Možnosti využití cloudových technologií v krizovém řízení

Štěpán Janda

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:	**Štěpán Janda**
Osobní číslo:	L14338
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

Téma práce: **Možnosti 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 ve zvolené oblasti krizového 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, Thomas., Richardo PUTTINI a Zaigham. MAHMOOD. Cloud computing: concepts, technology, & architecture. Vyd. 1. Prentice Hall, 2013. 528 s. ISBN 9780133387520.

[2] ROUNTREE, Derrick. a Ileana. CASTRILLO. The basics of cloud computing: understanding the fundamentals of cloud computing in theory and practice. Vyd. 1. Syngress, 2013. 172 s. ISBN 978-0-12-405932-0.

[3] ANTUŠÁK, Emil a Josef VILÁŠEK. Základy teorie krizového managementu. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2016. 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 20. února 2017

doc. RNDr. Jiří Dostál, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

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 15.5.2017

.....
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

Práce je koncipována jako jednoduchý návod na implementaci možných cloudových řešení pro složky Integrovaného záchranného systému. Teoretická část této práce je zaměřena na vytyčení pojmů faktů a analýzu informačních zdrojů světa. Praktická část obsahuje faktickou implementaci do Integrovaného záchranného systému a jeho složek a návrh této implementace

Klíčová slova: cloudové služby, Integrovaný záchranný systém, implementace

ABSTRACT

Thesis is conceived as a simple instructions on implementation of possible cloud computing for the Integrated rescue systém. Theoretical part of my thesis focused on definitions of facts and analysis of the information sources of the world. Practical part includes factual implementation of cloud into Integrated rescue systém and its parts and also a proposal of this implementation

Keywords:cloud services , Integrated rescue systém, implementation

Poděkování

Tímto bych chtěl poděkovat hlavně a především svojí přítelkyni, která mne velmi podporovala v průběhu celého studia a také mi moc pomáhala se všemi různými přípravami nejen na zkoušky, ale také na tuto práci. Dále bych chtěl taktéž poděkovat vedoucímu mojí bakalářské práce, panu Ing. Petru Svobodovi, který se mnou měl velkou trpělivost. Taktéž moje poděkování patří spolužákům, kteří mi také velmi pomohli se studiem a přípravou této práce.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do STAG jsou totožné

OBSAH

ÚVOD

V dnešní době čím dál častějších přírodních katastrof, teroristických útoků, častějších dopravních nehod, jelikož je také více lidí, tím pádem více aut, je velmi potřeba včasná reakce nejen obyvatelstva jako takového, ale také těch, kteří lidem nejvíce pomáhají. Integrovaného záchranného systému.

Informační technologie však nám lidem slouží a proto je třeba je využívat. Využívat můžeme různé informačně technologické pomůcky a nástroje. Poslední dobou je čím dál tím častější využívání cloud computingu a cloudu jako takového. Je to jednoduché, nabídka služeb je velice široká a člověk si tak může vybrat z široké škály produktů, které právě jemu nebo snad dané firmě bude vyhovovat. Cílem této bakalářské práce je právě implementace a využití cloudu pro krizové řízení. Výsledkem praktické části je následně konkrétní implementace pro Integrovaný záchranný systém.

Závěr mojí práce vyhodnocuje jak část teoretickou, tak část praktickou. Kde zhodnocuji reálné využití implementace cloud computingu v Integrovaném záchranném systému.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ DEFINICE

1.1 Cloud

Co to vlastně Cloud neboli Cloud computing je ? Je to v podstatě nový způsob pro využití zdrojů v IT oblasti, který vychází ze sdílení mezi aplikacemi a tím pádem odpadá přímá vazba na fyzické komponenty. Nejedná se tedy o fyzickou věc. Cloud je síť serverů, z nichž každý má jinou funkci. Některé servery používají výpočetní výkon pro běh aplikací, jiné „poskytují služby.“ Další servery v síti jsou zodpovědné za ukládání dat. Například, když pořídíte obrázek na vašem smartphonu, uloží se do interní paměti telefonu. Nicméně když budete nahrávat fotografie na Instagram či na domácí NAS server, budete je tím nahrávat do Cloudu. [1]

1.2 Typy a způsoby cloudu

Cloudu je mnoho typů. Zde jsou nejpoužívanější typy a jejich využití, nejsou však pořád ještě ustálené, jelikož se tato služba stále dále a více vyvíjí. Dovolím si použít terminologii, kterou využívají firmy, které jsou v tomto odvětví nejvyužívanější a jejich názvy pro dané využití se v podstatě neliší. Je to vlastně takový jednoduchý slovníček, který pro naši práci bude bohatě stačit.

1.2.1 Privátní cloud

Prostředí pro cloud computing, které si soukromé organizace vytvářejí pro vlastní interní využití. Prostředky, které daná organizace vlastní či přímo kontroluje, jsou konsolidovány a seskupeny jako federované prostředky. Ty jsou pak zpětně formou služby poskytovány uživatelům v rámci organizace.

