5.4.2 Možná řešení při nedostupnosti cloud služeb

Návrh je řešen tak, aby mohla firma vykonávat své hlavní činnosti bez cloud služeb samotných. Na uživatelských počítačích je nasazen Autodesk Maya, je fyzicky přítomen výpočetní server (oproti možnostem Azure Batch má omezené výpočetní možnosti) a poštovní server je také řešen vlastní realizací. I v případě nefunkčního internetového připojení může společnost vytvářet v nasazeném softwaru a renderovat na svém serveru. Funkce Exchange serveru budou také přístupné v rámci vnitřní sítě.

5.4.2.1 Nedostupnost Azure Web Sites

Webové stránky jsou užity pro prezentaci společnosti, projektů a technologických prostředků užitých při tvorbě. Webový server je nasazen ve třech replikách ve třech různých geografických lokalitách (EU, USA, Asie), kvůli latenci a lepší dostupnosti při výpadku jednoho ze serverů. Pokud by výpadek postihl celou službu a na delší dobu, je možné použít zálohu webových stránek z interního úložného serveru a stránky nasadit na jakýkoliv kompatibilní webhosting. Chvíli však potrvá obnova DNS záznamů pro přesměrování na nové umístění.

5.4.2.2 Nedostupnost Azure Storage

Služba Storage je spjata s výpočetní službou Batch a jejich funkčnost se tedy vzájemně ovlivňuje. Na úložišti máme uloženy výsledky renderingu a případně další zálohy dle individuálního rozhodnutí. Výsledky renderingu se stahují a ukládají na interní server a pokud výpadek nenastane v průběhu práce se službou, máme vše potřebné na vlastních discích.

5.4.2.3 Nedostupnost Azure Batch

Azure Batch je zásadní službou pro zpracování připravených materiálů. Máme sice instalován výpočetní server v prostorách firmy, ale výpočetními možnostmi se nemůže této službě vyrovnat. V nouzi či pro drobné práce však může svou práci odvést. Výhodou připojení služby jako Azure Batch je to, že v případě nedostupnosti, můžeme využít jinou výpočetní službu určenou pro rendering. Většina takto zaměřených služeb má širokou podporu pro software a Autodesk Maya mezi ty hlavní podporované produkty rozhodně patří. Stačí tedy registraci u jiné služby a máme výpočetní náhradu.

5.4.2.4 Nedostupnost Office365

Z této služby využíváme zejména desktop verze aplikací Office a webové prostředí a úložiště OneDrive slouží zejména pro práci z domova či pracovní cesty pro přístup z jiných PC. Nedostupnost služby nám zde příliš nevadí a využíváme zmíněné desktop verze. Více například v 5.2.2.3.

5.4.2.5 Nedostupnost YouTube

Pomocí této služby pouze nabízíme ke zhlédnutí potřebná videa a výpadek by mohl mít závažnější dopad pouze při propagaci nového důležitého projektu. Výpadek samotný by však musel být dlouhodobý. Videa uložená na Azure Storage lze vložit na webové stránky ze služby Web Site pro streaming, ale velký datový provoz by mohl být pro firmu nákladný.

5.4.3 Závažnost nedostupnosti služeb

Služba	1 hodina	4 hodiny	8 hodin	1 den	3 dny	> 1 týden
Web Sites						
Storage						
Batch						
Office365						
YoutTube						

Tabulka 9 - Míry závažnosti nedostupnosti služeb u animačního studia

ZÁVĚR

Cílem této práce bylo prozkoumat cloud computing zejména z bezpečnostního a legislativního hlediska. Při užívání cloudových služeb si někdy ani neuvědomujeme, že předáváme naše osobní údaje, data a správu přidružených prostředků do rukou jiného subjektu. Proto bychom měli, nejen ve firemním prostředí, nabízené služby a podmínky jejich užívání dostatečně prozkoumat. K tomu je zapotřebí tomuto tématu porozumět a při vyhodnocení se zaměřit na ty správné aspekty. Tyto služby mohou být pro nás vhodným pomocníkem při budování firmy či při snaze o snížení nákladů za ICT infrastrukturu a správu SW. Nesprávně zvolená služba může mít pro naše záměry zásadní následky v mnoha ohledech.

