Využití cloudových technologií v krizovém řízení

Jan Krýsa

Bakalářská práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2016/2017

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan Krýsa**
Osobní číslo:	**L14296**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**prezenční**

Téma práce: **Využití cloudových technologií v krizovém řízení**

Zásady pro vypracování:

1. **Seznamte se s problematikou cloudových technologií.**
2. **Seznamte se s teoretickými základy krizového řízení.**
3. **Analyzujte možnosti využití cloudových technologií v krizovém řízení.**
4. **Analyzujte získané informace s cílem identifikace klíčových částí.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] ERL, T., R. PUTTINI a M. ZAIGHAM. Cloud computing: concepts, technology & architecture. Vyd. 1. New Jersey: Prentice Hall, 2013. 528 s. ISBN 978-0133387520.

[2] ROUNTREE, Derrick. a CASTRILLO, Ileana. The basics of cloud computing: understanding the fundamentals of cloud computing in theory and practice. Vyd. 1. Rockland: Syngress Publishing, 2013. 172 s. ISBN 978-0124059320.

[3] ANTUŠÁK, Emil a VILÁŠEK, Josef. Základy teorie krizového managementu. Vyd. 1. Praha: Univerzita Karlova v Praze, Nakladatelství Karolinum, 2016. 134 s. ISBN 978-80-246-3443-2.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **3. února 2017**

Termín odevzdání bakalářské práce: **15. května 2017**

V Uherském Hradišti dne 10. února 2017

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

L.S.

doc. RNDr. Jiří Dostál, CSc.
děkan

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- odevzdáním 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[1)];
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji 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[2)];
- podle § 60[3)] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60[3)] odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se bakalářská práce skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti 2.5.2017

.....
podpis studenta

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje bakalářské, diplomové, disertační a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy. Vysoká škola disertační práce nezveřejňuje, byla-li již zveřejněna jiným způsobem.

(2) Bakalářské, diplomové, disertační a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.
(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

(4) Vysoká škola může odložit zveřejnění bakalářské, diplomové, disertační a rigorózní práce nebo jejich části, a to po dobu trvání překážky pro zveřejnění, nejdéle však na dobu 3 let. Informace o odložení zveřejnění musí být spolu s odůvodněním zveřejněna na stejném místě, kde jsou zveřejňovány bakalářské, diplomové, disertační a rigorózní práce, jíž se týká odklad zveřejnění podle věty první, jeden výtisk práce k uchování ministerstvu.
2) 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, § 35 odst. 3:
(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).
3) 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, § 60 Školní dílo:
(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.
(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.
(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Cílem práce je analyzovat v současnosti dostupná cloudová úložiště nabízené globálními poskytovateli a vybrat to nejvíce vhodné pro potřeby krizového řízení. V řešení je využito komparace úložišť na základě vybraných, různě důležitých kritérií. Provedenou komparací bylo zjištěno, že nejvhodnějším cloudovým úložištěm je na základě kritérií, vah a z nich vypočítaného váženého průměru, úložiště Google Drive Enterprise následované OneDrive Business Advanced. Na základě zjištěných údajů je možno učinit pozitivní závěr – cloudová úložiště jsou využitelná pro potřeby krizového řízení.

Klíčová slova: Cloudové technologie, Cloudová úložiště, Krizové řízení, Návrh využití

ABSTRACT

The aim of this thesis is to analyse available cloud storages offered by global providers and to choose the best one for the use in crisis management. Cloud storages comparison was used based on assessed, differently valued criteria and weighted average. The output of the comparison is a decision that the best storage for use by the crisis management is Google Drive Enterprise, followed by the OneDrive Business Advanced. Based on the data founded is possible to make a positive decision, cloud storages are usable for crisis management needs.

Keywords: Cloud technologies, Cloud storage, Crisis management, Proposal for use

Poděkování

Rád bych tímto poděkoval Ing. Petru Svobodovi za odborné vedení, rady a věnovaný čas konzultacím při vypracovávání této bakalářské práce.

Ing. Lumíru Lackovi děkuji za ochotu a poskytnutí informací o ukládání dat v současné praxi.

Motto

„Chceš-li dosáhnout dobrého výsledku, nemysli na to, že nemůžeš. Prostě to riskni a přidej. Jinak nemáš šanci!“

Lukáš Bauer

OBSAH

ÚVOD

Rozvoj technologií nabral obrovské tempo. S ohledem do historie, nikdy dříve nebylo vyvinuto tolik technologií a nových zařízení jako v uplynulých 100 letech. Pokrok nepřestává polevovat na tempu. Nemůžeme se tedy divit tomu, že před několika lety nejmodernější zařízení na světě jsou dnes svým výkonem zcela zastaralé a nedostačující požadavkům uživatelů. Zařízení jsou neustále zmenšována. Výpočetní kapacita dřívějších velkých halových počítačů je v dnešní době srovnatelná s výkonem smartphonů, které jsou svou cenou dostupné prakticky pro každého a vejdou se do kapsy kalhot.

Člověk je obklopen technologiemi ze všech stran. Nelze se tedy divit jeho snaze o ulehčení si práce s nimi, zjednodušení a vzájemné propojení. Jelikož během dne použije několik inteligentních zařízení, je užitečné ukládání vygenerovaných dat na místo odkudkoliv dostupné a bezpečné.

Dříve oblíbené diskety byly vytlačeny přenosnými médii typu CD a DVD. S rostoucím množství dat nutných k uložení však přestala tato 700 MB a 4,7 GB média stačit. Dlouhá doba ukládání, nutnost speciálního a dražšího typu těchto médií a požadavek na snadnou obsluhu způsobily snížení jejich využívání a nahrazení flash disky. Ty na rozdíl od CD a DVD vynikají zejména malou velikostí, rychlostí přenosu, snadnou obsluhou a možností opakovaného ukládání dat. I přesto se začíná počet jejich uživatelů snižovat. Nutnost neustále mít flash disk u sebe je pro mnoho lidí nepraktické, a to zvláště v okamžiku, kdy začala být veřejnosti dostupná cloudová úložiště.

Velký úložný prostor a minimální náklady na něj, doplňkové přidružené nástroje a další široké využití jsou dnes hlavními důvody, proč se mnoho lidí spoléhá právě na cloudová úložiště. Překážkou není ani nutnost připojení k internetu, který je v dnešní době dostupný všem generacím a umožňuje tak využití cloudových služeb téměř ve všech oborech. Od běžných obchodních zpráv až po sdílení informací v okamžiku ohrožení člověka.

Řešením těchto a podobných situací se zabývá vědní obor Krizové řízení.

Možností využití cloudových úložišť v oblasti krizového řízení se zabývá tato bakalářská práce.

I. TEORETICKÁ ČÁST

1 CLOUDOVÉ TECHNOLOGIE

Počet uživatelů cloudových technologií v posledních letech rychle roste a dá o nich hovořit jako o jednom z největších trendů celé oblasti IT. Jejich úkolem je poskytnout uživatelům skrze internet, softwarové a hardwarové nástroje jako sdílenou službu. Cloudové technologie poskytují příležitost pro vznikající nové obchodně-operační platformy, umožňující společnostem změnit jejich obchodní model a spolupráci tak, aby nalezli cesty k zákazníkům, uživatelům a obchodním partnerům jednodušeji než dříve.

Většina lidí si při otevření internetového prohlížeče ani neuvědomí své vstoupení do světa cloudových technologií. I e-mailová schránka jí je ve své podstatě. Každý e-mail musí být někde uložen. Místem, kde k tomu dojde, jsou servery poskytovatelů využité e-mailové služby.

Cloudové technologie může využít každý, firma i běžný uživatel. Nespočet těchto technologií je nabízeno v omezené míře zdarma, ať již jsou to balíky kancelářský programů, úložiště pro fotografie z dovolené či nástroje pro komunikaci s jinými lidmi v reálném čase.

1.1 Historie a předchůdci

První distribuční systémy se začaly objevovat v padesátých letech 20. století. Postupně vznikaly nové technologie, jež se staly předchůdci současného cloud computingu. [1]

Myšlenka vzdálené počítačové vědy (cloudu) vede k počátkům této vědy samotné. V roce 1961 John McCarthy, tehdejší odborník v oblasti IT, veřejně prohlásil: *„Pokud se počítače, takové, jaké obhajuji, stanou počítači budoucnosti, pak bude počítačová věda jednou organizována jako veřejný nástroj, právě tak jako je telefonní systém nástrojem veřejným … Počítačový nástroj se může stát základem nového a důležitého průmyslu.“* [2]

Také Leonard Kleimrock, vedoucí vědec ARPANETu[1], předpovídal následující: *„I když jsou nyní počítačové sítě stále v plenkách, ony vyrostou a stanou se více vyspělým. Pak teprve uvidíme rozšíření počítačových nástrojů...“* [2]

[1] Zkratka pro Advanced Research Projects Agency Network. Tato počítačová síť spuštěná v roce 1969 a byla zárodkem pro dnešní internet.

S rozvojem počítačových technologií vznikaly a byly vyvíjeny nejrůznější služby, jako webový vyhledávač Google, e-mailové služby Hotmail či Gmail, sociální sítě Facebook či Twitter. V roce 2002 spustil americký internetový obchod Amazon službu s názvem Amazon Web Service (dále jen AWS). Služba od svého počátku cílí na firemní klientelu. Poskytuje vzdálené úložiště, výpočetní výkon a nespočet obchodních funkce. Porovnají-li se cloudové služby dnes a AWS, můžeme říci, že se jedná o první cloud, tak jak ho známe.

1.2 Pojem „Cloud“

Pojem „Cloud“ vznikl z anglického výrazu pro obláček, jelikož v síťových diagramech jsou cloudové technologie, či cloudová úložiště, tak zobrazována.

První použití zmíněného termínu je datováno v roce 2006, kdy Amazon odstartoval Elastic Compute Cloud služby (zkráceně EC2) a Google začal poskytovat ve svých Google Apps, na prohlížeči založené aplikace pro podnikovou sféru. Rok 2009, ve kterém Google začal fungovat svého novém Google App Engine, se stal dalším historickým milníkem ve vývoji technologií.[2]

O definování cloud coumputingu se pokusilo nespočet autorů a expertů IT prostředí. Všeobecně uznávanou definici vytvořil v roce 2011 National Institute of Standards and Technology, známý pod svou zkratkou NIST. Podle ní je cloud computing (dále jen cloud) model umožňující pohodlný, vzdálený síťový přístup ke sdílenému fondu konfigurovatelných výpočetních zdrojů (např. sítě, servery, úložiště, aplikace a služby), které lze rychle opravit jako položky a jenž jsou poskytovány s minimálním úsilím pro správu nebo nutností interakce strany s poskytovatele služby. Model cloudu dle ní podporuje dostupnost a skládá se z pěti základních charakteristik:

- vlastní vzdálená služba
- široký přístup k síti
- sdružování prostředků
- velká pružnost
- měřená služba [4]

NIST rozlišuje tři modely služeb: Infrastruktura jakožto servis, Platforma jakožto servis a Software jakožto servis. Z hlediska užívání je dělen na čtyři modely nasazení infrastruktury: na veřejný, soukromý, komunitní a hybridní cloud. [4]

Pro činnost a aktivní využívání cloudu jsou podle NIST Cloud Computing Program klíčové tři faktory, jimiž jsou:

1. rychlý WAN
2. výkonné, levné serverové počítače
3. vysoce výkonná virtualizace pro komoditní hardware [4]

International Organisation for Standardisation (známá pod zkratkou ISO) naopak užívá vlastní definici. V ní cloud rozlišuje na sedm kategorií služeb. Nařazuje například specifičtější rozdělení sítě jakožto služby (NaaS) či ukládání dat jakožto služby (DSaaS). V dělení z hlediska umístění infrastruktury, jsou definice identické. ISO také rozlišuje cloud veřejný, soukromý, komunitní a hybridní. Komplexní pojednání je shrnuto ve dvou mezinárodních normách: ISO/IEC 17788:2014 a ISO/IEC 17789:2014. [5]

Peter Fingar, odborník v oblasti IT, rozlišuje dvě úrovně definice cloudu. Pro osoby znalé IT definuje cloud, hovoříme-li o něm, hovoříme o výpočetní mřížce, výpočetním nástroji, softwaru jakožto službě, o virtualizaci, o na internetu založených aplikacích, Peer-to-Peer a o dálkovém zpracování dat na vyžádání. Pro méně znalé IT definuje cloud jako platformu, kde jednotlivci a společnosti využívají internet k přístupu ke koncovému hardwarovým, softwarovým a datovým zdrojům pro potřeby vlastních výpočtů. [6]

Zcela zjednodušeně lze cloud charakterizovat také jako možnost využít software a výpočetní kapacity, které se nenachází fyzicky v zařízení uživatele, ale umístěného „někde jinde“, využitím připojení k internetu a dostačujícímu výkonu našeho zařízení.

Zamyslíme-li se nad definicemi cloudu a tím, jak je využíván internet, bylo mi možné zaměnit pojem cloud a internet. Symbol mráčku bývá někdy užit pro grafické znázornění internetu, ale nejde o totéž. Cloud je využíván pro vzdálené poskytování IT zdrojů a má konečné hranice. Kdežto internet slouží pouze jako nástroj, vzájemně propojující jednotlivé cloudy. Proto internet jako takový, nemá hranice. [2]

Tvrzení potvrzují i grafická znázornění zapojení cloudů do internetu. Jedním z nich je i následující obrázek znázorňující provázanost cloudů a internetu, ale i tzv. Internetu věcí (IoT).

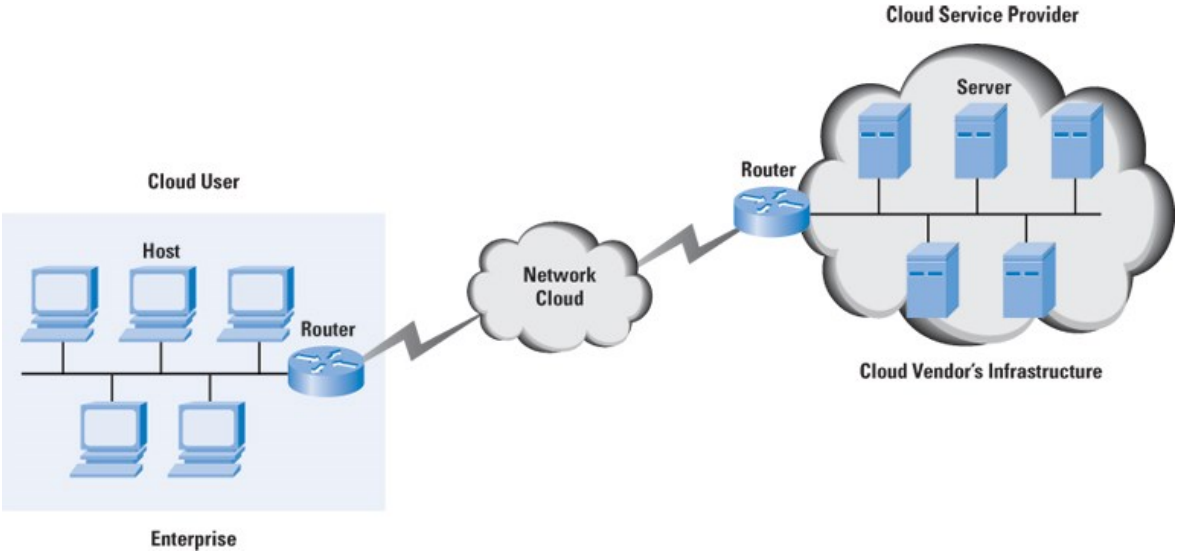
Obrázek 1: Propojení internetu s cloudy [42]

1.3 Role v cloudu

K využití cloudu je využíván internet, jak již bylo zmíněno. Jelikož skrze něj jej uživatel obsluhuje, jsou rozlišovány role jednotlivých subjektů v cloudu.

V základu se rozhlašují dva typy: poskytovatel a jeho uživatel. [7]

Již samotné názvy napovídají jejich hlavní úlohy. Na Obrázku 2: Propojení Poskytovatel-Internet-Uživatel lze vidět uživatele cloudové služby na straně jedné a jejího poskytovatele, na straně druhé, kteří jsou spojování internetem či jinou sítí.



Obrázek 2: Propojení Poskytovatel-Internet-Uživatel [43]

Poskytovatel cloudových služeb je subjekt, soukromá osoba či společnost, poskytující na cloudu založené IT zdroje, jenž řídí a servisuje. Vykonává též další úkony související s poskytováním cloudových služeb, jako je nezbytná administrativa, pojící se k poskytování služeb uživatelům obvykle za úplatu. [7]

Uživatelem cloudových služeb je subjekt, společnost či soukromá osoba, využívající IT zdroje, poskytované jejich poskytovatelem. Za využívání služeb obvykle odvádí poplatek na základě uzavřené smlouvy. Pro užití soukromou osobou velcí poskytovatelé (Google, DropBox aj.) nabízí základní balík služeb zdarma. Tyto služby jsou však omezeny kapacitou, jejíž zvětšení je zpoplatněno.[7]

Cloudové služby neposkytují však jen specializovaní poskytovatelé. Mnoho výrobců elektroniky nabízí svým zákazníkům zálohu dat z jejich zařízení na cloudová úložiště. Někteří provádí ukládání dat na vlastních serverech v datových centrech, jiní ji tzv. outsourcují, když ji odebírají jako službu od specializovaných společností.