1.2.2 Veřejný cloud

Cloud computing, který poskytovatel nabízí z vlastních sdílených prostředků jako službu zákazníkům z řad veřejnosti. Podobá se outsourcingu, ale musí splňovat všechny charakteristiky cloud computingu: schopnost poskytovat prostředky na vyžádání, elasticky a samoobslužně, síťový přístup a také měřitelnost spotřebované služby v rámci sdíleného fondu prostředků. Záleží jen na rozhodnutí daného poskytovatele, které prostředky zpřístupní

kterému zákazníkovi, a proto může být služba zabezpečená i nezabezpečená a prostředky mohou, ale nemusí být federovány s jinými (privátními) prostředky.

1.2.3 Komunitní cloud

Prostředí pro cloud computing, které vzniká sdružením prostředků vlastněných určitou skupinou členů (tzv. komunitou) a poskytuje tyto prostředky zpět formou služby stejné skupině členů.

1.2.4 Hybridní cloud

Prostředí pro cloud computing, které je vytvořeno federací a sdružením prostředků z privátního cloudu určité organizace s prostředky od jiného poskytovatele. Vzhledem k tomu, že před poskytnutím výpočetní služby organizaci dochází k federování a sdružení prostředků, vystupuje hybridní cloud vůči uživatelům, vlastníkům aplikací a organizačním jednotkám přesně stejně jako privátní cloud.

1.2.5 Virtuální privátní cloud

Nestandardní termín používaný některými dodavateli, avšak nikoli normalizačními institucemi, jako je NIST (National Institute of Standards and Technology, Národní normalizační a technologický institut v USA). Označuje hybridní cloud, jenž vystupuje vůči uživatelům, vlastníkům aplikací a organizačním jednotkám stejně jako privátní cloud. Základní podmínkou propojení a sdružení prostředků i jejich zpětné distribuce je federace, která právě umožňuje, že se prostředek uživatelům, vlastníkům aplikací a organizačním jednotkám jeví jako privátní cloud.

1.2.6 Infrastruktura cloudu

Infrastruktura nezbytná k poskytování (obvykle transparentnímu) služeb cloudu uživatelům. Jejími součástmi jsou funkce pro virtualizaci a federaci prostředků, standardizaci a automatizaci provozních operací, přístup uživatelů k výpočetní službě a možnost zvolit si kvalitu i kvantitu spotřebované služby, a v neposlední řadě způsob měření a vyúčtování poskytnutých služeb.

1.2.7 Služby cloudu

1. Infrastrukturní služby poskytované v prostředí pro cloud computing, které zajišťují splnění požadavků ustanovených v dohodě o úrovni poskytovaných služeb (např. výkon, dostupnost, uchování dat, zabezpečení, kapacita). 2. Služby, které umožňují funkčnost prostředí pro cloud computing (např. speciální účtovací software, který zajišťuje, aby v cloudových výpočetních prostředích různé velikosti a s různou úrovní poskytovaných služeb bylo možné vyúčtovat poskytnuté služby). 3. Konzultační služby, které pomáhají organizacím při transformaci a přechodu na cloud computing. 4. Aplikační služby poskytované v prostředí pro cloud computing, které nabízejí vývojářům aplikací standardizované aplikační funkce (např. rutiny pro ověřování, vyhledávání, zavádění politik nebo procesy podle metodiky ITIL)

1.2.8 Cloudové úložiště

Úložná kapacita a/nebo služby úložiště (výkon, dostupnost, uchování a vyhledatelnost dat, zabezpečení apod.), které jsou poskytovány jako služba splňující charakteristiky cloud computingu (sdružená, elastická a měřitelná služba na vyžádání se síťovým přístupem). Může, ale nemusí nabízet možnost federace se stávajícími prostředky úložiště.

1.2.9 Multi-tenancy

Výpočetní prostředí, které je sdíleno více skupinami či uživateli (tzv. nájemníky), avšak zajišťuje jejich vzájemné oddělení a izolaci, aby si uživatelé nebyli vědomi ostatních nájemníků a neměli přístup k jejich informacím a prostředkům.

1.2.10 Samospráva nájemníků

Možnost každého uživatele v prostředí multi-tenancy přímo měnit výpočetní charakteristiky a úroveň poskytovaných služeb ve svém vlastním prostředí (v některých případech jsou omezeni předem stanoveným rozmezím), a to bez zásahu centrálního správce IT. Taková přímá samospráva však neznamená neomezenou kontrolu – omezení mohou spočívat například v cenových podmínkách nebo v opatřeních typu schvalovací kroky či maximální a minimální přípustné nastavení úrovně poskytovaných služeb.

1.2.11 Federace

Propojení několika samostatných prostředků takovým způsobem, že vystupují jako jediný větší prostředek nebo je s nimi možné interagovat jako s jediným prostředkem. Takovýto větší prostředek umožňuje vytvořit a distribuovat uživatelům neboli nájemníkům jako službu balíčky, které se navzájem liší kvantitou nebo kvalitou obsaženého prostředku.

1.2.12 Software jako služba (SaaS)

Softwarová aplikace, kterou lze použít pouze prostřednictvím přístupu k danému softwaru a jeho předdefinovanému výpočetnímu prostředí ze sítě, a nikoli stažením softwaru a jeho instalací do místního počítače či výpočetního prostředí. Každý uživatel je nájemníkem ve sdíleném prostředí poskytovatele, které má charakteristiku multi-tenancy. Uživatel však obvykle nemívá mnoho možností volit poskytované služby a jejich úroveň.