V teoretické části jsem se zabýval právě palčivými problémy cloud computingu. Jaké jsou největší hrozby za poslední roky či jaké legislativní prvky musíme brát v potaz při výběru konkrétní služby. Jelikož se pohybujeme v prostředí otevřeného internet, je velmi důležitou částí legislativní stránky právě ochrana osobních údajů a z bezpečnostní stránky ochrana spravovaných dat. Je zapotřebí si uvědomit, že servery se mohou fyzicky nacházet kdekoliv na světě a každá země má při ochraně zákaznických dat svá specifika. Stejně tomu je u poskytovatelů cloudových služeb. U některých z pohledu garantovaného zaopatření můžeme cítit jako doma a u jiných bychom ani nevkročili na dvorek, natož se pohodlně zabydleli. Pokud vybíráme klíčové řešení, musíme partnerovi věřit. Rizika při nakládání s osobními údaji, porovnání on-premise a cloud řešení a ukázka smluvní stránky služby Windows Azure. To jsou další důležité aspekty na cestě k porozumění cloud computingu a jsou probrané v teoretické části této práce.

V části praktické bylo mým cílem navrhnout cloudová řešení u několika společností s různou závislostí na ICT. Těmi společnostmi bylo zvoleno truhlářství, personální agentura a animační studio. Každá z těchto firem potřebuje pro výkon předmětu své činnosti různou měrou ICT prostředky, což lze také zjistit z výsledných tabulek závažností při nedostupnosti zvolených služeb. Všechny využité služby jsou na začátku této části práce popsány z obecného pohledu a u jednotlivých návrhů poté popsány konkrétní použité části služeb. U každé firmy byly ilustrovány vazby mezi jednotlivými prvky, a jaké SW/HW řešení je konkrétně použito. U jednotlivých firem byly vždy shrnuty všechny využité služby z pohledu zálohování, bezpečnosti, legislativy a SLA. Na závěr obdržela každá společnost tabulku s mírami závažnosti při nedostupnosti jednotlivých cloudových služeb. Při návrzích byl kladen důraz na operabilitu firem i při krátkodobých výpadcích užívaných služeb.

SEZNAM POUŽITÉ LITERATURY

[1] The public cloud is more secure than your data center. *InfoWorld* [online]. San Francisco, 2015 [cit. 2016-04-10]. Dostupné z: http://www.infoworld.com/article/3010006/data-security/sorry-it-the-public-cloud-is-more-secure-than-your-data-center.html

[2] SIEPMANN, Frank. *Managing risk and security in outsourcing IT services: onshore, offshore and the cloud*. Boca Raton: CRC Press, 2014. ISBN 1439879095.

[3] CLOUD SECURITY ALLIANCE. *The Notorious Nine Cloud Computing Top Threats in 2013*. 2013. Dostupné také z: https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/

[4] CLOUD SECURITY ALLIANCE. *The Treacherous 12 Cloud Computing Top Threats in 2016*. 2016 Dostupné také z: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

[5] CHALUPSKÝ, Petr. *Využití technologie cloud computing v praxi*. České Budějovice, 2014. Bakalářská práce. Jihočeská univerzita. Vedoucí práce Doc. Ing. Ladislav Beránek, Csc., MBA.

[6] JANSEN, Wayne a Timothy GRANCE. *Guidelines on Security and Privacy in Public Cloud Computing: Special Publication 800-144*. Gaithersburg: National Institute of Statndard and Technology, 2011.

[7] CLOUD SECURITY ALLIANCE. *Top Threats to Cloud Computing V1.0*. 2010. Dostupné také z: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[8] The Impact of a Data Breach Can Be Minimized Through Encryption. *Security Intelligence* [online]. New York: IBM, 2014 [cit. 2016-04-10]. Dostupné z: https://securityintelligence.com/the-impact-of-a-data-breach-can-be-minimized-through-encryption/

[9] GAŠPARÍK, Petr. Vícefaktorová autentizace v praxi. *Security World* [online]. 2014, (4), 32-36 [cit. 2016-04-10]. Dostupné z: http://www.ami.cz/download/PR_clanky/SW1404-Vicefaktorova-autentizace.pdf

[10] BIRMAN, Kenneth P. *Guide to Reliable Distributed Systems: Building High-Assurance Applications andCloud-HostedService*. První. New York: Springer, 2012. ISBN 978-1-4471-2416-0.