1.4 Model nasazení

Cloud je z hlediska modelu nasazení dle Rountree a Castrillo [8] dělen na 4 typy:

- Soukromý
- Veřejný
- Komunitní
- Hybridní

1.4.1 Soukromý

Soukromý cloud je určen pro jednu společnost, čímž je umožněna vysoká kontrola a bezpečnost, díky nesdílení dat s dalšími organizacemi. Softwarové balíčky nabízené poskytovateli umožňují vytvoření vlastního soukromého cloudu. Infrastruktura může, avšak nemusí, být umístěna v prostorech dané společnosti.

1.4.2 Veřejný

Tato veřejně dostupná platforma je poskytovateli obvykle zpoplatněna, v závislosti na využívání. Infrastruktura je obvykle umístěna v prostorách poskytovatele cloudu. Výhodou tohoto typu je vysoký výkon, naopak jeho stinnou je vyšší náchylnost k útokům.

1.4.3 Komunitní

V rámci komunitního cloudu dochází ke sdílení zdrojů několika organizacemi, odpovídající za jeho provoz a servis. Tento model ideálním řešením pro společnosti, jenž mají požadavky bezpečnostního či zákonem stanoveného charakteru, u nichž nelze využít veřejného cloudu.

1.4.4 Hybridní

Hybridní cloud je kombinací předešlých modelů. Určité části infrastruktury bývají umístěny na vlastních serverech zákazníka, jiné jsou naopak v rámci veřejného cloudu.

1.5 Distribuční model

Dle Rountree a Castrilla [8] hovoří-li se o službě, kterou cloud nabízí, rozlišují se tři základní druhy:

- IaaS (Infrastructure-as-a-Service) – Infrastruktura jakožto servis
- PaaS (Platform-as-a-Service) – Platforma jakožto servis
- SaaS (Software-as-a-Service) – Software jakožto servis

1.5.1 IaaS – Infrastruktura jakožto služba

IaaS poskytuje uživateli výpočtové, úložné a síťové zdroje. Užitím tohoto modelu nejsou potřeba počátečních náklady k vybudování a správu vlastního datového centra. Uživatel má možnost výběru operačního systému, výkonu serverů a velikosti úložiště pro svůj software.

1.5.2 PaaS – Platforma jakožto služba

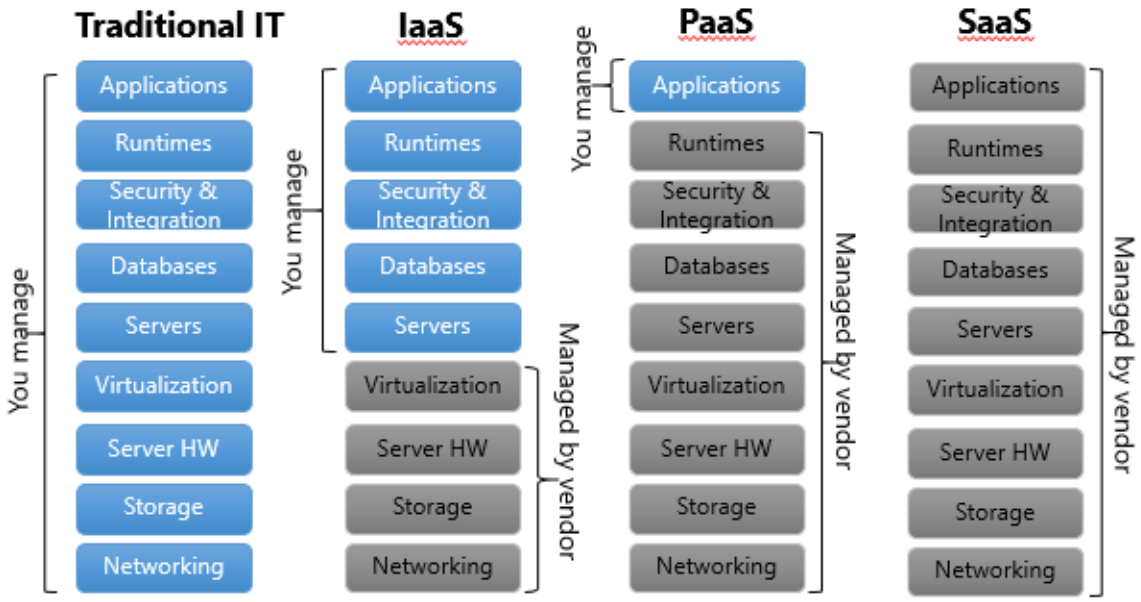
PaaS je nejčastěji využíván vývojáři pracujícími na vlastním softwarovém řešení. Předností PaaS je předkonfigurované, pouze obecné prostředí s vývojářskými nástroji a moduly. Tímto prostředím je cíleno na všechny vývojáři, jenž si jej upraví dle svých potřeb pro potřeby vytváření nových aplikací.

U tohoto druhu cloudu existuje riziko nekompatibility prostředí s cílovými technologiemi, je tedy nezbytné kompatibilitu vždy předem ověřit.

1.5.3 SaaS – Software jakožto servis

SaaS nabízí hotová řešení v podobě softwaru, dostupného uživatelům skrze jejich webové prohlížeče. Předností SaaS je minimalizace nákladů na správu zařízení s využívaným softwarem. Čas nutný na instalaci do zařízení (oproti klasické instalaci na HDD zařízení) se výrazně zkracuje a jsou výrazně vylepšeny prostředky pro komunikaci jednotlivých uživatelů mezi sebou.

K přehlednému porovnání funkcí jednotlivých distribučních modelů, v grafické úpravě, poslouží Obrázek č. 1 – Druhy cloudu. Je rozlišitelné, které funkce a části uživatel řídí během využívání při využívání daného distribučního modelu, v porovnání se stolním PC bez cloudových služeb. Části umožněné administrovat samotným uživatelem, jsou zobrazeny modrou barvou, naopak šedou jsou lze vidět služby bez této možnosti.



Obrázek 3: Druhy cloudu [44]

1.6 Ukotvení cloudových technologií v legislativě

V aktuálně platné legislativě České republiky existuje několik zákonů a právních norem zasahující do oblast zabezpečení informačních systémů, do nichž jsou řazeny cloudové technologie. Zákon či norma, vymezující výhradně cloudové technologie však momentálně neexistuje. Nakládání s údaji upravuje Zákon č. 101/2000 Sb., o ochraně osobních údajů a Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Ve fázi příprav je Národní strategie cloud computingu a s ním spojený tzv. e-Government.

1.6.1 Aktuální legislativa

- **Zákon č. 101/2000 Sb. o ochraně osobních údajů** se dle §3 tohoto zákona, vztahuje na všechny osobní údaje, jakkoliv zpracovávané fyzickými a právnickými, státními orgány, orgány územní samosprávy a jinými orgány veřejné moci. Výjimkou je zpracování osobních údajů výhradně pro osobní potřebu. Zákon stanovuje správci dat povinnosti, např. přijímat opatření zabraňující neoprávněnému přístupu či manipulaci s daty. Dále také povinnosti stanovit účel, prostředky a způsob zpracování a nakládání s osobními údaji, jak je uvedeno v §5 odst. 1.
    - **Osobním údajem** se dle §4 tohoto zákona rozumí jakýkoliv osobní údaj týkající se určitého nebo určitelného subjektu. Za takový subjekt se považuje

údaj využitelný pro přímou či nepřímou identifikaci subjektu, na základě čísla, kódu atd.

- **Citlivý údaj** je dle §4 odstavce b) tohoto zákona, osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, náboženství a filozofickém přesvědčení, zdravotním stavu apod. Citlivé údaje je dle §9 odstavce c) povoleno zpracovávat při poskytování ochrany veřejného zdraví. Výjimka platí tedy i pro, jinak stanovenou povinnost, správce dat informovat subjekty údajů z jakých důvodů jsou data zpracovávány, jak je uvedeno v §11. Výjimka zprošťuje také povinnosti uložené §12. Požádá-li subjekt osobních údajů o informaci o zpracování svých osobních údajů, správce dat mu není. na základě této podmínky, povinen informaci předat. [9]

- **Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti** upravuje dle §1 tohoto zákona: „*zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy*.“ [10]
  - **Utajovanou informací** se pro potřeby tohoto zákona dle §2 odstavce a) rozumí: „*informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací (§ 139)“* V případě krizového řízení lze předpokládat potřeba manipulace se zmíněnými údaji.

- **Zákon č. 181/2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)**, známý též jako Kybernetický zákon, nelze podle §2 odstavec d) tohoto zákona, aplikovat na řešené cloudové technologie. Odstavec jasně říká: „*významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci“*. [11]

  Dle přílohy nařízení vlády č. 315/2014 Sb. nazvané: Odvětvová kritéria pro určení prvku kritické infrastruktury [12], jsou komunikační a informační systémy považovány za prvek kritické infrastruktury.

Případné narušení bezpečnosti informací tak může ohrozit výkon působnosti orgánů veřejné moci, jimiž jsou orgány krizového řízení a narušit kritickou infrastrukturu. Tuto skutečnost potvrzuje také Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. [13]

1.6.2 Národní strategie Cloud computingu

Dle Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 [14] se definuje zmíněná strategie jako: *„koncepce, jak ve veřejné správě řešit celou řadu dlouhodobých problémů v oblasti informačních systémů, informačních a komunikačních technologií a jak v této oblasti maximalizovat výhody plynoucí z využívání sdílených služeb. Strategie obsahuje opatření, které se týkají jak na stávajících aplikací, resp. ICT služeb veřejné správy, tak nově vytvářených aplikací, resp. ICT služeb. Klíčovým opatřením, které je zaměřeno na stávající aplikace/ICT služby je jejich postupná migrace do eGovernment cloudu, který má státní a privátní část (státní cloud a komerční cloud). Strategie je vedena snahou vybalancovat využití státního a komerčního cloudu tak, aby stát měl pod kontrolou kritickou IT infrastrukturu a kritická data a současně aby pro ostatní ICT služby maximálně využil tlaku tržního prostředí na cenu služeb.“* [14]

Akční plán počítá pro rok 2016 a 2017, s přípravami technických, organizačních a legislativních podmínek pro národní cloud. Dokončení strategie je naplánováno v roce 2020.

2 KRIZOVÉ ŘÍZENÍ

Ve všeobecně známé terminologii je termín „krizové řízení“, popř. „krizový management“, chápán v negativním smyslu, z důvodu jeho častého spojování s nebezpečnými situacemi. V minulosti byl tento termín často používán v souvislosti s Kubánskou krizí v roce 1962 za amerického prezidenta J.F. Kennedyho. [15]

Termín nalezneme také v terminologii NATO, které jej integrovalo do vlastní užívané terminologie a používá jej jako název pro jeden ze svých hlavních bezpečnostních úkolů – krizové řízení může zahrnovat vojenské i nevojenské opatření k řešení celého spektra krizí před, během a po konfliktech. [15]

Jednou ze silných stránek Severoatlantické aliance jsou její kapacity pro krizové řízení, založené na zkušenostech, osvědčených a vyzkoušených postupech krizového řízení a integrované vojenské struktury velení. To umožňuje řešit širokou škálu krizí ve stále složitějším bezpečnostního prostředí, používat vhodnou kombinaci politických a vojenských nástrojů, které pomáhají řídit nově vznikající krize, jež by mohly ohrozit bezpečnost území a obyvatelstva zemí Aliance. [15]

V kontextu s NATO je krizové řízení chápáno však v širším měřítku – hrozby a rizika jsou mezinárodního, regionálního a světového charakteru.

Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu vymezuje pojmy hrozba a riziko následovně: *„Za hrozbu je v obecné rovině považován přírodní nebo člověkem podmíněný proces představující potenciál, tj. schopnost zdroje hrozby být aktivován a způsobit škodu. Tento potenciál může být spuštěn záměrně nebo náhodně využit pro atakování specifických zranitelností aktiva. Hrozba bývá zdrojem rizika.“* [17]

Riziko je definováno jako: *„Možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit. Riziko také představuje účinek nejistoty na dosažení cílů nebo pravděpodobnost výskytu nežádoucí události s nežádoucími následky.“* [17]

2.1 Krizový management

Krizový management je řazen do skupiny tzv. prediktivního projektového managementu, zaměřeného na aktivní předcházení problémů, řízení rizik a jejich zvládání. Projevuje se vnitřní efektivností řízení a následnou vysokou produktivitou realizačních týmů. Proaktivním řešením problémů dochází k vytváření konstruktivního prostředí, kde výjimečné jevy, krizové situace a krize narušují postup vpřed. [20]

Názorů na otázku „Co je to krizový management?“, existuje nespočet, stejně jako pro obecný management. V životě se lze setkat s užíváním zmíněného pojmu pro profesi, pro skupinu řídících pracovníků a pro krizový management, jakožto vědní disciplínou. Pro potřeby bakalářské práce užijeme definici podle Antušáka: „*Krizový management je ucelený soubor teoretických přístupů. Praktických doporučení a metod, uplatňovaných v hierarchizovaném a funkčně propojeném systému orgánů veřejné správy, právnických a fyzických osob, jehož cílem je minimalizovat (zamezit) možnosti vzniku krize nebo (v případě že krize již nastala) redukovat rozsah škod a minimalizovat dobu trvání krize. Důležitou součástí krizového řízení je i odstraňování následků působení negativních krizových faktorů, obnova systému a jeho návrat do nového (vylepšeného) běžného stavu*.“ [20]

2.1.1 Funkce a úrovně krizového managementu

Základními funkcemi krizového managementu, na nichž je založen celý jeho proces, jsou podle Antušáka a Viláška [20] postupně:

1. Prevence
2. Korekce
3. Protikrizové (krizové) intervence
4. Redukce
5. Obnova

Prevence spočívá v organizační přípravě subjektu na činnosti, které budou prováděny, s cílem zabránit eskalování hrozeb do krizových situací a krizí. V rámci korekce dochází k přijímání opatření právního, ekonomického, hospodářského a jiného charakteru, s cílem minimalizovat zdroje krizových situací a zvýšit zabezpečení vůči možným krizovým situacím. Protikrizová situace naopak zahrnuje opatření, která aktivně zabrání vzniku krizové situace, její eskalaci, a postupnému návratu do běžného stavu. Následující funkce cyklu – redukce, spočívá v aktivní realizaci opatření krizových plánů, provádění záchranných akcí apod.

Poslední funkcí je Obnova, během níž probíhá likvidace následků krize a navrácení systému do běžného stavu.

Krizový management je však nikdy nekončící proces, jak lze vidět na Obrázku 4 - Proces Krizového managementu. Krize jsou, byly, a i nadále budou, proto příprava na ně je nezbytná

Obrázek 4: Proces krizového managementu (Zdroj: Vlastní)

2.1.2 Současné pojetí krizového managementu

S technologickým vývojem a rostoucí globalizací dochází k vývoji celého světa. Manažeři jsou dnes z důvodu vzniku nových a nových hrozeb a rizik, nuceni učit se velkému množství nových dovedností.

Změna bezpečnostního prostředí je dalším následkem rychlého světového vývoje. Charakter války, dříve vedené s pomocí velkého množství vojáků a vojenské techniky, se změnil. V současné době jsou vedeny války s menšími počty a s využitím jiných metod boje. Příkladem, nechť je válka na Ukrajině. V souvislosti s ní začal být velmi diskutován pojem tzv. hybridní války, jenž lze byl definován jako: „O*zbrojený konflikt vedený kombinací nevojenských a vojenských prostředků s cílem jejich synergickým efektem přinutit protivníka k učinění takových kroků, které by sám o sobě neučinil. Alespoň jednou stranou konfliktu je stát. Hlavní roli při dosažení cílů války hrají nevojenské prostředky v podobě psychologických operací a propagandy, ekonomických sankcí, embarg, kriminálních aktivit, teroristických aktivit a jiných subversivních aktivit obdobného charakteru. Vojenské operace útočníka jsou vedeny na zapřenou nepravidelnými silami kombinujícími symetrické a asymetrické způsoby vedení bojové činnosti proti celé společnosti a zejména proti jejím politickým strukturám, orgánům státní správy a samosprávy, ekonomice státu, morálce obyvatelstva a ozbrojeným silám.*“ [21]

S ohledem na zmíněné změny ve světě, popisuje Antušák krizový management jako ucelený soubor přístupů, názorů, zkušeností, doporučení, metod a opatření, které vedoucí pracovníci (manažeři) a krizoví manažeři užívají ke zvládnutí specifických činností (manažerských funkcí) při:

- Minimalizaci zdrojů (příčin vzniku) krizových situací (fáze prevence)
- Přípravě na činnosti v krizových situacích (fáze korekce)
- Bránění vzniku a eskalaci krizových situací a jejich negativního působení (fáze redukce)
- Odstraňování následků působení negativních faktorů krizové situace (fáze obnovy) [20]

Krizový management lze dle něj rozdělit na dvě úrovně – na řízení rizik (risk management) a proces zvládání krizí (managering crisis). Jeho cílem je činit kroky k zamezení vzniku krize, příp. k její eliminaci, minimalizaci a obnovení normální činnosti za pomocí velkého množství metod a nástrojů. [20]

2.2 Krizové řízení

Pojem „krizové řízení“ se v české legislativě vyskytl poprvé v tzv. kompetenčním zákoně č. 2/1969 Sb. o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky.[22]

Přesná definice je součástí zákona č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon). Podle kterého je krizové řízení: „*souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s:*

1. *přípravou na krizové situace a jejich řešením, nebo*
2. *ochranou kritické infrastruktury“*. [23]

K oblasti krizového řízení se vztahují i další zákony? Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů [13] a Zákon č. 241/2000 o hospodářských opatřeních pro krizové stavy [25]

Tyto zákony se zaměřují na krizovou připravenost na státní úrovni, tj. na schopnost reagovat na kritickou situaci týkající se bezpečnosti na území ČR a s tím související krizové stavy. Jsou podřazeny ústavnímu zákonu č. 110/1998 Sb. o bezpečnosti České republiky.[26]

2.2.1 Orgány krizového řízení

Ústavní zákon č. 110/1998 Sb. o bezpečnosti České Republiky [26] ukládá za základní povinnost státu zajistit státní svrchovanost, územní celistvost, ochranu demokratických základů, ochranu životů, zdraví a majetkových hodnot občanů.