1.2.13 Platforma jako služba (PaaS)

Sdílené výpočetní prostředí jiného poskytovatele, ke kterému může uživatel získat vzdálený přístup za účelem vývoje a spouštění softwarové aplikace (nebo úprav softwaru nabízeného jako služba). Každý uživatel je nájemníkem ve sdíleném prostředí poskytovatele, které má charakteristiku multi-tenancy. Přímo z definice plyne, že každý uživatel může vytvářet libovolné funkce a aplikační služby. Nebývá však obvyklé, aby samotné výpočetní prostředí nabízelo uživateli významné možnosti volit úroveň poskytovaných infrastrukturních služeb.

1.2.14 Infrastruktura jako služba (IaaS)

Úplná IT infrastruktura, která je formou služby nabízena uživatelům, vlastníkům aplikací, organizačním jednotkám apod. Každý z uživatelů neboli nájemníků má přístup k části konsolidovaného fondu federovaných prostředků, z nichž si může podle potřeby kdykoli a jakkoli vytvořit vlastní výpočetní infrastrukturu. Konsolidovaný fond prostředků je navržen tak, aby zajišťoval sdílené výpočetní prostředí s charakteristikou multi-tenancy a aby každý nájemník mohl rozhodovat o typu a vlastnostech požadované infrastrukturní služby. Takovéto sdílené prostředí typu multi-tenancy může zcela vlastnit a řídit daná organizace (tj. private cloud), nebo může jít o propojení a federaci firemních prostředků s doplňujícími

externími prostředky (tj. hybridní cloud), anebo může být zcela poskytováno jinou organizací (tj. veřejný cloud).

1.2.15 Samospráva na vyžádání

Výpočetní prostředí, ke kterému přistupují a které využívají uživatelé podle potřeby, a přitom není poskytováno ani řízeno centralizovanou správou infrastruktury. Samospráva na vyžádání však neznamená neomezenou kontrolu – omezení mohou spočívat například v cenových podmínkách nebo v opatřeních typu schvalovací kroky či maximální a minimální přípustné nastavení úrovně poskytovaných služeb.

1.2.16 Rychlá elasticita

Schopnost rychle a snadno vytvářet, zvyšovat, přidávat, snižovat nebo eliminovat využití prostředků. Požadované prostředky pocházejí ze sdíleného fondu prostředků, a jakmile přestanou být potřebné, jsou do fondu prostředků vráceny.

1.2.17 Měřitelná služba

Umožňuje účtování, tj. sledování, o kvantitě a kvalitě využitých („spotřebovaných“) výpočetních prostředků a služeb. Kvantitou prostředků rozumíme mimo jiné výpočetní výkon serverů, přenosovou kapacitu sítě, kapacitu úložiště apod. Kvalita služeb zahrnuje mimo jiné různé stupně neboli úrovně výkonu, dostupnosti, ochrany, uchování dat, rychlosti vyhledávání nebo zabezpečení. [3]

2 KRIZOVÉ ŘÍZENÍ

Krizové řízení je souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešením, nebo ochranou kritické infrastruktury (zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů). [2]

V České republice jsou cíle pro krizové řízení státu ukotveny v ústavním zákoně. Je to zákon č. 110/1998 Sb., o bezpečnosti České republiky. V článku 1 se zde píše – „Krizové řízení je souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešením, nebo ochranou kritické infrastruktury (zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů).“ A poté v článku 3. odstavec 2 – „Krizové řízení je souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešením, nebo ochranou kritické infrastruktury (zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů).“

2.1 Orgány krizového řízení

Orgány, které ve prospěch svého zřizovatele zabezpečují analýzu a vyhodnocení možných ohrožení jeho bezpečnosti, plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravnými opatřeními a řešením krizových situací.[4] Definuje je zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů ve znění pozdějších předpisů. Jde sice o orgány:

- Ministerstva
- Vláda České republiky
- Česká národní banka
- Orgány krajů, obcí

- Určené orgány s územní působností
- Bezpečnostní rady
- Ostatní ústřední správní úřady

2.2 Legislativa

Klíčové a ústavní zákony, které se zabývají krizovým řízením a krizovými situacemi:

- Zákon č. 12/2002 Sb., o státní pomoci při obnově území postiženého živelnou nebo jinou pohromou, ve znění pozdějších předpisů a novelizací.
- Zákon č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon), ve znění pozdějších předpisů a novelizací.
- Zákon č. 59/2006 Sb., o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými přípravky, ve znění pozdějších předpisů a novelizací.
- Zákon č. 133/1985 Sb., o požární ochraně, ve znění pozdějších předpisů a novelizací.
- Zákon č. 222/1999 Sb., o zajišťování obrany ČR, ve znění pozdějších předpisů a novelizací.
- Zákon č. 238/2000 Sb., o Hasičském záchranném sboru ČR, ve znění pozdějších předpisů a novelizací.
- Zákon č. 239 Sb., o integrovaném záchranném systému, ve znění pozdějších předpisů a novelizací.
- Zákon 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů a novelizací.
- Zákon 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, ve znění pozdějších předpisů a novelizací.
- Zákon 254/2001 Sb., o vodách (vodní zákon), ve znění pozdějších předpisů a novelizací.