[11] SEMANČÍK, Radovan a Stanislav GRÜNFELD. Cesta k efektivnímu identity managementu (1. díl): Základy správy identit a přístupů. *IT systems*. 2015**,** (1-2), 38-39. Dostupné také z: http://www.systemonline.cz/clanky/cesta-k-efektivnimu-identity-managementu-1-dil.htm

[12] Jak vytvořit opravdu silné heslo. *LinuxEXPRES: opravdový linuxový magazín* [online]. Brno: CCB, 2008 [cit. 2016-04-11]. Dostupné z: http://www.linuxexpres.cz/praxe/jak-vytvorit-opravdu-silne-heslo

[13] *Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments*. National Security Agency. Dostupné také z: https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

[14] CAPPELLI, Dawn, Andrew MOORE a Randall TRZECIAK. *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*. Upper Saddle River, NJ: Addison-Wesley, c2012. ISBN 9780321812575.

[15] *2015 Data Breach Investigations Report: Quantify the impact of a data breach with new data from the 2015 DBIR*. Verizon, 2015. Dostupné také z: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf

[16] Advanced Persistent Threat (APT). *Schneier on Security* [online]. 2011 [cit. 2016-04-11]. Dostupné z: https://www.schneier.com/blog/archives/2011/11/advanced_persis.html

[17] APT je jen další buzzword. *Clever and Smart* [online]. 2011 [cit. 2016-04-11]. Dostupné z: http://www.cleverandsmart.cz/apt-je-jen-dalsi-buzzword/

[18] FERNANDES, Diogo A. B., Liliana F. B. SOARES, João V. GOMES, Mário M. FREIRE a Pedro R. M. INÁCIO. Security issues in cloud environments: a survey. *International Journal of Information Security* [online]. 2014, **13**(2), 113-170 [cit. 2016-04-11]. DOI: 10.1007/s10207-013-0208-7. ISSN 16155262. Dostupné z: http://link.springer.com/10.1007/s10207-013-0208-7

[19] WHITMAN, Michael E a Herbert J MATTORD. *Principles of information security*. 4th ed. Boston, MA: Course Technology, c2012. ISBN 1111138214.

[20] IT Due Diligence and the Cloud. HOFFMAN, jim. *IT DUE DILIGENCE GUIDE* [online]. Secaucus, 2012 [cit. 2016-04-11]. Dostupné z: http://www.itduediligenceguide.com/it-due-diligence-cloud/

[21] SULLIVAN, Bryan. *Application-Level Denial of Service Attacks and Defenses*. San Francisco: Adobe, 2010. Dostupné také z: https://media.blackhat.com/bh-dc-11/Sullivan/BlackHat_DC_2011_Sullivan_Application-Level_Denial_of_Service_Att_&_Def-wp.pdf

[22] FURHT, Borivoje a Armando ESCALANTE. *Handbook of cloud computing*. New York: Springer, c2010. ISBN 9781441965240.

[23] BALÁŽIK, Milan. Cloud z hlediska řízení rizik a nákladů (2. díl). *IT systems*. 2014, (12), 16-17. Dostupné také z: http://www.systemonline.cz/virtualizace/cloud-z-hlediska-rizeni-rizik-a-nakladu-2.-dil.htm

[24] LEGISLATIVA V CLOUDU. *Cloud.cz (www.cloud.cz): server o Cloud computingu* [online]. [cit. 2016-04-11]. Dostupné z: http://www.cloud.cz/legislativa/191-legislativa-v-cloudu.html

[25] MATĚJKA, Jan. Základní otázky spojené s migrací části IT do cloudu. *IT Systems: Cloud computing a virtualizace IT I*. 2015, (2), 4-5. Dostupné také z: http://www.systemonline.cz/virtualizace/zakladni-otazky-spojene-s-migraci-casti-it-do-cloudu.htm

[26] Licenční smlouva. MARTINKA, Marek. *Epravo.cz* [online]. Praha: epravo.cz, 2014 [cit. 2016-04-11]. Dostupné z: http://www.epravo.cz/top/clanky/licencni-smlouva-95097.html

[27] PATTYNOVÁ, Jana. *Cloud Computing: Právní a regulační rámec*. Pierstone, 2015. Dostupné také z: http://data.eventworld.cz/file/cloud_computing_2015/prezentace/13_10.pdf

[28] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29 SMĚRNICE 95/46/ES. Stanovisko č. 05/2012 ke cloud computingu. Přijato dne 1. července 2012. Online na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_cs.pdf [cit. 20. 1. 2016]

[29] SLA (Service Level reement). *ManagementMania.com* [online]. Plzeň: MANAGEMENTMANIA.COM, 2015 [cit. 2016-04-11]. Dostupné z: https://managementmania.com/cs/service-level-agreement

[30] HORA, Michal. Tajemství zkratky SLA. *IT Systems: Obsah Outsourcing IT*. 2015, 12-13. Dostupné také z: http://www.systemonline.cz/outsourcing-ict/tajemstvi-zkratky-sla-1.htm

[31] GRAUX, Hans a Jos DUMORTIER. *Standards terms and performance criteria in service level agreements for cloud computing services*. Brusel: European Union, 2015. ISBN 978-92-79-50117-3.