Povinnost chránit životy, zdraví a majetek občanů je stavena též zákonem č. 128/2000 Sb. o obcích [27] a zákonem č. 129/2000 Sb. o krajích [28] . Tyto zákony přenáší povinnost chránit, i na menší samosprávní celky ČR.

Jednotlivé státní, krajské a obecní orgány činné v této problematice – orgány krizového řízení, vymezuje Zákon č. 239/2000 Sb. o integrovaném záchranném sboru [13] a Zákon č. 240/2000 Sb. o krizovém řízení. [23]

Orgány krizového řízení jsou zákonem stanovené orgány veřejné správy, předurčené k řešení nevojenských i vojenských krizových situací, jež by mohly vzniknout na území státu. Orgány krizového řízení jsou:

- Vláda ČR
- Ministerstva a jiné ústřední správní úřady
- Česká národní banka
- Orgány kraje a další orgány s působností na území kraje
- Orgány obce s rozšířenou působností
- Orgány obce [23]

Každý zmíněný orgán si v rámci své působnosti vytváří prvky krizového řízení, jimiž jsou pracovní a koordinační orgány (pracoviště krizového řízení, bezpečnostní rady a krizové štáby), napomáhající v přípravě na řešení krizových situací, ale i jejich samotnému řešení.

2.2.2 Krizové plánování

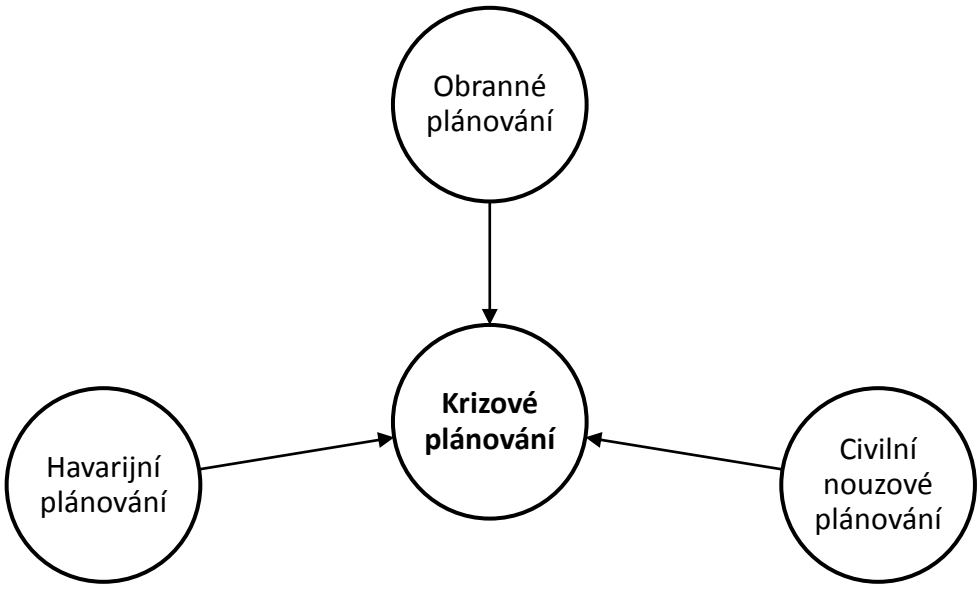
Hlavním cílem krizové plánování jsou aktivity orgánů krizového řízení zaměřené na:

- minimalizaci (prevenci) možnosti vzniku krizových situací přírodního, antropogenního nebo sociálního a společenského charakteru,
- hledání nejvhodnějších způsobů protikrizové intervence,
- optimalizaci metod a forem zvládání těchto nežádoucích jevů (tj. redukci dopadů krizových situací) a

- stanovení nejracionálnějších a ekonomicky nejvýhodnějších cest obnovy postižených systémů a jejich návratu do nového běžného stavu.

V České republice je krizové plánování tvořeno třemi, téměř samostatnými pilíři – obranným plánováním, civilním nouzovým plánováním a havarijním plánováním, jak lze vidět na Obrázku 5: Krizové plánování ČR.

Obranné plánování se zabývá plánováním sil, zdrojů, výzbroje, komunikačních a informačních prostředků, logistické podpory, zdravotnického zabezpečení, nevojenské obrany. Plánování činnosti složek IZS, zpracování vnitřních a vnějších havarijních plánů a příprava složek IZS a obyvatelstva ke zvládání krizových jevů, náleží do havarijnímu plánování. Součástí civilního nouzové plánování je plánování zdrojů, prvků ekonomické bezpečnosti, ochrany obyvatelstva, zabezpečení základních funkcí státu a opatření k předcházení krizím.[20]



Obrázek 5: Krizové plánování ČR (Zdroj: Vlastní)

Výstupem krizového plánování je tzv. krizový plán, obsahující stručné, přehledné a v praxi využitelné instrukce pro případ krizové situace.

3 CÍL A METODIKA PRÁCE

Práce je zaměřena na seznámení se s cloudovými technologiemi jejich historií, typy, druhy a základy krizového řízení. Cílem je zhodnotit možnost využití cloudových úložišť pro potřeby krizového řízení a vybrat úložiště na základě stanovených kritérií, nejvhodnější pro tuto potřebu. Pro zpracování je využíváno rešerše dostupných zdrojů v předmětné oblasti a analýza zjištěných informací.

Praktická část práce zahrnuje výsledek sběru dat z rozhovorů s odborníky z praxe krizového řízení. Důraz je kladen na rešerše nabídek poskytovatelů cloudových úložišť a dokumentů o zabezpečení jejich služeb. Jsou stanoveny váhy a kritéria, jejichž využitím je vybráno nejlepší řešení, za komparace výstupů po aplikaci komparačních kritérií. Pro potřebu simulace předpokládaných činností pracovníka krizového řízení při práci s cloudovým úložištěm, je využito poskytovaného kancelářského balíku Office 365 Univerzitou Tomáše Bati. Univerzita jej poskytuje, na základě vlastnictví softwarové licence kancelářského balík Office 365 Education, svým zaměstnancům a studentům.

Cíly práce jsou:

- Obeznámení se s vývojem, principy, druhy a možnostmi nasazení cloudových technologií
- Seznámení se se základy krizového řízení a krizového plánování v ČR
- Analýza nabídek cloudových úložišť, jejich rešerše a výběru nejvhodnějšího pro potřeby využití v krizovém řízení za využití komparačních kritérií.
- Zhodnocení možnosti využití cloudových úložišť, s ohledem na názor pracovníka krizového řízení a rozpracovanou legislativu, jenž obor ovlivní.

Bakalářská práce je zpracována v přehledné návaznosti zaručující, i osobě neznalé, možnost obeznámit se se základními principy a získat přehled v problematice, o níž je pojednáváno.

II. PRAKTICKÁ ČÁST

4 ANALÝZA MOŽNOSTI VYUŽITÍ CLOUDOVÝCH ULOŽIŠŤ GLOBÁLNÍCH POSKYTOVATELŮ V PODMÍNKÁCH KRIZOVÉHO ŘÍZENÍ

Využívá cloudových technologií pro pracovní i soukromé účely je již pro mnoho lidí denní běžnou činností. Z toho důvodu jsou vybrány právě taková cloudová úložiště, jejichž služby běžně uživatel zná, alespoň dle jejich názvu.

Především velké subjekty a projekty, využívají možnost vývoje softwaru tzv. na míru, striktně pro potřeby konkrétního subjektu – za jednorázový poplatek a následný pravidelný měsíční poplatek za zprávu. Příkladem může být například software/zařízení na ovládání např. jaderné elektrárny, kdy je dodavatelská firma povinna držet pohotovost pověřeným pracovníkem v místě JE pro případ možného problému, a jeho okamžitého vyřešení.

Další možností je zakoupení licence softwaru, který si kupující „nasadí“ na vlastní systém a jeho správu si zajišťuje svépomocí, příp. jej za poplatek vykonává dodavatel.

Pro účely marketingu a související snaze o rozšiřování klientské základny nabízí někteří poskytovatelé cloudových služeb jejich omezenou část zdarma. Chce-li uživatel využívat více (potřebuje-li více úložného prostoru, chce-li využívat lepší a komplexnější služby, více výpočetního výkonu apod.) musí jej platit, často v podobě měsíčního paušálu. Spokojenost uživatele s verzí zdarma je pro poskytovatele důležitá. Není-li spokojen, pravděpodobně vyzkouší služby i jiného poskytovatele, k nalezení pro sebe té nejlepší a nejlevnější služby.

Lze říci: *čím více služeb a softwaru, od jednoho poskytovatele, tím menší je riziko nekompatibility* atd. Uživatel se v případě spokojenosti může stát loajálním vůči poskytovateli, v případě problémů s některou funkcí, je ochoten čekat déle na její opravu, než například nový zákazník. Chování uživatelů se věnuje celá řada knih.

4.1 SOUČASNÉ ŘEŠENÍ UKLÁDÁNÍ DAT KRIZOVÉHO ŘÍZENÍ

Pro potřebu analýzy současného řešení ukládání dat krizového řízení byl kontaktován zástupce města Uherské Hradiště pan Ing. Lumír Lacka z Útvaru kanceláře starosty města Uherské Hradiště, v jehož gesci je problematika krizového řízení, ochrana obyvatelstva, obrana, JSDH a utajované informace.

4.1.1 Ukládání dat ve městě Uherské Hradiště

Město Uherské Hradiště vybudovalo z dotačního titulu vlastní technologické centrum (dále jen TC) dle technických norem ČSN EN 50600-1 – Informační technologie – Zařízení a infrastruktury datových center, a v současné době se stará pouze o zajištění jeho provozu.

Data a servery jsou v současnosti využívány pouze pro potřeby městského úřadu. Do budoucna se zvažuje využití pro příspěvkové organizace města a městem zřizované organizace. Přístup k datům je možný výhradně z vnitřní sítě města.

Všechny servery, fyzické i virtuální, jsou umístěny v serverovně TC, zabezpečené zabezpečena elektronickým zabezpečovacím systémem, kamerovým systémem, náhradním zdrojem elektrické energie, klimatizací a nepřetržitým dohledem městské policie. Vnitřní uzavřená síť úložišť má v současnosti úložnou kapacitu 5 TB, jenž je užívána k ukládání všech dat úřadu města. Síť je rozdělena do několika části, ve kterých probíhá replikace (vícenásobné uložení) dat. V nočních hodinách dochází k pravidelnému zálohování dat na pásky a jejich následné uchovávaní mimo TC, do menších úložišť mimo TC, prostřednictvím optické metropolitní sítě Města Uherské Hradiště (dále jen MANUH).

Počítač, ze kterého je přistupováno je spolu s uživatelským účtem, nejprve ověřen, zda přihlašovaná osoba má oprávnění požadované ke vstupu. Hesla k přístupu jsou měněna pravidelně každých 90 dnů dle stanovených pravidel. Připojované počítače jsou zapojeny do domény, jejich OS jsou pravidelně aktualizovány, mají nakonfigurovaný firewall a nainstalovány antivirové programy s automatickou aktualizací a další bezpečnostními utilitami. Zlepšování zabezpečení dat se provádí průběžně s ohledem na vznikající hrozby a rizika, novou legislativu a rozvoj bezpečnostních prvků a technologií. Do budoucna Uherské Hradiště zvažuje pořízení bezpečnostního softwaru DLP (Data Lost Prevention), jenž podrobně monitoruje a zaznamenává nakládání s konkrétními daty k zabránění jejich ztráty.

Servery jsou chráněny perimetrem tvořeným bezpečnostními prvky Router-Firewall a HA Firewall Cisco Meraki v HA clusteru. Síťový provoz je monitorován sondou v síti GreyCortex Mendel a bezpečnostním prvkem SIEM – Security Information Event Management.

Data samotného krizového řízení jsou uložena v technologickém a datovém centru Zlínského kraje. Tyto data jsou sdílena a pravidelně aktualizována prostřednictvím optické komunikační infrastruktury Zlínského kraje (KIZK) k jejímuž připojení pracovníci města Uherské Hradiště využívají městskou síť MANUH.

Ing. Lacka z Městského úřadu města Uherské Hradiště, se v rámci rozhovorů o současném řešení ukládání dat městem UH vyslovil pro možnost využití cloudových úložišť, byť s výhradami. Zaujímá názor, že v případě určitého druhu citlivých dat je lepší, aby byla uložena na vlastním serveru v případě krizového řízení. Zvláště v případě, kdy zákon jasně hovoří o tom, který subjekt je zpracovatelem krizového plánu na úrovních kraj a obec s rozšířenou působností. Určitou logiku spatřuje v ukládání dat u zpracovatele těchto plánu, což dle jeho názoru, zajišťuje celkovou provázanost a ucelenost. Majitele a uživatele dat však mohou vést k využití cloudových úložišť od soukromých poskytovatelů vlastní důvody. Za předpokladu dodržení požadavků stanovených zákonem a splnění požadavků majitele na zabezpečení, se nevyslovuje proti možnosti využití ukládání dat na cloudová úložiště.

4.2 Charakteristika vybraných úložišť

Dle uvážení autora práce a všeobecné známosti cloudových úložišť, jsou pro potřeby porovnání a nalezení nejlepšího řešení, vybrána úložiště:

- Dropbox Business Enterprise
- Google Drive
- iCloud Drive
- MEGA
- Microsoft Azure
- Microsoft OneDrive

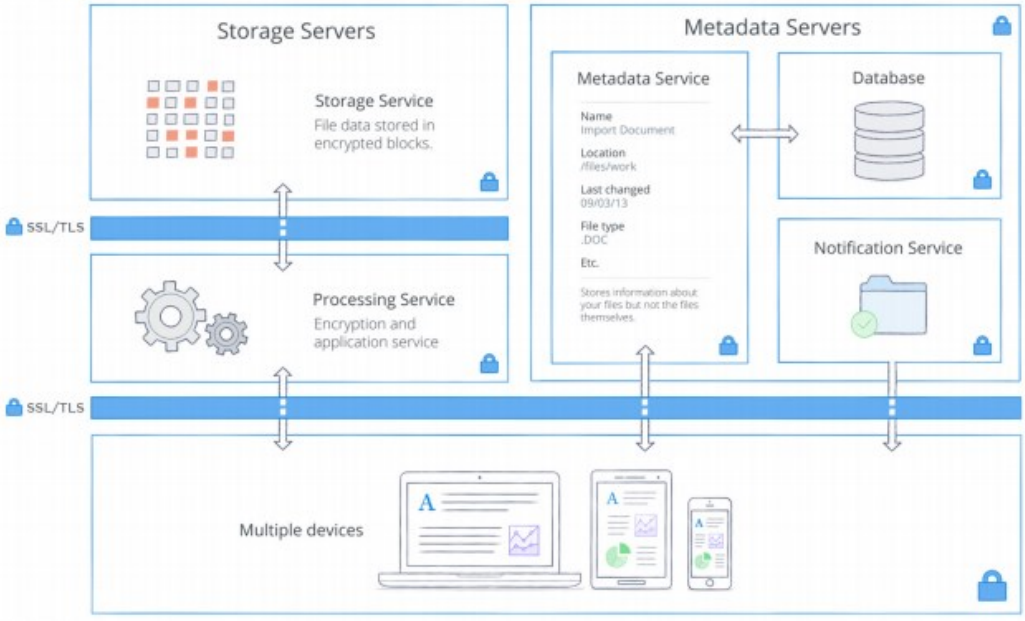
4.2.1 Dropbox Business Enterprise

Úložný prostor Dropbox Business nabízí na výběr tři tarify pro týmy či skupiny uživatelů. Základní tarif nazvaný Standard je limitován 2 TB velikostí úložiště. Pro potřeby krizového řízení však předpokládejme potřebu většího prostoru. Zbylé dva tarify již nabízí neomezený prostor pro ukládání dat a jeví se tak vhodnějšími. Druhý z tarifů – Advanced, nabízí již více funkcí. Pro potřeby srovnání není tento tarif vybrán z důvodu dostupnosti technické podpory pouze v pracovní době, což je pro potřeby krizového řízení zcela nedostatečné. Z toho důvodu je pro potřeby porovnání vybrán třetí tarif – Enterprise. [29]

Enterprise poskytuje uživatelům neomezené úložné prostory, jež jsou umístěny na serverech třetích stran a spravovány poskytovateli služeb se sídlem v USA. Konečná cena je smluvní a kalkulována na základě požadavků zákazníka. Jedním z prvků, který ovlivňuje cenu je počet uživatelů. [29]

Uložená data jsou v klidovém stavu chráněna 256-bitovým AES. Každý soubor je rozdělen do bloků a šifrován zvlášť. Při přenosu jsou bloky dat šifrovány nejméně 128-bitovým AES a přenos dat, jako takový, je zabezpečen kryptografickými protokoly Secure Sockets Layer (SSL) / Transport Layer Security (TLS). V případě jakékoliv změny/úpravy dat jsou synchronizovány pouze změněné bloky. Základní informace o datech uživatele (včetně názvů souborů), tzv. metadata, jsou ke zvýšení bezpečnosti uložena odděleně od samotných dat. [30]

Umístění dat a způsob šifrování znázorňuje graficky následující schéma společnosti Dropbox, Obrázek 6: Dropbox architektura.