- Zákon 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon), ve znění pozdějších předpisů a novelizací.
- Zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů a novelizací.
- Zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů a novelizací.

3 VÝHODY CLOUDU

V dnešním světě je vlastně přirozené přistupovat k informacím odkudkoliv a kdykoliv chceme. Cloud je proto naprosto ideální mobilní řešení pro práci. Pracovníci samozřejmě pořád musí být na nějakém určitém místě pro jejich danou práci, neznamená to nutně však, že musejí sedět u stolu. Proto je to výhodné pro povolání v terénu, kde je mobilnost, neboli pohyb pro pracovníka nutností. Při využití cloudu však s sebou nemusí brát nějaký obrovský stroj, stačí mu pouze jen jakékoliv mobilní zařízení, které má přístup na internet. Toho si začalo všímat také čím dál více firem a společností. Mobilita pro zaměstnance znamená snadný kontakt s ostatními zaměstnanci nebo samozřejmě se zákazníky. Chytré telefony nebo tablety má v dnešní době skoro každý a vlastně každý tyto cloudové služby v podstatě využíváme již na denním pořádku, možná aniž si to uvědomujeme. Office 365, Google docs nebo dokonce Facebook či Twitter jsou také cloudovými technologiemi. Prvním krokem ke cloudu v jakékoliv firmě, je však virtualizace prostředí.

3.1 Virtualizace

Virtualizace není jen a pouze umožnění přístupu k data centru všem ve firmě, jak zařízením, tak uživatelům. Virtualizace je také úprava sítě a její architektury pro větší mobilitu jejích uživatelů. Umožňuje v podstatě oddělení systémů, hardwaru a také i aplikací od zařízení uživatelů a také velmi zlehčuje udělování práv a přístupů všem různým uživatelům a skupinám uživatelů. Firmy si tím v podstatě ochrání svá duševní vlastnictví a přitom uživatelé dostanou co chtějí. Svobodu – mobilitu.

3.2 Infrastruktura

S tím souvisí také malé nebo nízké náklady na infrastrukturu. Firma vlastně neřeší nový nákup serverů nebo hardware obecně, protože to za ní řeší poskytovatel. Nemusí se tedy obnovovat každých 3-5 let nový hardware, jako tomu tak bývá, protože většinou skončí podpora u daného zařízení a řešit opravu na vlastní náklady je mnohdy velmi finančně náročné. Firma takto platí pouze za vedení cloudového řešení. Čímž také odpadá údržba datových center nebo sálů.

4 BEZPEČNOST CLOUDU

Pokud budeme uvažovat, že chce naše firma nebo podnik přejít nebo si pořídit služby cloudu, musíme se nutné také zabývat bezpečností této služby. Ať už budeme spoléhat na cloud třetí strany nebo budeme mít svůj, bezpečnost je vždy až na prvním místě. Obzvláště, pokud jde o citlivá data jednotlivých uživatelů. Jednoznačně je nejdůležitější nejprve zvážit pro a proti, která má cloud oproti obyčejnému IT prostředí. Je nutné vzít v potaz vliv ohrožení. Z business hlediska vznikne vlastně riziko až tehdy, pokud jsou v ohrožení určitá slabá místa, která právě mohou způsobit škodu.

Ke stanovení rizika pro IT či obchod je nejprve třeba identifikovat ohrožení ve smyslu příležitostí a vlivů příčin. Co se může v modelu IT služeb cloud computing v zásadě či konkrétně přihodit? Ve druhém kroku je třeba zjistit, zda existují slabá místa – například nekvalitní či nedokonalé ověřování identity před přístupem ke zdrojům ICT a datům nebo nedostatečná opatření datové bezpečnosti. Integrace bezpečnostních postupů je věcí poskytovatele služeb. Slabá místa nelze zjistit, aniž by byla posouzena technika a její použití, a bezpečnostní riziko může být vyhodnoceno, jen když uživatel vyčíslí potenciální škodu a její dopad na obchod. [5]

Spoustu firem, ať už jde o velké nebo středně malé, konají však své kroky směrem ke cloudu bez jakékoliv profesionality. Mají jasné dané postupy a také odpovědnosti, stejně však dojde při denní praxi k nějakému trvalému porušení předpisů této firmy. V tomto případě by přinesl přesun IT do cloudu jasné bezpečnostní výhody, protože pro poskytovatele na profesionální úrovni by bylo zajištění IT bezpečnosti hlavním cílem jeho činnosti. Podle svých zkušeností by mohl totiž pomoct vyřešit bezpečnost lepší a výkonnější infrastrukturou, kterou disponuje. Nemluvě o kvalitě pracovníků. Tím pádem lépe chrání své výpočetní středisko a datové sály před vnějšími útoky a mohou poskytovat služby bez jakýchkoliv výpadků na jejich straně.

4.1 Srovnání potencionálních rizik cloudu a klasických formách ICT

Zde si nyní vysvětlím rozdíly v rámci bezpečnosti a potencionálního rizika mezi normálními ICT službami a cloudovými službami. Různá bezpečnostní opatření u cloudu na rozdíl od normálních ICT služeb odpadá, avšak samozřejmě musí se na druhou stranu brát větší pozornost na odlišná nebezpečí.