[32] BARTÍK, Václav a Eva JANEČKOVÁ. *Zpracování osobních údajů školami*. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2013. Řízení školy (Wolters Kluwer). ISBN 978-80-7478-359-3.

[33] Ochrana osobních údajů. *BusinessInfo.cz* [online]. Praha: CzechTrade, 2015 [cit. 2016-04-11]. Dostupné z: http://www.businessinfo.cz/cs/clanky/ochrana-osobnich-udaju-ppbi-51068.html#!&chapter=1

[34] Alternativa jménem zálohování v cloudu. In: *Hospodářské noviny: www.ihned.cz* [online]. Praha: Economia, 2016 [cit. 2016-04-11]. Dostupné z: http://ictrevue.ihned.cz/c1-65203130-alternativa-jmenem-zalohovani-v-cloudu

[35] HRDLÍK, Martin a Filip HORÁK. Konec režimu bezpečného přístavu: pro osobní údaje občanů EU na území USA. *IT Systems*. Brno: CCB, 2015, (11), 40-41. Dostupné také z: http://www.systemonline.cz/it-pravo/konec-rezimu-bezpecneho-pristavu-pro-osobni-udaje-obcanu-eu-na-uzemi-usa.htm

[36] Neplatnost rozhodnutí Komise o tzv. Safe Harbor - doporučení Úřadu. *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, 2015 [cit. 2016-04-11]. Dostupné z: https://www.uoou.cz/neplatnost-rozhodnuti-komise-o-tzv-safe-harbor-doporuceni-uradu/d-17119/p1=1099

[37] ADAMOVÁ, Marie. Zpracování osobních údajů a jejich předávání v koncernu. *Daňaři online* [online]. Praha: Wolters Kluwer, 2015 [cit. 2016-04-11]. Dostupné z: http://www.danarionline.cz/archiv/dokument/doc-d49280v60774-zpracovani-osobnich-udaju-a-jejich-predavani-v-koncernu/

[38] *Obnovení důvěry v přenos údajů přes Atlantik: štít mezi EU a USA pro ochranu údajů*. Brusel: Evropská komise - Tisková zpráva, 2016. Dostupné také z: http://europa.eu/rapid/press-release_IP-16-433_cs.pdf

[39] Co je ISO 27001 Systém managementu bezpečnosti informací. *ManagementMania.com*[online]. Plzeň: MANAGEMENTMANIA.COM, 2015 [cit. 2016-04-11]. Dostupné z: https://managementmania.com/cs/iso-27001

[40] Cloud jako alternativa řešení bezpečnosti. *IT Systems: Small Business Solutions II*. Brno: CCB, 2012, 26-27. Dostupné také z: http://www.systemonline.cz/it-security/cloud-jako-alternativa-reseni-bezpecnosti.htm

[41] PANETTIERI, Joe. 25 Most Popular Cloud Applications and SaaS Services for Business. *After Nines* [online]. After Nines, 2015 [cit. 2016-04-11]. Dostupné z: http://www.afternines.com/news/2015/8/25/25-most-popular-cloud-applications-and-saas-services-for-business

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES Advanced Encryption System

API Aplication Programming Interface

APT Advanced Persistent Threats

CRM Customer Relationship Management

CSA Cloud Security Alliance

CSP Cloud Service Provider

DDoS Distributed Denial-of-Service

DNS Domain Name System

DoS Denial-of-Service

EHP Evropský hospodářský prostor

EHS Evropské hospodářské společenství

FTP File Transfer Protocol

IaaS Infrastructure as a Service

IAM Identity and Access Management

ICT Information and Communication Technologies

IDS Intrusion Detection System

NAS Nettwork Attached Storage

PaaS Platform as a Service

SaaS Software as a Service

SLA Service Level Agreement

SOA Service Oriented Architecture

SSL Secure Socket Layer

TLS Transport Layer Security

UI User Interface

VM Virtual Machine

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