Obrázek 6: Dropbox architektura [30]

Přístup k datům je umožněn pouze skrze dvou-faktorové ověření skládající se z šestimístného jedinečného kódu a hesla pro přístup k účtu. Užitečnou funkcí pro uživatelé je též možnost udělit oprávnění k přístupu ke konkrétním datům pouze vybraným uživatelům.[2] Lze i limitovat přístup pouze po určitý čas. Pro potřeby obnovení smazaných dat a jejich verzí

[2] Tato funkce by byla v praxi využitelná pro sdílení dat pouze pro konkrétní subjekt(y) krizového řízení. Např. pouze pro jednotky HZS ČR, apod.

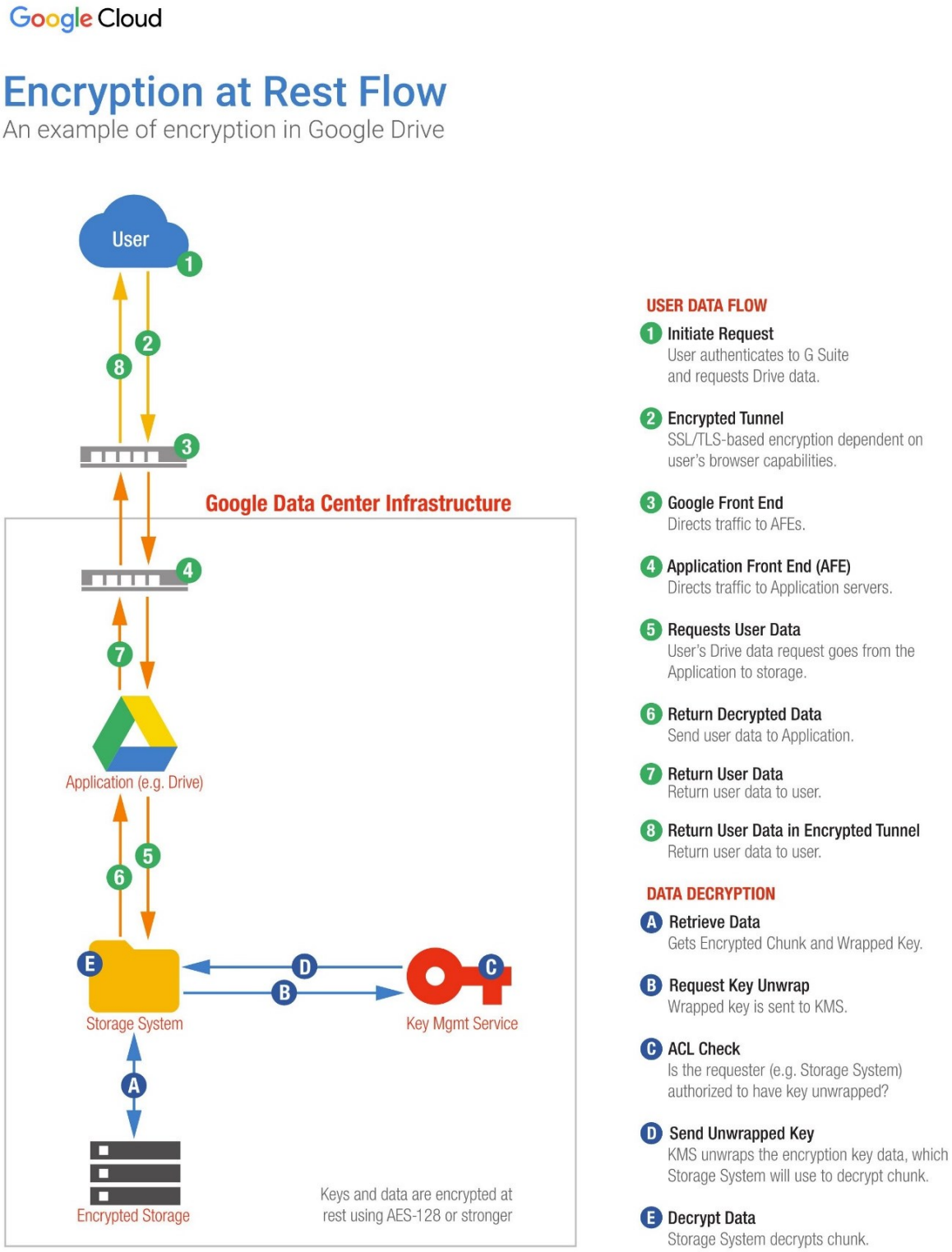
slouží tzv. verzování v délce 120 dní. K uloženým datům lze přistupovat ze zařízení ze zařízení se všemi operačními systémy, bez rozdílu. [30]

4.2.2 Google Drive

Google Drive nabízí stejně jako Dropbox tři tarify – Basic, Business a Enterprise. První balík – Basic nabízí sadu kancelářských nástrojů a úložiště o velikosti 30 GB za cenu 4€ za měsíc pro jednoho uživatele. Balík ovšem není kompatibilní se softwarem třetích stran a stejně Dropbox Standard tak není vhodný pro potřeby krizového řízení. Tarif Business poskytuje neomezený úložný prostor (nebo 1 TB pro uživatele při týmu menším než 5 zaměstnanců) za cenu 8€ za měsíc. Není ovšem také kompatibilní se softwarem třetích stran. Svými nabízenými službami a funkcemi, jež jsou součástí, je určen spíše pro obchodní sféru. Nejlepším tarifem se proto jeví tarif Enterprise s neomezeným úložištěm. Konečná cena opět záleží na požadavcích zákazníka. [31]

Data uživatele jsou po celou dobu existence šifrovány nejméně 128 bitovým AES, přičemž jsou rozdělena na menší, samostatné části, které jsou dešifrovány jedinečnými klíči. Ty jsou šifrovány dalším klíčem, jenž je uložen spolu s daty. Klíč k dešifraci takového balíku je uložen zcela samostatně a zná jej pouze Key management systém, jenž tyto kódy dokáže spárovat. Celý proces šifrování je popsán na Obrázku 7: Šifrování dat v klidu z GSuite Encryption Whitepaper od Google Cloud. [32]

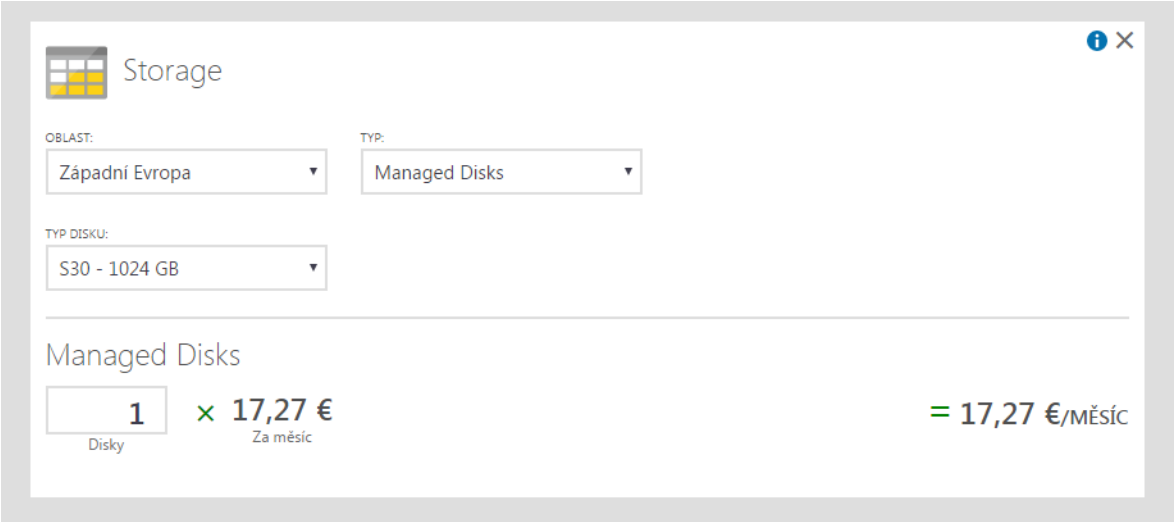
Data jsou ukládány na servery datacenter společnosti Google, která jsou rozmístěna po celém světě a tvoří tak jednu velkou síť. V klidovém stavu jsou data uložena na discích a záložních médiích, a jsou používána pouze data na discích. Záložní média slouží pro obnovu dat v případě mimořádné události způsobené chybou lidského faktoru či přírodního charakteru. V případě smazání dat je lze obnovit do 25 dnů od smazání. Pro obnovení dat po této lhůtě je nutno kontaktovat technickou podporu, nejpozději však do 180 dnů. K uloženým datům lze přistupovat ze zařízení se všemi operačními systémy, bez rozdílu.[32]



Obrázek 7: Šifrování dat v klidu [32]

4.2.3 Microsoft Azure – Storage

Microsoft Azure je stále se rozšiřující kolekce integrovaných cloudových služeb. Na rozdíl od dvou předchozích cloudových úložišť, nenabízí pevný tarif, ale umožňuje nakonfigurovat potřebné prvky a detaily cloudu dle potřeby. Konfigurátor ve svém základu obsahuje možnost výběru regionu datového centra[3], kde bude cloud umístěn, dále typ úložiště a požadovanou velikost úložiště. Vybereme-li oblast datového centra – Západní Evropa a úložištěm bude pevný disk o velikosti 1024 GB (1 TB), cena bude 17,27 €/měsíc. Pro potřeby krizového řízení však je předpokládáno větší úložiště, proto bude třeba více disků a tím se bude skokově zvyšovat i samotná cena. [33]

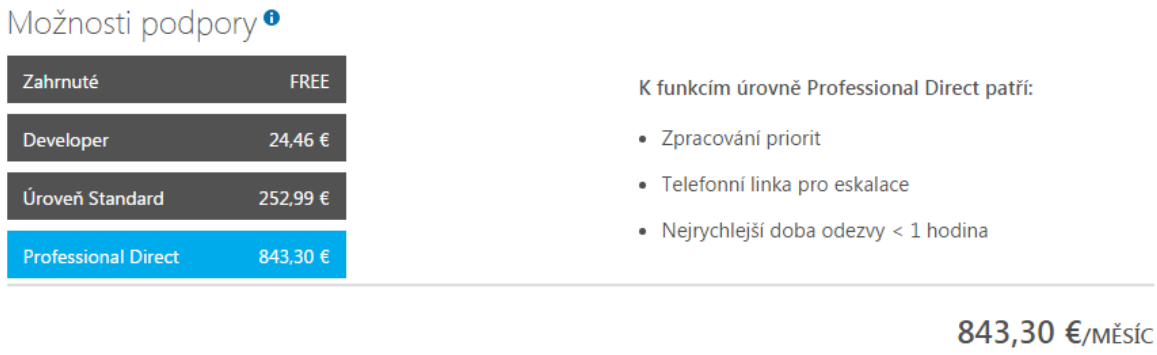


Obrázek 8: Konfigurátor MS Azure Storage [33]

Microsoft klade důraz na zabezpečení a uživatelům svých služeb umožňuje vybrat si z několika možností zabezpečení samotného účtu, šifrování dat při přenosu atd. Data jsou chráněna 256-bitovým AES a jejich přenos probíhá pomocí protokolů SSL/TLS. Před otevřením jsou opět dešifrována. Uživatel k nim přistupuje skrze Resource Manager storage account. Všechny šifrovací klíče jsou opětovně šifrovány, uloženy a spravovány společností Microsoft. Dostatečná zákaznická a technická podpora pro Azure, není na rozdíl od předešlých

[3] Nabízenými oblastmi pro uložená data jsou různé kouty USA, Kanady, Brazílie, Koreji, Austrálie, Německa, Velké Británie či Asie.

cloudů v ceně služby. Její cena je odstupňována, přičemž nejlepší nabídka zákaznické podpory stojí 843,30 €/měsíc, jak je vidět na následujícím obrázku.



Obrázek 9: možnosti podpory Azure [33]

Připojení a využití dalších nejen zabezpečovacích utilit je umožněno. Azure nabízí například přidat oprávnění ke zpracování souborů, možnost spravovat přístupové klíče, omezit přístup pouze skrze HTTPs, vybrané IP adresy atd. Výčet základních možností a kombinací publikoval Microsoft ve svém dokumentu Introduction to Azure Storage, čítající 900 stran. K uloženým datům lze přistupovat ze zařízení se všemi operačními systémy, bez rozdílu. [34]

4.2.4 iCloud Drive

ICloud Drive je součástí systému iOS společnosti Apple – tzv. uzavřeného operačního systému. Rozšíření systému, v podobě dalšího softwaru, lze provést výhradně skrze tržiště aplikací AppStore. Čímž se minimalizuje hrozba pro data uživatele zvenčí. Každé zařízení s iOS kombinuje software, hardware a služby navržené pro poskytnutí maximálního zabezpečení dat uživatele.

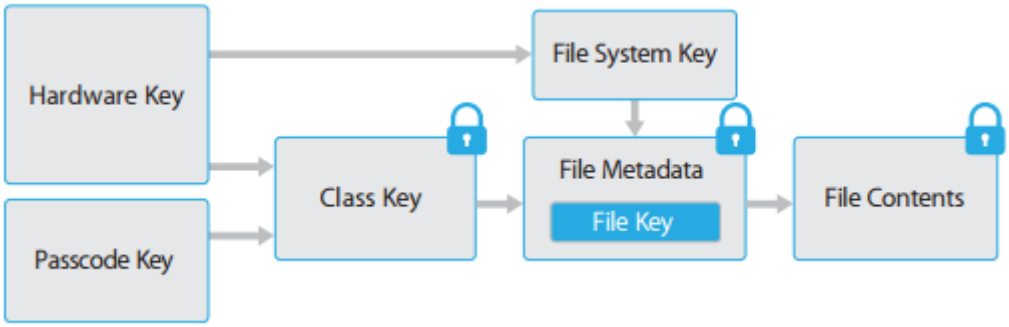
Každému novému uživateli produktů společnosti Apple je vygenerován tzv. Apple-ID, uživatelský účet, který využívá k přihlašování k zařízením zmíněné značky. Každé takové ID má pouze jedno cloudové úložiště, jenž sdílí na všech svých zařízení. Je tím však limitována použitelnost na ostatních operačních systémech – bez zaregistrování se skrze zařízení od Apple, nelze úložiště použít.

Obrázek 10: Domovská obrazovka iCloud[4]

Každé zařízení s iOS má vestavěný AES 256 Engine, který se stará o maximálně efektivní šifrování dat pomocí 256-bitového AES. Tomu dopomáhá též implementovaná hierarchie klíčů, jenž je součástí. Jednotlivé soubory jsou rozděleny do malých bloků, které jsou po změně synchronizovány samostatně. Přenos dat, síť, je zabezpečena SSL/TLS protokoly.

V okamžiku vytvoření nového souboru je vygenerován jedinečný 256 bitový AES klíč, se kterým soubor putuje do AES 256 Enginu, kde dojde ke společnému zašifrování. Následně je šifrováno opětovně a spolu s klíčem na dešifraci tzv. zabaleným souborovým klíčem, je celý balík uložen s metadaty. Dešifrování probíhá opačným způsobem. Systém klíčů užívaných k zabezpečení je vyobrazen na schématu na Obrázku 11: iOS systém klíčů.