4.1.1 Výpadky kvůli přetížení

V běžném serverovém prostředí může docházet ke ztrátám výkonu nebo výpadkům kvůli neočekávaným zátěžovým či výkonovým špičkám. Podstatnou výhodou cloud computingu je, že lze zdroje dynamicky a pružně přizpůsobovat, a že tak nedochází k přetížení.

4.1.2 Utajení

Používá-li firma ve vlastním datovem centru vlastní systémy, může dbát na ochranu dat sám. K datům nemá přístup žádný poskytovatel. V cloudu jej poskytovatel má, avšak lze jej šifrováním dat spolehlivě vyloučit.

4.1.3 Ztráta nebo krádež hardware

V klasickém prostředí mimo neoprávněných přístupů k podnikovým datům existuje jiný, velmi reálný zdroj ztrát podnikového duchovního vlastnictví: zaměstnanci nosí koncové přístroje či USB s důvěrnými či kritickými daty sebou. Jsou-li ztraceny či ukradeny a dostanou se do nepovolaných rukou, může nastat enormní škoda. Kolik uživatelů má data ve svých systémech skutečně zašifrována či zajištěna? Cloud computing může toto nebezpečí ztráty dat odstranit centralizovaným uložením dat a používáním tenkých klientů.

4.1.4 Problémy s dostupností kvůli výpadkům serverů

Dojde-li v klasickém prostředí IT k výpadkům hardwaru, dochází, pokud není systém redundantně uspořádán, k velkým škodám. Z hlediska nákladů je náprava poměrně obtížná. Cloud computing charakterizuje vysoká dostupnost díky nejrůznějším opatřením, které si lze díky přizpůsobivosti dovolit. Výpadky jsou „odchytávány“.

4.1.5 Problémy se shodou v důsledku odděleného uložení dat

V cloudu není na rozdíl od běžných prostředí IT známo kdy se data a aplikace nacházejí na jakém serveru. Mnoho poskytovatelů navíc najímá subdodavatele. Právní problémy při tom mohou nastávat zvláště při zpracování osobních dat (viz též kapitolu 5 „Právní požadavky a další aspekty shody“). Existují však též poskytovatelé, kteří mohou uložení dat smluvně omezit například na právní oblast České republiky nebo Evropské unie.

4.1.6 Zastaralý software

Jestliže firma své IT prostředí provozuje ve vlastní režii, stará se o svůj software sám. V každém softwaru existují chyby a vznikají tak mezery v bezpečnosti, které lze, jakmile jsou známy, odstranit aktualizacemi. Tato potřebná péče o systém je složitá, může narušovat pracovní postupy a vést mimoto k dalším chybám. U cloud computingu za to odpovídá poskytovatel: nahrává centrálně aktualizace a tím zajišťuje stabilitu a spolehlivost systému.

4.1.7 Otázky záruk

Ke sporným otázkám může docházet i u cloud computingu. Příkladně porušením smluv o úrovních služeb v důsledku technických problémů vsíti či při provozu IT. Viníka lze často jen těžko zjistit. Jinak tomu je, pokud je poskytovatel cloudu odpovědný za síť a odpovídá za kompletní (end-to-end) řešení.

4.1.8 Virová hrozba

V běžných prostředích IT se zpravidla používají antivirové programy. V důsledku malého výpočetního výkonu a často nedostatečné aktuálností virových skenerů je rozpoznání nového škodlivého softwaru obtížné. U cloud computingu lze centralizovat i tento úkol a tím jej provádět efektivněji a aktuálněji. Všichni zákazníci poskytovatele se automaticky těší stejné ochraně.