[4] Zdroj: Vlastní



Obrázek 11: iOS systém klíčů [35] APPLE. *iOS Securit*

Vůbec prvním zabezpečovacím prvkem pro data je heslo k zařízení, mající charakter čtyř nebo šestimístného, případně alfanumerického kódu. Samozřejmě čím složitější heslo k zařízení, tím lépe. Bez tohoto kódu se nelze dostat k samotným zašifrovaný datům. Bude-li se někdo pokoušet náhodně zadávat klíč, po 5. zadání špatného klíče, je možnost opětovného zadání až po 1 minutě. Nebude-li zadán kód ani na 6. pokus, zařízení odepře přístup na 5 minut. 7. a 8. neúspěšný pokus znamená odepření přístupu vždy na 15 minut a 9. neúspěšný pokus odepře přístup na celou hodinu. [35] APPLE. *iOS Securit*

Servery společnosti Apple jsou nově umístěny nejen v USA, ale i v několik státech Evropy. [36]

Společnost Apple veřejně ceny svých služeb pro Business, jak zní oficiální název sekce pro společnosti, nemá přístupné. Kalkulace nabízených služeb poskytuje po kontaktu na některé ze svých prodejen, či skrze zákaznickou podporu. Pro soukromé uživatele nabízí Apple za měsíční paušál rozšíření základního 5GB úložiště. Za 50 GB uživatel zaplatí 0,99 €, za 200 GB: 2,99 €, za 1 TB činí cena 9,99 € a za 2TB zaplatí 19,99 €. [37]

4.2.5 MEGA

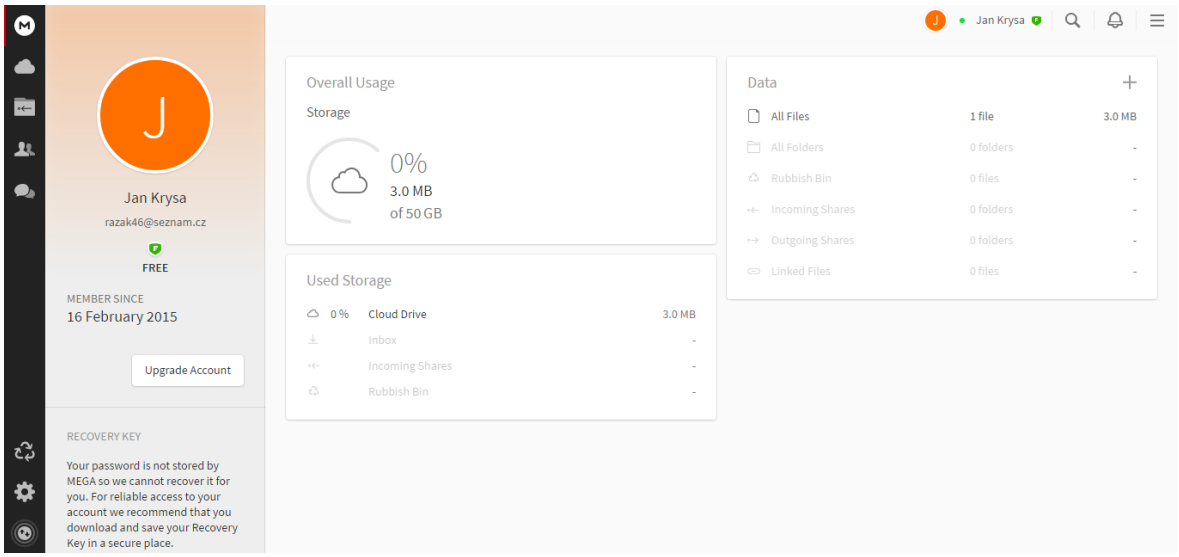
Společnost MEGA provozuje stejnojmenné úložiště a hrdě se prezentuje jako nejlépe zabezpečené na světě. Důvodem je používání tzv. End-to-End ochrany, kdy jsou odchozí data zašifrována již při odeslání z prohlížeče, nikoliv až na ukládaném serveru. Tímto způsobem zamezuje MEGA možnému odposlouchávání komunikace. Samozřejmostí je přístupnost bez předchozí instalace softwaru, jako je tomu u ostatních úložišť.[39]

Základní nabídka úložiště se skládá z pěti tarifů s měsíční platbou. První, základní tarif s 50 GB prostoru je nabízen zdarma. Druhý, nazvané LITE, o velikosti 200 GB stojí 4,99 €. 500 GB PRO I stojí 9,99 €. Za 2TB úložiště PRO II zákazník zaplatí 19,99 € a za 4 TB PRO III

29,99 €. MEGA však nabízí také možnost kontaktu a řešení tzv. na míru, což by bylo vhodné řešení pro subjekty krizového řízení.[38]

U tarifů pro jsou nabízeny rozšiřující funkce v podobě nastavení ochrany heslem pro soubor na úložišti, časové omezení pro sdílené soubory aj. Více funkcí, dostupných pro verzi PRO však při užívání pouze Free tarifu, MEGA nezobrazí. Náhled, alespoň free verze, je k prohlédnutí na Obrázku 12: Náhled MEGA Free po přihlášení.

První věcí, která uživatele zaujme, je absence funkce obnovení hesla, obvyklé u většiny ostatních služeb. K obnovení hesla slouží Obnovovací klíč – soubor, který si uživatel stáhne na bezpečné místo a v případě zapomenutí hesla ke svému účtu jej obnoví skrze tento klíč. Soubory jsou děleny do bloků atributů. Bloky těchto bloků tvoří samotný soubor a jsou od bloků šifrovány 128 bitovým AES. Šifrování je následně šifrováno hlavním symetrickým klíčem, uloženým na serverech MEGA, k nimiž je přístup šifrován užitím slova odvozeného od přihlašovacího hesla uživatele. K uloženým datům lze přistupovat ze zařízení se všemi operačními systémy, bez rozdílu. [39]



Obrázek 12: Náhled MEGA Free po přihlášení[5]

[5] Zdroj: Vlastní

4.2.6 Microsoft OneDrive

Microsoft OneDrive ve své nabídce pro firmy nabízí tři tarify. Prvním z nich je tarif One-Drive Business All-In-One obsahující úložiště spolu s kancelářským balíkem Office 365. Z důvodu zabývá se v práci pouze úložišti, je zmíněný kancelářský balík nadbytečný a tarif je tím nevyhovující. Druhý tarif OneDrive pro firmy obsahuje již pouze cloudové úložiště, limitované však velikostí úložiště o velikosti 1 TB pro uživatele. Pro potřeby krizového řízení je tato kapacita považována za nedostatečnou a tarif tak není vhodný. Vhodným je třetí z nabízených tarifů – OneDrive Business Advanced, jehož součástí je sice úložný prostor o velikosti 1 TB, ovšem se zvětšením na neomezený při pěti a více uživatelích (pro krizové řízení pravděpodobné). Cena tohoto tarifu činí 100,80 €/rok na uživatele. [40]

V oficiálním dokumentu File Security in Microsoft SharePoint and OneDrive for Business společnost Microsoft udává, umístění dat na serverech vlastních datacenter po celém světě. Šifrování souboru je prováděno dvojitě. Každý soubor je při změně opětovně šifrován svým unikátním 256bitovým AES a celý disk pak šifrovacím nástrojem BitLocker. Šifrovací klíče jsou následně sami šifrovány a uloženy v jiném datacentru. Bezpečnost komunikace je zajištěna 2048 bitovým TLS. Přístup k úložišti je založen na ověření uživatele v podobě kombinace několika způsobů, jimiž mohou být:

- ověření identity uživatele nebo skupiny
- přístup skrze schválenou bezpečnou síť
- schválení zařízení a využívané aplikace
- selekce typu dat, ke kterým se uživatel snaží přihlásit.

Každý soubor může být např. omezen koncem platnosti sdílení a zákazem externího sdílení. K záloze dat a tzv. verzování oficiálně Microsoft neuvádí v oficiálním dokumentu počet dní. Zákaznická podpora je dostupná v ceně tarifu a k uloženým datům lze přistupovat ze zařízení se všemi operačními systémy, bez rozdílu. [41]

4.3 Komparace vybraných cloudových úložišť

Pro potřeby komparace je třeba nejprve stanovit váhy (užijeme stupnice 0-5), a ohodnotit parametry u každého úložiště (stupnice 0–10). Číslo nula bude hodnocením pro absenci či neexistenci. Naopak, čísly 5 u váhy a číslem 10 u hodnocení, to nejdůležitější, a z hlediska

technologií nejlepší dostupné řešení[6]. Informace, které poskytovatel neuvádí, budou hodnoceny známkou 3.

Výstupem samotné komparace budou dvě tabulky. První přehledně shrnující charakteristiku úložišť, druhá obsahující samotné ohodnocení parametrů, s ohledem na jejich důležitost a složitost.

Nejlepší cloudové úložiště, bude určeno na základě vah a hodnot kritérií – výpočtem váženého průměru.

Komparační kritéria

Cloudová úložiště od poskytovatelů je třeba komparovat. K tomuto účelu jsou vybrána kritéria:

1. **Tarif – velikost úložiště**

Prvním aspektem při výběru úložiště je jeho velikost. Pro krizové řízení se jeví nejvhodnější volbou úložiště s neomezeným prostorem. V případě potřeby uložení většího množství dat v krátkém časovém sledu, by omezená kapacita úložiště znamenala hrozbu pro funkčnost celého řešení, v krajním případě by mohlo dojít k absolutní paralýzu využívaného systému.

Z uvedených důvodů je velikost úložiště hodnoceno známkou 4,5/5. Jeho cena je na stupnici důležitosti při výběru vhodného cloudového úložiště hodnoceno známkou 2/5.

2. **Umístění serverů**

Fyzické umístění serverů s úložišti souvisí s vícenásobným ukládáním dat v různých datových centrech, zpravidla v jiných státech. Velcí poskytovatelé vlastní datacentra rozmístěná po celém světě, např. kvůli hrozbě porušení podmořského kabelu na dni oceánů a přerušení internetu pro některé oblasti, možnosti výpadku elektrické energie v oblasti datacentra apod. Z tohoto důvodu je toto kritérium hodnoceno známkou 2/5.

[6] Hodnoty u jednotlivých parametrů budou přiřazovány autorem práce na základě vlastního uvážení a s ohledem na znalost problematiky.

3. Šifrování dat (File Encryption) v klidovém stavu a při přenosu

Hodnocení tohoto kritéria se odvíjí od složitosti využitých kryptografických protokolů, jenž jsou užity pro převedení dat do zašifrované podoby za pomocí šifrovacího klíče. Zašifrovaná data oprávněný uživatel dešifruje svým dešifračním klíčem. Platí úměra: čím více využitých bitů pro šifrování, tím je dešifrace bez dešifračního klíče složitější a náročnější.

K šifrování souborů pro cloudová úložiště, je dnes užíváno tzv. AES (Advanced Encryption System), což je pokročilý systém šifrování užívající totožný klíč pro šifraci i dešifraci dat rozdělených do bloků o pevně dané délce.

Počet užívaných bitů pro šifraci dat bude porovnávaným prvkem. Z hlediska důležitosti je toto kritérium ohodnoceno známkou 5/5.

4. Zabezpečení komunikace protokoly

Pro zvýšení bezpečnosti dat při přenosu jsou běžně užívány kryptografické protokoly SSL/TLS[7] zabezpečující komunikace na internetu. Je třeba tedy zjistit, zda cloudová úložiště využívají alespoň těchto protokolů. Kritérium má pro výběr cloudového úložiště váhu 5/5.

5. Synchronizace upravených bloků

V kritériu Šifrování dat (File Encryption) v klidovém stavu a při přenosu, je zmínka o rozdělení dat do bloků o přesné délce či velikosti. Synchronizace pouze upravených bloků urychluje přenos a ukládání dat, je tím tak snížena náročnost na tuto operaci. Cílem tohoto kritéria je potvrdit, zda porovnávaná cloudová úložiště využívají popsaného principu či nikoliv. Důležitost je stanovena známkou 1,5/5.

6. Uložení metadat

Úkolem metadat je poskytnout informace o dalších (větších) datech.

Z důvodu bezpečnosti a přístupu ke koncovým datům jsou metadata ukládána samostatně. Nutno potvrdit, je-li tomu tak i u komparovaných úložišť. Důležitost uložení metadat je hodnocena známkou 2,5/5.

[7] Bližší popis protokolů dostupný online na adrese: https://www.ssls.cz/slovnik/tls.html

7. Autentizace pro přístup k datům

Tímto kritériem se dostáváme k velmi důležitému, či téměř nejdůležitějšímu, faktoru při výběru. Je jím zabezpečení úložiště a uložených dat před neautorizovaným přístupem či jejich zcizením. Jak bylo zmíněno v teoretické části, na úložiště jsou ukládána data soukromého či důvěrného charakteru. V případě krizového řízení, je nutno uložit i data, jenž podléhají některému ze stupňů utajení. Proto není radno podcenit zabezpečení.

Přístup k datům je třeba ošetřit alespoň dvou-faktorovým ověřením identity, tak jak je to již u mnoha poskytovatelů běžnou praxí i pro soukromé uživatele. Je nutno zjistit, zdali poskytovatel skutečně nabízí dostatečné zabezpečení, případně zdali je nabízeno několik možností pro vlastní výběr.

Úroveň zabezpečení přístupu je důležitým prvkem, proto je toto kritérium hodnoceno známkou 4,5/5 na stanovené stupnici důležitosti.

8. Verzování a záloha dat (Backup)

Přestože nemusí dojít ke zcizení dat, může se stát, že dojde k chybě lidského faktoru a vymazání nesprávných dat nebo se vyskytne porucha na serverech úložiště a tím dojde ke ztrátě. K eliminaci škod ztráty se využívá tzv. zálohování čili uložení přesné kopie na jiné, nezávislé místo, ze něhož jsou data případně obnovena.

Zálohovat lze nejen koncové soubory, ale i jejich jednotlivé verze. Tento způsob zálohy je znám jako tzv. verzování. Porovnávaným prvkem proto bude časový údaj pro stáří dané verze souboru, který lze obnovit. Jinými slovy, jestli lze obnovit verzi souboru, která je starší než 30/60/90 a více dnů. Pro bezpečnost a zachování důležitých dat je tato funkce pro cloudové úložiště důležitá, a tedy hodnocena známkou 3,5/5.

9. Dostupnost technické podpory

V okamžiku technické poruchy, případně neobvyklé (ne)funkčnosti cloudového úložiště je nutno nastalou situaci řešit okamžitě a nelze se spokojit s dostupností technické podpory např. pouze pomocí e-mailů a v pracovních dnech. Dostupnost podpory nonstop a součást tarifu/služba za příplatek, jsou dalším kritériem při výběru vhodného cloudového úložiště. S ohledem na nezbytnost této služby pro cloudové úložiště využívané krizovým řízením, je toto kritérium hodnoceno známkou 4,5/5.

10. Kompatibilita se softwarem třetích stran

V oblasti krizového řízení je užíván speciální, většinou veřejně nedostupný, software. Neschopnost spuštění a možnost správného užívání tohoto softwaru je nepřípustná. Vydavatelé z tohoto důvodu nabízí distribuce softwaru pro konkrétní operační systémy, čímž předchází nemožnosti užít všechny jeho funkce. Kritérium hodnoceno je velmi důležité, proto hodnoceno známkou 4,5/5.

11. Přístupnost k datům ze zařízení z jakéhokoliv OS

Posledním kritériem pro komparaci cloudových úložišť je možnost přístupu ze zařízení s jakýmkoliv operačním systémem. V dnešní době jsou známy tři druhy operačních systémů – Windows od společnosti Microsoft, Linux v různých distribucích a distribuce OS od společnosti Apple.

Cílem je zjistit, zda lze k datům přistupovat ze všech operačních systémů bez rozdílů a omezení. Na stupnici významnosti ohodnoceno známkou 2/5.

4.4 Vyhodnocení komparace cloudových úložišť

Srovnáváme-li postupně dle kritérií z předešlé kapitoly a jež jsou uvedeny také v Tabulce 1: Přehled úložišť v tabulce, všichni poskytovatelé úložišť nabízí krom pevného tarifu i možnost dojednání individuálních potřeb a prakticky neomezené úložiště. Nelze tedy říct na základě alespoň ceny říci, které úložiště je v tomto kritériu nejlepší.

Z hlediska lokace serverů s úložišti opět nelze porovnat, která služba je nejlepší pro potřeby vícenásobného uložení dat. Zatímco Dropbox Enterprise využívá pro ukládání dat uživatelů úložiště 3. stran, Google i Microsoft mají vlastní datacentra rozmístěná po celém světě. Společnost Apple spravuje také vlastní datacentra, v letošním roce již kromě USA i v Evropě. Úložiště MEGA informace o umístění datacenter veřejně neuvádí.

Porovnávaná cloudová úložiště využívají všechny nejméně 128 bitové AES poskytující dostatečné šifrování pro bezpečnost dat. Protokoly, skrze něž probíhá komunikace, tedy přenos uložených dat, neuvádí iCloud a MEGA. Lze však přepokládat, že stejně jako u ostatních tří

úložišť, je chráněna alespoň SSL/TLS protokoly. Z důvodu využití způsobu End-To-End[8] zabezpečení úložištěm MEGA a 2048 bitového TLS protokolu služby OneDrive, lze tyto služby hodnotit jako nejlépe zabezpečené z porovnávaných úložišť.

Synchronizace dat u všech úložišť probíhá pouze u bloků, kde byla provedena změna. Uvádí-li poskytovatel úložiště kde jsou uložena metadata, je tomu tak vždy samostatně. Přístup k datům mají poskytovatelé vždy ošetřen nutností mít alespoň kombinaci dvou bezpečnostních faktorů.

Tzv. verzování čili dostupnost předešlých verzí uložených dat deklarují DropBox a Google Drive. U zbylých úložišť lze na základě možnosti dohodnutí individuálních požadavků, předpokládat i tato funkce.

Stejný předpoklad je i u dostupnosti online podpory. Překvapením u tohoto kritéria, je příplatek za ni u Microsoft Azure Storage, jelikož DropBox, Google Drive či Microsoft OneDrive ji nabízí již v ceně. Neznámou však může být komplexnost a schopnost všech podpor v praxi.

S výjimkou iCloud jsou všechny cloudová úložiště dostupná bez rozdílu na operační systém. Z důvodu není iCloud považován za vhodný pro potřeby subjektů krizového řízení.

Z důvodu kompatibility a komplexnosti nabízeného softwaru a utilit společností Microsoft jsou nejvhodnějším cloudovým úložištěm pro krizové řízení Microsoft Azure a Microsoft OneDrive. V případě nevyužívání žádného softwaru od zmíněné společnosti, je nejvhodnějším řešením (bez přidělení vah a hodnot) Google Drive Enterprise, díky rozmístění vlastních datacenter po celém světě, možností vybrat způsob zabezpečení pro přístup k úložišti, verzování souboru po dobu až180 dnů atd.