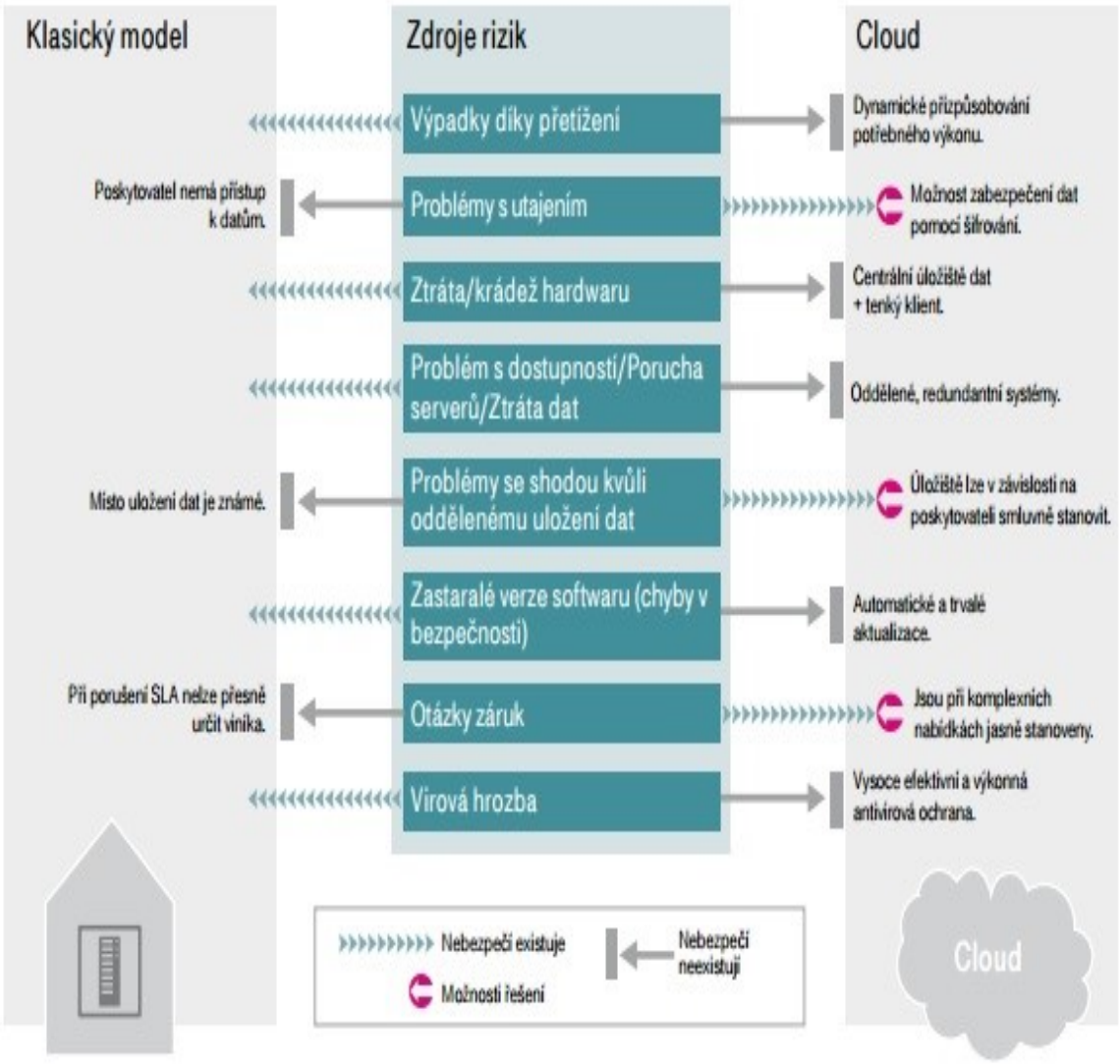
4.1.9 Útoky hackerů

Teoreticky napadnutelné jsou všechny systémy, aplikace a data zjakéhokoli prostředí. V klasických IT prostředích odpovídá za ochranu sám uživatel amusí plánovat, realizovat, kontrolovat a aktualizovat opatření jako Firewall, Intrusion Detector, skenování virů či izolaceserveru od veřejné sítě. V cloudu přebírá tyto úkoly poskytovatel.

4.1.10 Změna poskytovatele

Kvůli přechodu na cloud computing nebo při změně poskytovatele je třeba přemístit celé aplikační prostředí. Znamená migraci velkého množství dat a celých pracovních prostředí. Aby zaměstnanci mohli dále pracovat bez přerušení, musí být po přechodné období případně souběžně k dispozici staré a nové prostředí a soubory dat musejí být správně migrovány.

K zajištění dostupnosti a bezpodmínečnémuvyloučení ztráty dat je zapotřebí zkušenosti. [6]



1Klasický model proti cloudu

5 VYUŽITÍ CLOUDU V KRIZOVÉM ŘÍZENÍ

Nejjednodušší si bude ukázat na příkladu. Tento systém se již využívá hojně ve velkých, respektive krajských městech. Jeho řešení často zahrnuje také službu GIS neboli geografický informační systém. Ten je využíván v mnoha oblastech řízení rizik a především integrovanými záchrannými složkami. Například v Praze byl systém Informačního systému krizového řízení spuštěn v roce 2008. Systém byl v podstatě vytvořen na míru a slouží pro podporu krizového řízení a při krizových a mimořádných situacích. Neřeší však jen krizové situace, ale také běžné situace jako jsou obnovy dodávek pitné vody nebo například řešení dopravní situace.

Hlavními součástmi jsou:

- Katalogy - evidence všech potřebných údajů o subjektech, objektech a zdrojích využitelných pro řešení vzniklých událostí na území HMP.
- Analýza rizik – podpora identifikace zdrojů rizik na území HMP a jejich dopadů, vytipování nejvážnějších rizik k přípravě řešení.
- Plánování – podpora zpracování plánů řešení vytipovaných rizik včetně stanovení zodpovědností a např. zajištění komunikace.
- Řízení a řešení – podpora řízení řešení události na základě připravených podkladů.
- Sběr dat – nástroj pro sběr dat o subjektech zařazených do krizového plánu a aktualizace dat o subjektech (organizacích), jež nejsou uživateli systému.
- Analýza škod – evidence škod, které vznikly jednotlivým subjektům při řešené události.
- Dokumentace – podpora práce s dokumenty (tiskové sestavy, ukládání, verzování dokumentů apod.).
- GIS – vizualizace dat uložených v systému, společný obraz situace, analytické nástroje. [7]

Obrázek 2Části systému

II. PRAKTICKÁ ČÁST

6 INTEGROVANÝ ZÁCHRANNÝ SYSTÉM

Integrovaný záchranný systém (IZS) můžeme definovat jako systém vazeb nebo spolupráci a koordinaci záchranných a bezpečnostních složek fyzických a právnických osob při společném provádění záchranných a likvidačních prací a přípravě na mimořádné události. Je to proto, aby bylo využito každé součásti tohoto systému a všech jeho součástí.