[8] Pro připomenutí: odesílaná data jsou ještě před samotným přenosem zašifrována, tj. prakticky po celou svoji existenci.

Tabulka 1: Přehled úložišť v tabulce (Zdroj: Vlastní)

Název cloudové služby		**Dropbox**	**Google Drive**	**Microsoft Azure - Storage**	**iCloud Drive**	**Mega**	**Microsoft OneDrive**
Tarif	**Název**	Enterprise	Enterprise	-	-	-	Business Advanced
	Velikost Neomezena	✓	✓	✓	Neuvádí	Smluvní	✓
	Cena	Smluvní	Smluvní	Dle konfigurace	Neuvádí	Smluvní	100,80 €/rok/už.
Umístění serverů		Servery třetích stran se sídlem v USA	Vlastní po celém světě	Vlastní po celém světě	USA a Evropa	Neuvádí	Vlastní po celém světě
Zabezpe-čení	**Šifrování v klidu**	256 bit AES	> 128 bit AES	256 bit AES	256 bit AES	128 bit AES *	256 bit AES
	Při přenosu	> 128 bit AES	> 128 bit AES	256 bit AES	256 bit AES	128 bit AES *	256 bit AES
	Protokoly	SSL/TLS	SSL/TLS	SSL/TLS	Neuvádí	Neuvádí	TLS (2048 bit)
Synchronizace upravených bloků		✓	✓	✓	✓	✓	✓
Uložení metadat samostatně		✓	✓	✓	✓	✓	✓
Přihlášení		6místný jedinečný kód + heslo	2step/sample 2.0/ Auth 2.0/ Open id connect	Neuvádí	Specifické	Specifické	Kombinace Několika
Verzování (počet dnů)		120	180	Neuvádí	Neuvádí	Neuvádí	Neuvádí
Nonstop podpora v ceně		✓	✓	X	Neuvádí	Neuvádí	✓
Kompatibilní se softwarem třetích stran		✓	✓	✓	X	✓	✓
Kompatibilní se všemi OS		✓	✓	✓	X	✓	✓

poznámka: * END-TO-END způsob šifrování

Tabulka 2: Přehled úložišť s přiřazenými vahami a hodnotami (Zdroj: Vlastní)

		VÁHA KRITÉRIA	**HODNOTA**	**HODNOTA**	**HODNOTA**	**HODNOTA**	**HODNOTA**	**HODNOTA**
Název cloudové služby			Dropbox	Google Drive	Microsoft Azure (Storage)	iCloud Drive	Mega	Microsoft OneDrive
Tarif	***Název***		Enterprise	Enterprise	-	-	-	Business Advanced
	Velikost neomezena	4,5	10	10	10	3*	10	10
	Cena	2	9	9	6	3*	9	8
Umístění serverů		2	7	10	10	8	9	10
Zabezpe-čení	***Šifrování v klidu***	5	9	8	9	9	10	9
	Při přenosu	5	9	8	9	9	10	9
	Protokoly	5	8	8	8	3*	3*	10
Synchronizace upravených bloků		1,5	10	10	10	10	10	10
Uložení metadat samostatně		2,5	10	10	10	10	10	10
Přihlášení		4,5	8	9	3*	9	9	9
Verzování (počet dnů)		3,5	8	9	3*	3*	3*	3*
Nonstop podpora v ceně		4,5	10	10	0	3*	3*	10
Kompatibilní se všemi OS		4,5	10	10	10	5	10	10

poznámka: * Informace neuvedena poskytovatelem

Výpočet váženého průměru

Vážený průměr se užívá v případě rozdílné důležitosti hodnot (x), kterým se přiřazuje váha (p). V případě totožnosti vah u všech hodnot, by se již nejednalo o průměr vážený, nýbrž aritmetický. Pro výpočet váženého průměru platí obecně známý vzorec:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i p_i}{\sum_{i=1}^{n} p_i} = \frac{x_1 p_1 + x_2 p_2 + \ldots + x_n p_n}{p_1 + p_2 + \cdots + p_n}$$

Výsledky výpočtu nezaokrouhlených vážených průměrů jednotlivých úložišť z Tabulky 3: Výpočet váženého průměru na následující straně:

- Dropbox Enterprise = 9,011235955
- Google Drive Enterprise = 9,101123596
- Microsoft Azure (Storage) = 7,179775281
- iCloud Drive = 6,337078652
- MEGA = 7,764044944
- Microsoft OneDrive Business Advanced = 9,033707865

Z uvedených hodnot lze vyčíst výsledek: Nejlepšího výsledku dosáhl Google Drive Enterprise s váženým průměrem 9,10 následovaný uložištěm Microsoft OneDrive Business Advanced s 9,03 a Dropbox Enterprise s 9,01.

Tabulka 3: Výpočet váženého průměru (Zdroj: Vlastní)

Vzorec užitý k výpočtu váženého průměru: $\bar{x} = \frac{\sum_{i=1}^{n} x_i p_i}{\sum_{i=1}^{n} p_i} = \frac{x_1 p_1 + x_2 p_2 + \ldots + x_n p_n}{p_1 + p_2 + \cdots + p_n}$

		Dropbox		Google Drive		MS Azure		iCloud		MEGA		MS OneDrive	
krité-rium č.	váha (p) kritérií	**přiřazené hodnoty x_n**	$p*x_n$	**přiřazené hodnoty x_n**	$p*x_n$	**přiřazené hodnoty x_n**	$p*x_n$	**přiřazené hodnoty x_n**	$p*x_n$	**přiřazené hodnoty x_n**	$p*x_n$	**přiřazené hodnoty x_6**	$p*x_n$
1	4,5	**10**	45	**10**	45	**10**	45	**3**	13,5	**10**	45	**10**	45
2	2	**9**	18	**9**	18	**6**	12	**3**	6	**9**	18	**8**	16
3	2	**7**	14	**10**	20	**10**	20	**8**	16	**9**	18	**10**	20
4	5	**9**	45	**8**	40	**9**	45	**9**	45	**10**	50	**9**	45
5	5	**9**	45	**8**	40	**9**	45	**9**	45	**10**	50	**9**	45
6	5	**8**	40	**8**	40	**8**	40	**5**	25	**3**	15	**10**	50
7	1,5	**10**	15	**10**	15	**10**	15	**10**	15	**10**	15	**10**	15
8	2,5	**10**	25	**10**	25	**10**	25	**10**	25	**10**	25	**10**	25
9	4,5	**8**	36	**9**	40,5	**3**	13,5	**9**	40,5	**9**	40,5	**9**	40,5
10	3,5	**8**	28	**9**	31,5	**4**	14	**3**	10,5	**3**	10,5	**3**	10,5
11	4,5	**10**	45	**10**	45	**0**	0	**6**	27	**3**	13,5	**10**	45
12	4,5	**10**	45	**10**	45	**10**	45	**3**	13,5	**10**	45	**10**	45

Suma vah:	Vážený průměr Dropbox:	Vážený průměr Google Drive:	Vážený průměr MS Azure:	Vážený průměr iCloud	Vážený průměr MEGA	Vážený průměr MS OneDrive
44,5	**9,01**	**9,10**	**7,17**	**6,33**	**7,76**	**9,03**

4.5 Návrh vlastního cloudového řešení

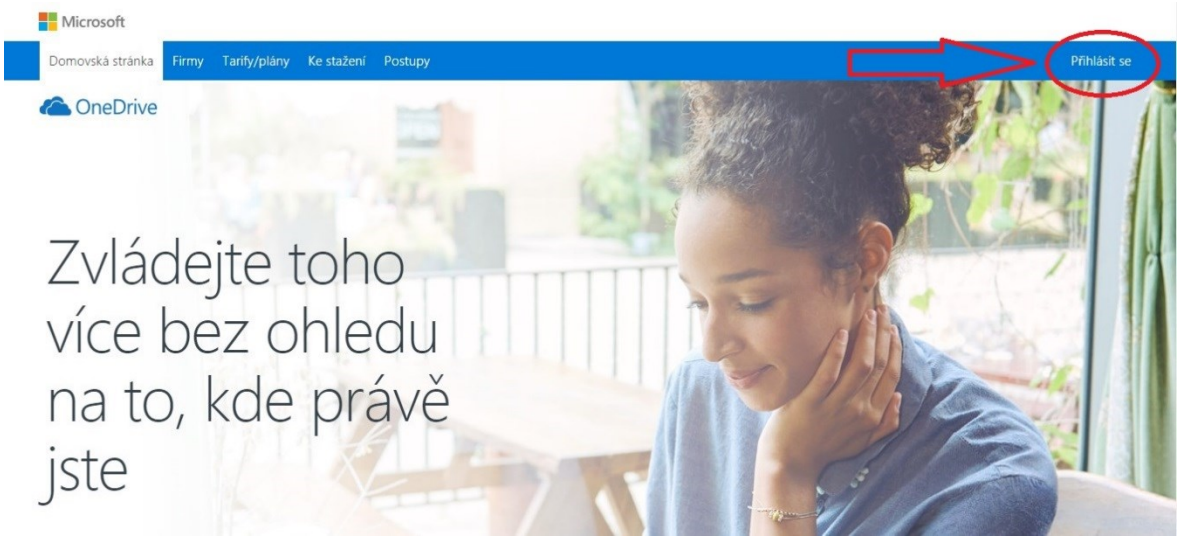
Pomyslným vítězem komparace cloudových úložišť v předešlé kapitole se stal Google Drive Enterprise. Toto úložiště však není pro autora práce dostupné, z tohoto důvodu bude pro potřeby návrhu a simulace potřebných kroků pracovníka krizového řízení, využit Microsoft OneDrive, umístěný druhý v pořadí.

Využití zmíněného úložiště je možné na základě studiu autora práce na Univerzitě Tomáše Bati ve Zlíně. Každému studentovi a pracovníkovi univerzity je v rámci zakoupené licence Microsoft Office 365 Education[9], umožněno využívat funkce tohoto balíku, jehož součástí je také úložiště OneDrive.

4.5.1 Přihlášení se

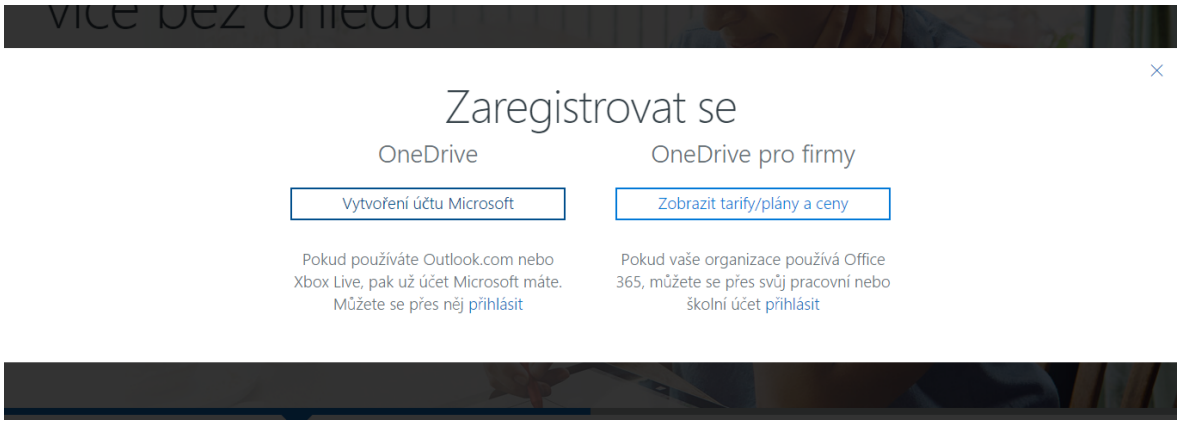
Přihlášení se k úložišti OneDrive je možné dvěma způsoby. Prvním z nich je přihlášení se na adrese defaultní adrese pro Office 365: office365.utb.cz. Druhou možností je přistoupení k úložišti vyhledáním úložiště prostřednictvím webového prohlížeče, případně zadání adresy https://onedrive.live.com. Na této webové stránce je třeba kliknout na tlačítko „Přihlásit se“, umístěné na vpravo na liště nabídky (Obrázek 13: OneDrive – domovská stránka před přihlášením).

[9] Součástí školní licence Office365 Education for Students jsou mmj. licence na: Microsoft Teams, Microsoft StaffHub, Flow for Office 365, PowerApps for Office 365, Azure Rights Management, Microsoft Forms (Plan 2), Microsoft Planner, Sway, Mobile Device Management for Office 365, Yammer for Academic, Office Online for Education, Skype for Business Online (Plan 2), SharePoint Plan 1 for EDU a Exchange Online (Plan 1). Seznam licencí uživatelského účtu je k zobrazení po přihlášení, v sekci Můj účet – Předplatná.



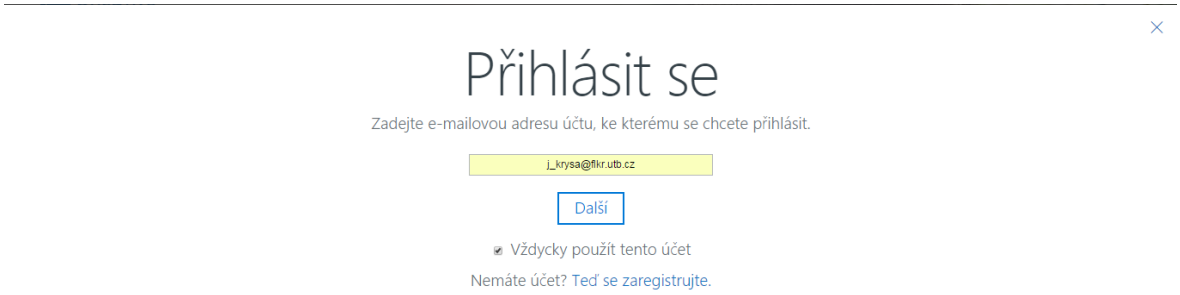
Obrázek 13: OneDrive – domovská stránka před přihlášením (Zdroj: Vlastní)

Následně je zobrazena nabídka Zaregistrovat, jak je vidět na Obrázku 14: OneDrive – okno s nabídkou registrace. Díky školnímu účtu vybereme možnost „přihlásit“ pod nabídkou One-Drive pro firmy.



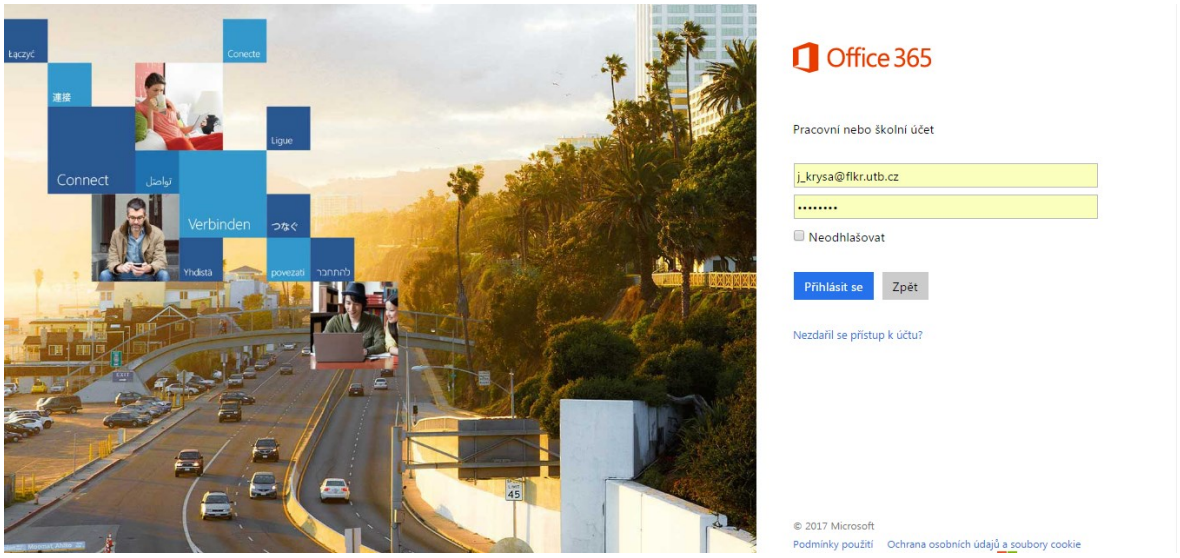
Obrázek 14: OneDrive – okno s nabídkou registrace (Zdroj: Vlastní)

Uživatel je v dalším kroku vyzván k přihlášení, zadáním svého univerzitního e-mailu. Autor práce se tedy přihlašuje skrze e-mailovou adresu j_krysa@flkr.utb.cz, jak je vidět na Obrázek 15: OneDrive – zadávání „firemního“ e-mailu.