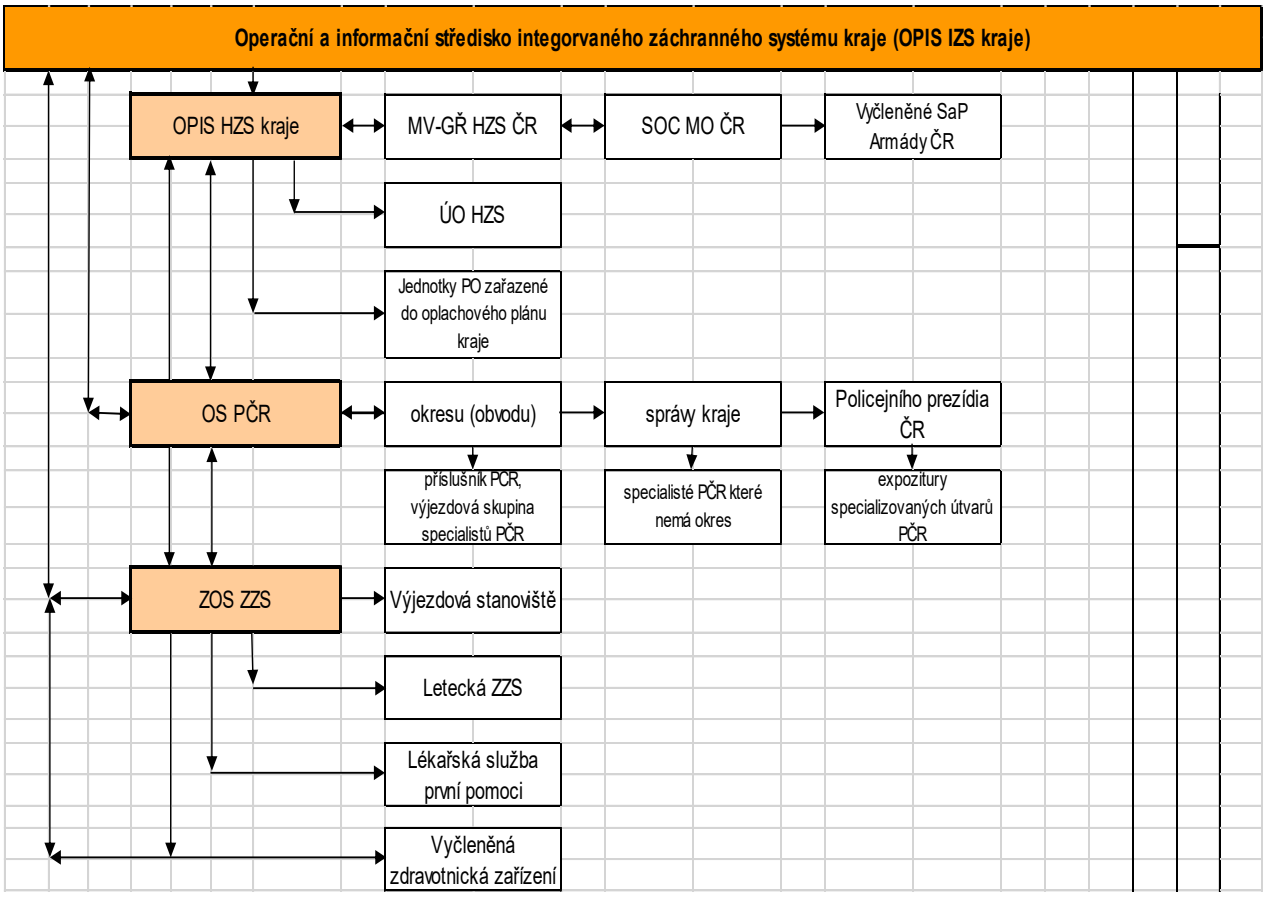
6.1 Struktura IZS

Struktura IZS by se dala rozdělit do dvou menších celků. Jsou jimi základní složky a ostatní složky IZS.

Základní složky jsou

1) Hasičský záchranný sbor
2) Jednotky požární ochrany pokrývající kraje jednotkami požární ochrany
3) Policie České republiky

Ostatní složky jsou vyčleněné síly a prostředky ozbrojených sil, zařízení civilní ochrany, obecní policie, orgány ochrany veřejného zdraví a jiné.



Obrázek 3Schéma IZS [9]

Hlavní složkou IZS je především Hasičský záchranný sbor. Je hlavním koordinátorem akcí a zásahů, při nichž zasahují více složek IZS. Velitelem zásahu bývá zpravidla velící příslušník hasičského záchranného sboru. Ten řídí součinnost složek a koordinuje zásah nebo danou akci. Nadřazeným mu je pak Operační a informační středisko IZS, kterým je právě také středisko HZS České republiky. To nasazuje a povolává náležité potřebné síly složek IZS v daných lokalitách, dle potřeby. Strategická úroveň integrovaného záchranného systému je poté koordinována krizovými orgány krajů a MV České republiky. Proto se v mojí práci zaměřím především na HZS a možnosti využití cloudu v něm.