Obrázek 15: OneDrive – zadávání „firemního“ e-mailu (Zdroj: Vlastní)

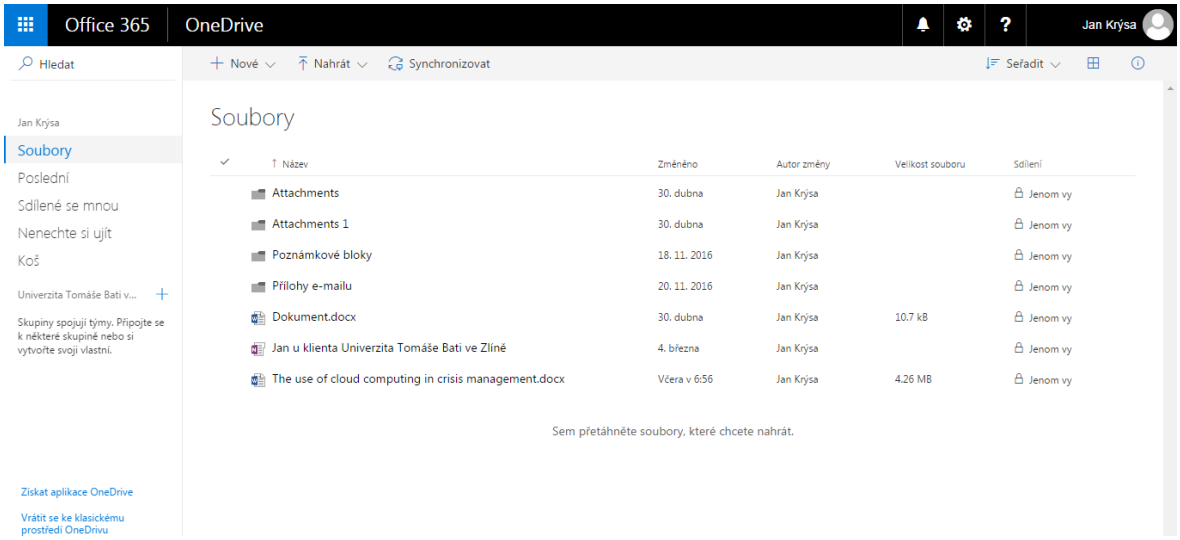
Nutností je také přihlášení se ke zmíněnému kancelářskému balíku Office365 v dalším kroku, opět zadáním zmíněného e-mailu a svého hesla. Viz Obrázek 16: OneDrive – Přihlášení do Office 365. Z důvodu přihlášení se ke službě již dříve a zapamatování si údajů prohlížečem, jsou okna s přihlašovacími údaji podbarvena žlutou barvou (závislé na předešlém nastavení prohlížeče uživatelem). Jsou-li údaje zadávány poprvé či nezapamatovány, okna jsou podbarvena bílou barvou.



Obrázek 16: OneDrive – Přihlášení do Office 365 (Zdroj: Vlastní)

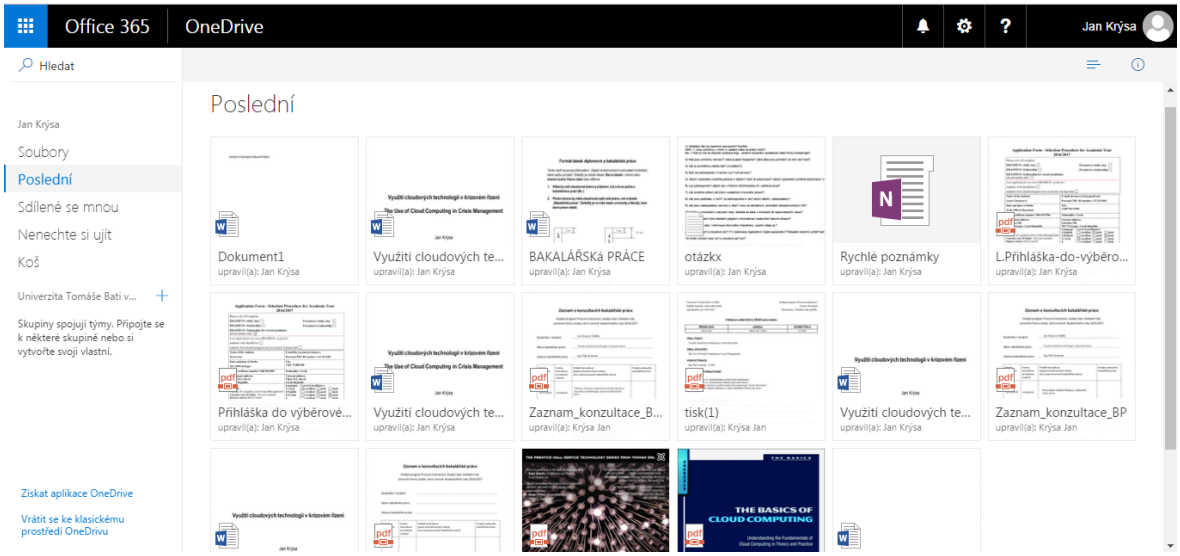
4.5.2 Prostředí úložiště

Po přihlášení se již uživatel dostává do svého cloudového úložiště, kde se mu zobrazují mmj. i soubory z jiných nástrojů Office 365, k nimiž má účet licenci. Například poznámkové bloky z nástroje OneNote. Na Obrázku 17: OneDrive – rozhraní cloudu po přihlášení se, lze vidět soubor (předposlední v seznamu) právě z tohoto nástroje.



Obrázek 17: OneDrive – rozhraní cloudu po přihlášení se (Zdroj: Vlastní)

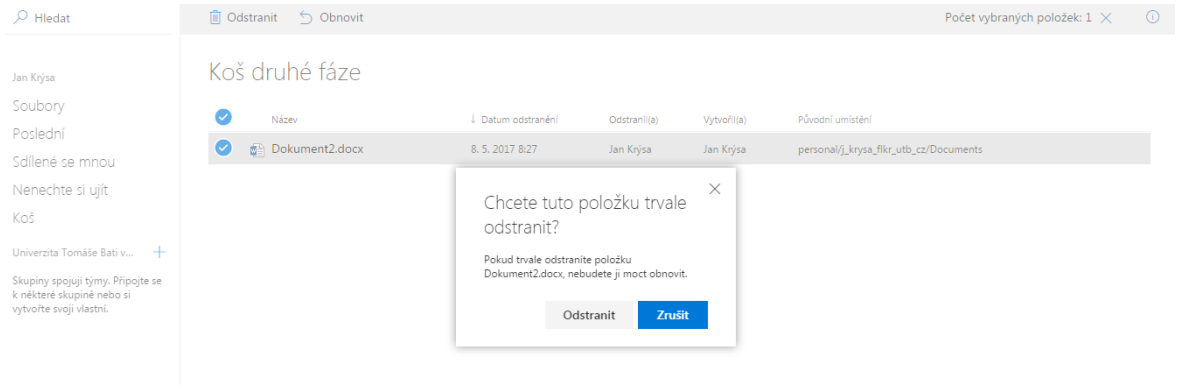
Z hlediska přehlednosti je úložiště řešeno dostatečně. Na levé straně se nachází nabídka vlastních souborů, posledních upravovaných souborů (užitečný nástroj zejména při větším množství souborů uložených na disku, kde by složité hledání naposledy upravovaného souboru zabralo zbytečný čas - Obrázek 18: OneDrive – Položka nabídky „Poslední“), souborů, jenž s uživatelem sdílí jiná osoba skrze OneDrive, a Koš pro odstaněné soubory.



Obrázek 18: OneDrive – Položka nabídky „Poslední“ (Zdroj: Vlastní)

Zajímavostí tohoto koše je jeho dvoufázovost. Smaže-li uživatel, či některý z uživatelů, ze seznamu souborů některý z nich, je přesunut do koše, jeho první fáze. Pro přesunutí do druhé fáze je třeba opětovně zadat příkaz ke smazání. K nenávratnému smazání dojde až v okamžiku zadání smazání a potvrzení vyskakovací hlášky na následujícím Obrázku 19:

Druhá fáze koše. Zmíněná dvoufázovost je užita jako záchrana souboru v případě jeho nechtěného odstranění. Odstraní-li uživatel trvale soubor, jenž sdílí s jiným uživatelem, je tento soubor odstraněn i jemu. Záleží však na samotném nastavení sdílení.

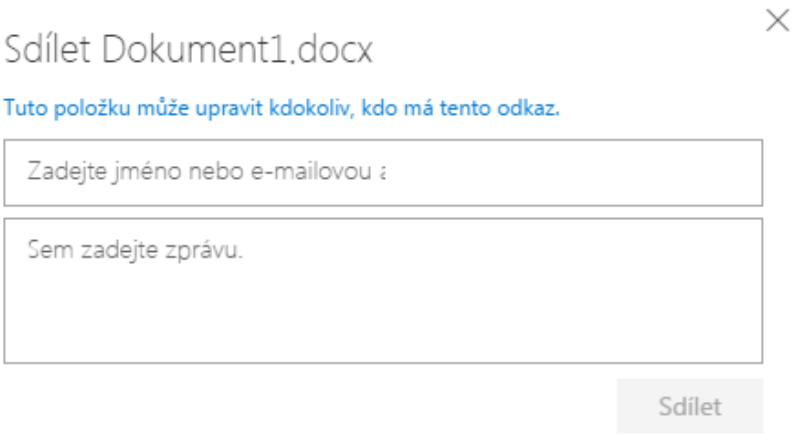


Obrázek 19: Druhá fáze koše (Zdroj: Vlastní)

Prostředí úložiště nabízí také vytvoření nového souboru online po vybrání „Nové“ na vodorovné šedé liště. Uživatel tak může vytvořit prezentace, tabulky, dokumenty, složky, poznámkové bloky a odkazy bez nutnosti instalace softwaru na své zařízení. Soubory a složky, vytvořené může pohodlně nahrát skrze funkci „Nahrát“ umístěnou hned vedle tlačítka pro nové soubory. Pro potřeby průběžné aktualizace souborů a složek (předpokládá se pro potřeby krizového řízení) nabízí OneDrive možnost stažení a instalaci softwaru – synchronizačního klienta, jenž vytvoří v zařízení složku. Vše, co je umístěno do této složky, je v případě zapnutého zmíněného klienta a aktivního připojení k internetu, ihned synchronizováno.

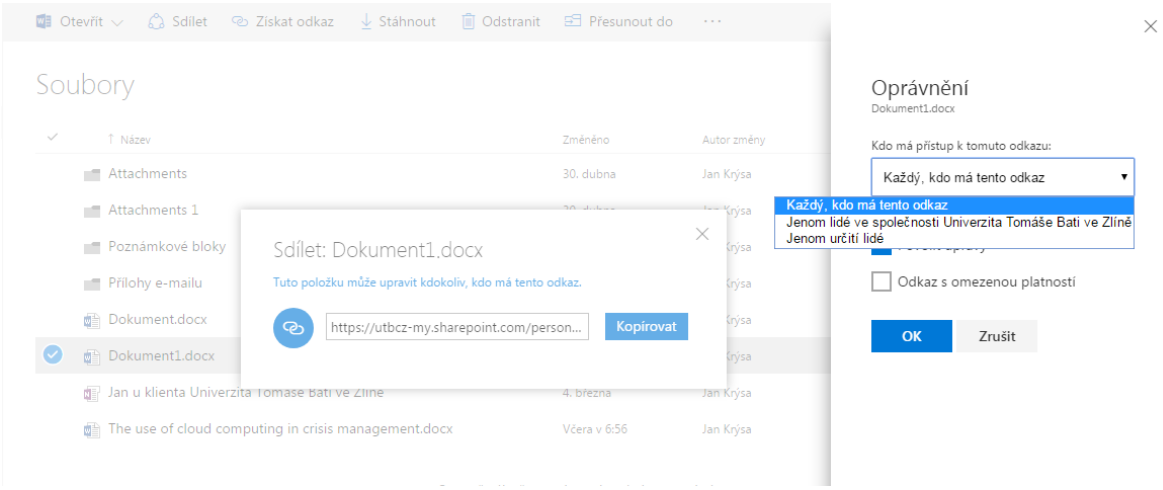
4.5.3 Sdílení souborů

Sdílení souborů je uživateli umožněno vybráním konkrétních souborů ke sdílení a následnému využití funkce „Sdílet“ na šedé liště nad seznamem (funkce se zobrazí na liště až po vybrání souborů). Do vyskočeného okna, jenž je zobrazeno na Obrázku 20: OneDrive – nastavení sdílení dokumentu, je následně možnost vepsat e-mailové adresy adresátů a doplňující zprávu k souboru.



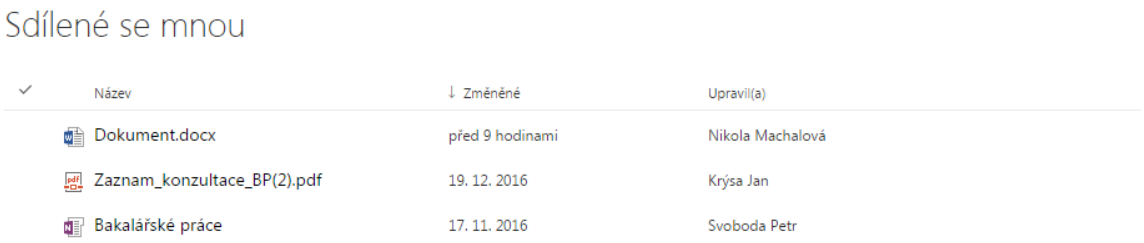
Obrázek 20: OneDrive – Nastavení sdílení dokumentu (Zdroj: Vlastní)

Druhou možností, jak sdílet soubor, je pomocí funkce „Sdílet odkaz“ vygenerovat přímo odkaz na soubor, který je uložen na disku. Tímto odkazem je soubor přístupný komukoliv, není-li nastaveno jinak. Možností je omezit přístup pouze pro osoby ve společnosti nebo jen vybraným lidem, což je zobrazeno na Obrázku 21: OneDrive – nastavení oprávnění sdíleného souboru



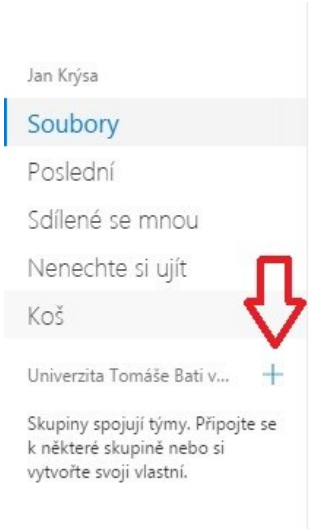
Obrázek 21: OneDrive – nastavení oprávnění sdíleného souboru (Zdroj: Vlastní)

Sdílený soubor se uživatel zobrazí v seznamu ve složce „Sdílené se mnou“, jak je vidět u Document.docx, který upravil(a) Nikola Machalová, a u poznámkového bloku aplikace OneNote, jenž upravil vedoucí práce Ing. Petr Svoboda, na Obrázku 22: OneDrive – soubory Sdílené se mnou.

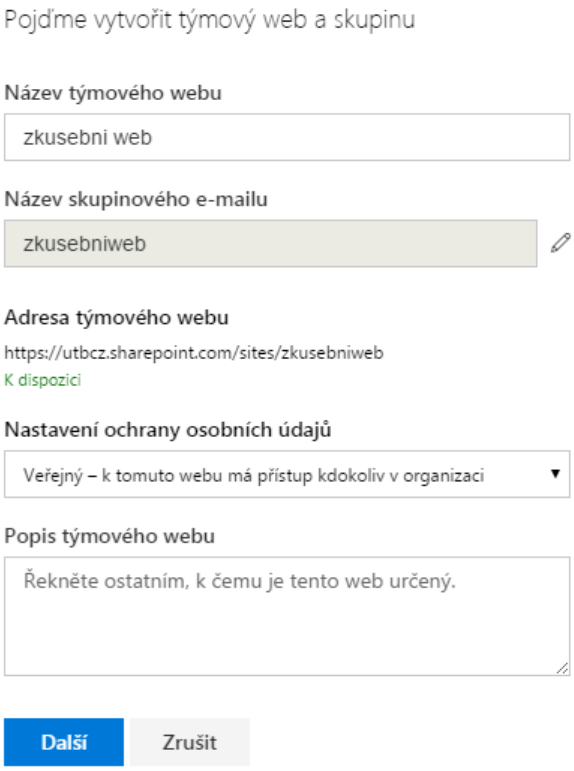


Obrázek 22: OneDrive – soubory Sdílené se mnou

OneDrive nabízí také možnost vytvoření týmového webu pomocí funkce „Vytvořit skupiny“, dostupné po kliknutí na symbol „+“ vedle názvu společnosti, viz Obrázek 23: Tlačítko k vytvoření týmového webu a Obrázek 24: Nastavení týmového webu při jeho zakládání.



Obrázek 23: Tlačítko k vytvoření týmového webu (Zdroj: Vlastní)



Obrázek 24: Nastavení týmového webu při jeho zakládání (Zdroj: Vlastní)

Vytvořením webu vznikne pracovní prostor určený pro spolupráci členů týmu. Tato funkce však již není úložištěm OneDrive pro firmy, ale sdíleným pracovním prostorem fungujícím na podobném principu jako osobní OneDrive, s jedním základním rozdílem. V rámci webu mohou uživatelé spolupracovat na souborech, dokumentech a nápadech současně v reálném čase. SharePoint nabízí „virtuální kancelář“ - možnosti knihoven dokumentů, seznamů úkolů, kalendářů, pracovních postupů a dalších funkcí, které usnadňují týmovou komunikaci a spolupráci.

ZÁVĚR

V teoretické části práce je provedeno vymezení cloudových služeb, rešerše jejich vývoje, formování, současných typů a účelů jejich využívání. S rostoucím důrazem na bezpečnost ukládaných informací jsou cloudové služby dány do kontextu s aktuální legislativou České republiky. Z důvodu neexistence jasného legislativního rámce pro cloudová úložiště či cloudové technologie, zadala Vláda ČR pokyn k přípravám realizace eGovernmentu, umožňující dosažení dokumentů a služeb veřejné správy v jednom místě. První takovou fungující službou je tzv. Czech Point, kde si lidé mohou nechat za poplatek vyhotovit výpis z rejstříku trestů apod.

Za krok správným směrem lze považovat také vytvoření Národní strategie cloud computingu, která se bude dotýkat právě i eGovernmentu. Cílem strategie je vytvořit národní cloud pro potřeby veřejné správy, státních institucí a jiných státních orgánů, mmj. též orgánů krizového řízení. V budoucnu by to tak mohlo přinést celkové zjednodušení a urychlení práce s daty. V případě krizové situace by například starosta obce mohl v reálném čase vidět jakým způsobem pracují složky IZS, zda mají správné informace o místě zásahu, jaké jsou kapacity zásob či materiálu, které hasičské jednotky zasahují na místě apod. Nemusela by se tak například opakovat situace z Uherského Brodu, kde se ozbrojený muž zabarikádoval v místní restauraci a držel uvnitř rukojmí. Přestože složky a jednotky Policie ČR byly na místě události a obklíčily budovu, místní samospráva se starostou v čele, ani nikdo jiný, nebyl o aktuální situaci vyrozuměn. Starosta města se tak dopustil několika nešťastných odpovědí na otázky od vystrašených místních občanů a zástupců médií, což mu bylo v médiích následně vytknuto Ministrem vnitra Milanem Chovancem. [45]

Na zbývajících stranách teoretické části je vymezen pojem a oblast krizového řízení, krizového managementu a orgánů krizového řízení s funkcemi.

Praktická část je věnována cloudovým úložištím, nejprve popisu úložišť společností Dropbox, Google, Microsoft, iCloud a MEGA. Pro potřebu vyhodnocení nejvhodnějšího řešení je užito komparačních kritérií a matematické metody, přičemž vstupními daty jsou stanovené váhy a hodnoty kritérií jednotlivých služeb. Nejlepšího výsledku na základě váženého průměru vah a hodnot, mezi těmito službami dosáhl Google Drive od společnosti Google. Toto úložiště klade důraz na dostupnost, zabezpečení aj. Těží také z velkého počtu uživatelů i jiných poskytovaných služeb zmíněnou společností.

V poslední části je provedena simulace možného využití funkcí a obsluhy cloudového úložiště Microsoft OneDrive, druhé nejlepší v komparaci, pro pracovníky krizového řízení. Snadná registrace, přístup k úložišti a pomyslná virtuální kancelář umožňuje zpracovat dokumenty v reálném čase bez nutnosti fyzické přítomnosti v jednom místě. Jednoduché vytvoření, nahrání, sdílení dat a přehledná obsluha, může v budoucnu způsobit masové využívání těchto úložišť. Bude-li chystaná legislativa kvalitně zpracována a poskytovatelé cloudových úložišť budou používat kvalitní zabezpečení, nebude nic bránit k rušení malých, na správu náročných datacenter a příliv zákazníků specializovaným poskytovatelům.

Přestože v současné době orgány krizového řízení vlastní technologická centra, případně užívají center na krajské úrovni, jak je tomu v případě Zlínského kraj a pracovníci krizového řízení v rámci tohoto kraje připojují k serverům krizového řízení skrze speciální síť, jenž je spravována Hasičským záchranným sborem Zlínského kraje, existuje do budoucna možnost využití komerčních cloudových úložišť.

V budoucnu je teoreticky možné, že dočkáme využívání smartphonů pro potřeby krizového řízení. Při dopravní nehodě by jím mohla být pořízena fotografie aktuální situace, jež by byla nahrána díky široce rozšířenému datovému připojení, na národní cloudové úložiště a spolu s přesnou polohou a dalšími daty, odeslána pro zpracování na Operační a informační středisko IZS. Díky takovým informacím by bylo schopno např. vyslat nezbytný počet jednotek

SEZNAM POUŽITÉ LITERATURY

[1] KIS, Matej. *Analýza současných cloudových řešení* [online]. *Brno: Vysoké učení technické*, 2015 [cit. 2017-01-30]. Dostupné z DSSpace: https://dspace.vutbr.cz/bitstream/handle/11012/40005/DP%20Matej%20Kis.pdf?sequence=1&isAllowed=y

[2] EARL, Thomas., PUTTINI, Richardo a Mahmood ZAIGHAM. *Cloud computing: Concepts, Technology, & Architecture*. Vyd. 1. New Jersey: Prentice Hall, 2013. 528 s. ISBN 978-0133387520.

[4] MELL, Peter a GRANCE, Timothy. *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology* [online]. 2011 [cit. 2017-01-30]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[4] Cloud Computing: NIST Cloud Computing Program [online]. 2016 [cit. 2017-01-30]. Dostupné z: https://www.nist.gov/programs-projects/cloud-computing

[5] BOURNE, James. I*SO publishes new cloud computing standards and definitions*. In: CloudTech [online]. 2014 [cit. 2017-01-30]. Dostupné z: http://www.cloudcomputing-news.net/news/2014/oct/20/iso-publishes-new-cloud-computing-standards-and-definitions/

[6] FINGAR, Peter. *Dot.cloud: the 21st century business platform built on cloud computing.* Vyd. 1. Tampa, FL: Meghan-Kiffer Press, 2009. 235 s. ISBN 9780929652498.

[7] CLOUDTWEAKS. *Understanding the different roles in a cloud computing setup* [online]. 2012 [cit. 2017-01-30]. Dostupné z: http://cloudtweaks.com/2012/04/understanding-the-different-roles-in-a-cloud-computing-setup/

[8] ROUNTREE, Derrick a Ileana CASTRILLO. *The basics of cloud computing: understanding the fundamentals of cloud computing in theory and practice*. Vyd. 1. Rockland: Syngress Publishing, 2013. 172 s. ISBN 978-0124059320.

[9] Zákon č. 101/2000 Sb. o ochraně osobních údajů. In: *Zákony pro lidi.cz*. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101

[10] Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Zákony pro lidi.cz*. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

[11] Zákon č. 181/2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lidi.cz*. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[12] Nařízení vlády č. 315/2014 Sb. kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. In: *Zákony pro lidi.cz*. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-315

[13] Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích. In: *Zákony pro lidi.cz*. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317

[14] NÁRODNÍ STRATEGIE CLOUD COMPUTINGU. *Akční plán kybernetické bezpečnosti České republiky na období let 2015 až 2020.* Verze 9.1. [online]. 2016 [cit. 1.5.2017]. Dostupné z: http://www.komora.cz/pro-podnikani/legislativa-a-normy/pripominkovani-legislativy/nove-materialy-k-pripominkam/57-16-narodni-strategie-cloud-computingu-t-17-3-2016.aspx

[15] NATO summit in Lisbon. *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. [online]. 2010 [cit. 2017-01-30]. Dostupné z: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

[16] CRISIS MANAGEMENT. *North Atlantic Treaty Organisation* [online]. 2015 [cit. 2017-01-30]. Dostupné z: http://www.nato.int/cps/en/natohq/topics_49192.htm

[17] Terminologický slovník – krizové řízení a plánování obrany státu [online]. 2016[cit. 2017-01-30]. Praha: Ministerstvo vnitra, 216 s. Dostupné z: http://www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx

[19] ANTUŠÁK, Emil. *Krizový management: hrozby – krize – příležitosti*. Praha: Wolters Kluwer Česká republika, 2009. 396 s. ISBN 978-80-7357-488-8.

[20] ANTUŠÁK, Emil a VILÁŠEK, Josef. *Základy teorie krizového managementu*. Praha: Univerzita Karlova v Praze, Nakladatelství Karolinum, 2016. 134 s. ISBN 978-80-246-3443-2.

[21] PETER, Števkov a kol. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy* [online] [cit. 2017-01-30]. Vyd. 2. Praha: Jagello 2000. 2016. 8 s. ISBN 978-80-904850-4-4.

[22] Zákon č. 2/1969 Sb. České národní rady o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky. In: *Zákony pro lidi.cz*. [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://www.zakonyprolidi.cz/cs/1969-2

[23] Zákon č. 240/2000 Zákon o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Zákony pro lidi.cz*. [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240

[24] Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů. In: *Zákony pro lidi.cz*. [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-239

[25] Zákon č. 241/2000 Sb. o hospodářských opatření během krizových stavů. In: *Zákony pro lidi.cz*. [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-241

[26] Ústavní zákon č. 110/1998 Sb. o bezpečnosti České republiky. In: *Zákony pro lidi.cz*. [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://www.zakonyprolidi.cz/cs/1998-110

[27] Zákon č. 128/2000 Sb. o obcích (obecní zřízení). In: *Zákony pro lidi.cz*. [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-128

[28] Zákon č.129/2000 Sb. o krajích (krajské zřízení). In: *Zákony pro lidi.cz*. [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-129

[29] Dropbox Business pricing. [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://www.dropbox.com/business/pricing

[30] DROPBOX. Dropbox Business security. Dropbox whitepaper [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://cfl.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vfllunodj.pdf

[31] Cenové tarify služby G Suite. [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://gsuite.google.com/pricing.html?tab_activeEl=tabset-companies

[32] GOOGLE. Google for Work Security and Compliance Whitepaper [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://static.googleusercontent.com/media/gsuite.google.com/cs//files/google-apps-security-and-compliance-whitepaper.pdf

[33] Microsoft Azure. Cenová kalkulačka [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://azure.microsoft.com/cs-cz/pricing/calculator/

[34] MICROSOFT DOCS. *Introduction to Azure Storage* [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://opbuildstorageprod.blob.core.windows.net/output-pdf-files/en-us/Azure.azure-documents/live/storage.pdf

[35] APPLE. *iOS Security - March 2017* [online]. 2017 [cit. 1.5.2017]. Dostupné z: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[36] The Apple Data Center FAQ [online]. 2016 [cit. 1.5.2017]. Dostupné z: http://www.datacenterknowledge.com/the-apple-data-center-faq/

[37] Ceny tarifů úložiště na iCloudu. [online] 2017 [cit. 1.5.2017]. Dostupné z: https://support.apple.com/cs-cz/HT201238

[38] MEGA. *PRO account* [online] 2017 [cit. 1.5.2017]. Dostupné z: https://mega.nz/pro

[39] MEGA. *Developers - Documentation*. [online] 2017 [cit. 1.5.2017] Dostupné z: https://mega.nz/doc

[40] MICROSOFT. *Tarify/Plány pro Microsoft OneDrive.* [online] 2017 [cit. 1.5.2017] Dostupné z: https://onedrive.live.com/about/cs-CZ/plans/

[41] MICROSOFT. *File Security in Microsoft SharePoint and OneDrive for Business* [online] 2017 [cit. 1.5.2017]. Dostupné z: https://www.microsoft.com/en-us/download/confirmation.aspx?id=53884

[42] APPLE. iStock, *Internet of things – design concept with icons vector* [online] ©2017 [cit. 1.5.2017] Dostupné z: http://media.istockphoto.com/vectors/cloud-computing-internet-of-things-design-concept-with-icons-vector-id582298542

[43] CISCO. *Cloud fig01* [online] ©2017 [cit. 1.5.2017] Dostupné z: http://www.cisco.com/c/dam/en_us/about/ac123/ac147/images/ipj/ipj_12-3/123_cloud_fig01_lg.jpg

[44] MAZIK GLOBAL. *Cloud service models* [online] ©2017 [cit. 1.5.2017] Dostupné z: http://www.mazikglobal.com/blog/wp-content/uploads/2014/06/Cloud-Service-Models.png

[45] LIBINGER, Milan. *Tragédie v Brodě mění pravidla, policie musí být při neštěstí sdílnější.* iDnes.cz [online] ©2016 [cit. 1.5.2017] Dostupné z: http://zlin.idnes.cz/kvuli-brodu-vznikla-pravidla-komunikace-mezi-zachranari-a-radnici-1cu-/zlin-zpravy.aspx?c=A160120_2219766_zlin-zpravy_ppr

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AWS	Amazon Web Service
IoT	Internet věcí
JE	Jaderná elektrárna
MANUH	Metropolitní síť města Uherské Hradiště
NIST	National Institute of Standards and Technology
OS	Operační systém

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: OTÁZKY A ODPOVĚDI ING. LACKY

(Odpovědi Ing. Lacky jsou zabarveny zelenou barvou)

1) Ukládání dat na vlastních serverech? Ano/Ne
ANO -> Jsou umístěny v místě (v úřadu) nebo na jiném místě?
Ne -> Kdo to má na starosti (outsourcing) - externí komerční společnost nebo firma města/kraje?

- *ANO – jsou umístěny v místě úřadu*

2) Kde jsou umístěny servery? Jaká je jejich kapacita? Jaká data jsou primárně na nich uložena?

- *Všechny fyzické i virtuální servery jsou umístěny v TC technologickém centru města v nově vybudované serverovně, která je zabezpečena EZS, kamerovým systémem, náhradním zdrojem elektrické energie, klimatizací a také je pod 24 hodinovým dohledem městské policie. SAN infrastruktura má v současnosti kapacitu 5 TB. Jsou zde uložena všechna data úřadu.*

3) Jak je prováděna záloha dat? (zrcadlení?)

- *SAN infrastruktura je rozdělena do několika částí, kde probíhá pravidelná replikace dat. Dále jsou data v nočních hodinách zálohována na pásky, které se následně uchovávají v jiné lokalitě či objektu než je samotné TC. Také v nočních hodinách probíhá automatická replikace důležitých dat do menšího úložiště prostřednictvím optické metropolitní sítě, opět v jiné lokalitě než je samotné TC.*

4) Kdo má přístup/kdo všechno využívá servery?

- *Data a servery jsou v současnosti využívány jen pro potřeby městského úřadu. Do budoucna se uvažuje o využití pro příspěvkové organizace města a zřizované organizace města.*

5) Jakým způsobem probíhá přístup k datům? Volně či autorizace? Jakým způsobem probíhá autorizace? Jak často se např. mění hesla?

- *Přístup k datům probíhá čistě z vnitřní sítě města. Dochází k ověření samotného počítače a uživatelského účtu oproti AD (Active Directory) na základě příslušných oprávnění. Hesla se pravidelně mění po 90 dnech a mají pevně stanovená pravidla pro jejich tvorbu.*

6) Lze přistupovat k datům jen z firemní sítě (intranetu) či i odněkud jinud?

- *Jen z vnitřní sítě.*

7) Jak probíhá sdílení dat jiným subjektům krizového řízení?

- *Samotná data krizového řízení jsou uložena v technologickém a datovém centru Zlínského kraje. Tyto jsou sdílena a pravidelně aktualizována prostřednictvím optické komunikační infrastruktury Zlínského kraje (KIZK) a optické metropolitní sítě Města Uherské Hradiště (MANUH). Pracovníci krizového řízení se prostřednictvím této infrastruktury přímo připojují do technologického a datového centra Zlínského kraje.*

8) Jak jsou počítače, z nichž je přistupováno k uloženým datům, zabezpečeny?

- *Počítače jsou zapojeny v doméně, automaticky pravidelně aktualizovány, je na nich aktuální antivirový program a jsou chráněny bezpečnostními prvky proti škodlivému kódu, který by se mohl dostat do počítače při brouzdání po internetu nebo emailovou komunikací.*

9) Jak jsou zabezpečeny servery s daty? Jsou na aktuálních, pravidelně aktualizovaných OS?

- *Na serverech je pravidelně aktualizovaný OS, nastavený a nakonfigurovaný firewall a také jsou tyto servery chráněny perimetrem tvořeným bezpečnostími prvky Router-Firewall a HA Firewall Cisco Meraki v HA clustru. Dále je síťový provoz monitorován sondou v síti GreyCortex Mendel a bezpečnostním prvkem SIEM – Security Information Event Management.*

10) Došlo v minulosti k odcizení resp. dostala se data v minulosti do nepovolaných rukou?

- *NE*

11) Jaká opatření byla následně přijata k minimalizaci opakování takové situace?

- *Zabezpečení dat se provádí kontinuálně na základě vznikajících hrozeb a rizik, dle nově vznikajících požadavků legislativy jako je nový zákon o kybernetické bezpečnosti a na základě vývoje a rozvoje bezpečnostních prvků a technologií. Do budoucna se uvažuje o pořízení bezpečnostního software DLP – Data Lost Prevention. Tento podrobně monitoruje, co se s konkrétními daty průběžně děje.*

12) Jsou mezi daty i informace důvěrného charakteru, osobní údaje aj.?

- *ANO*

13) Jsou pro vaše cloudové úložiště stanoveny legislativně nějaké parametry? Případně kterými vyhláškami/nařízeními?

- *Vše se řídí dle technických norem ČSN EN 50600-1 – Informační technologie – Zařízení a infrastruktury datových center.*

14) Kolik měsíčně stojí vaše cloudové řešení?

- *Město vybudovalo z dotačního titulu své vlastní technologické centrum s vlastním úložištěm. V současné době jsou náklady spojené pouze na zajištění jeho provozu.*

15) Podléhají ukládaná data některému stupni utajení? (Vyhrazené/důvěrné/tajné/přísně tajné)

- *nepodléhají, práce s osobními údaji se řídí dle zákona o ochraně osobních údajů*