7 ANALÝZA SOUČASNÉHO STAVU V IZS

Integrovaný záchranný systém je vlastně více složek sloučených vazbami na sebe v jeden celek-systém. Tento systém má mezi sebou svoje vazby, návaznosti, pravidla. Součástí tohoto celku jsou záchranné a bezpečnostní složky, orgány státní správy a samosprávy a také fyzické a právnické osoby, kteří všichni mohou vypomáhat s řešením dané krizové situace nebo mimořádné události. Jednotlivé složky jsou spolu většinou propojeny vysílačkami. Co ale dělat, když se stane MU velkých rozměrů nebo je potřeba zadat více úkolů v jeden okamžik mnoha jednotkám najednou nebo je jen potřeba popsat nějakou situaci velmi důsledně a co víc řekne než tisíc slov najednou, je samozřejmě obrázek. Určitě je v takových situacích, si myslím, co zlepšovat. Právě a nejen tento problém by se dal vyřešit tímto návrhem. Samozřejmě to bude chtít školení a řádné cvičení, protože složky IZS mají již nějaký svůj zaběhlý systém, který by museli měnit. Myslím si však, že v době dnešních technologií je krok kupředu tímto směrem ten správný.

8 IMPLEMENTACE CLOUDOVÝCH TECHNOLOGIÍ HZS

Implementaci cloudu lze zavést pomocí v podstatě jakýchkoliv firem, které tento způsob sdílení dat nabízí, respektive zprostředkovávají. Z mého hlediska by bylo však úplně nejjednodušší využít ten způsob, který využívá jednoduché webové rozhraní, které je v dnešní době dostupné prakticky z jakéhokoliv zařízení. Tento způsob se nazývá také Rich internet application neboli RIA. Je to vlastně jednoduché využití webového klienta, který má v sobě již řadu konkrétních a dostupných technologií. Proto je velmi důležité si zvolit tu správnou.

Jelikož je však těchto možností mnoho, je jednoduché si zvolit.

Další volba potom padá na hardware, na kterém budou tyto technologie zobrazovány. Hlavní nutností pro volbu hardwaru je samozřejmě dostupnost mobilních dat. Mobilní data jsou potřebná pro přístup ke cloudu odkudkoliv z terénu. V tom tkví právě největší vyhoda cloudu. Přístup k aktuálním informacím, odkudkoliv. V dnešní době však s tímto rozhodně problém nebude, jelikož pokrytí operátorů českých sítí je v podstatě stoprocentní. Zvolil bych v tomto případě v dnešní době velmi rozšířené a snadno dostupné tablety. Jejich ovládání je velmi intuitivní a snadné a zvládne to opravdu každý. Proto by bylo implementování právě pro ně vhodné. Další výhodou je, že nejen tablety se dají použít pro tento účel, ale také v podstatě jakékoliv mobilní zařízení s přístupem k mobilním datům. Dalo by se pak taktéž ještě dále rozšířit tuto implementaci ne jen pro každou posádku, ale také pro každého člena zásahu. Každý by mohl mít potom svoje zařízení, na které by mu mohli chodit data o zásahu přímo od svých velitelů. Kam se mají například přesunout, co se kde v které části zásahu změnilo, atp. Ale to už by bylo si myslím na další, jiné téma, které lze však samozřejmě dále rozvinout.

8.1 Možnosti

Možností implementace cloudu je spoustu. Hasičský záchranný sbor v dnešní době využívá systém, který je sice efektivní, ale pouze do doby, než posádka vyjede. Čili pouze v rámci budovy dané jednotky. Cloud lze využít právě a především za „běhu“.

Jednotky by mohly dostávat tímto způsobem více informací například o místě zásahu, o počtu osob na místě zásahu, o rozsahu požáru, jestli potřebují další posádku, a mnoho dalšího a to pouze na dosah „jednoho kliku“.

V podstatě jde o to, že jednotky v dnešní době vidí pouze to kam jedou a co je tam může čekat a jak na to mají reagovat. Pokud však náhle dojde k nějaké změně, musí reagovat až na místě po obhlédnutí situace. Po implementaci cloudu by však mohli reagovat již za jízdy k danému místu. To by znamenalo rychlejší reakce na zásah nebo lepší koordinaci zásahů pro velitele a pro koordinátory. Mohly by přímo v cloudu v reálném čase rozmisťovat nebo přemisťovat jednotky dle potřeby. Možností je opravdu mnoho, budu se jim více věnovat v následujících kapitolách.

8.1.1 Návrhy možností

Možností je, jak jsem již zmínil, mnoho. Moje návrhy na možnosti nejsou samozřejmě konečné, ale to je právě na tom to nejlépe využitelné. Možnosti by si totiž takto mohli přidávat jednotky sami, jelikož je samozřejmě každá situace naprosto unikátní. Tím pádem by se dali přizpůsobit opravdu přesně dané situaci.

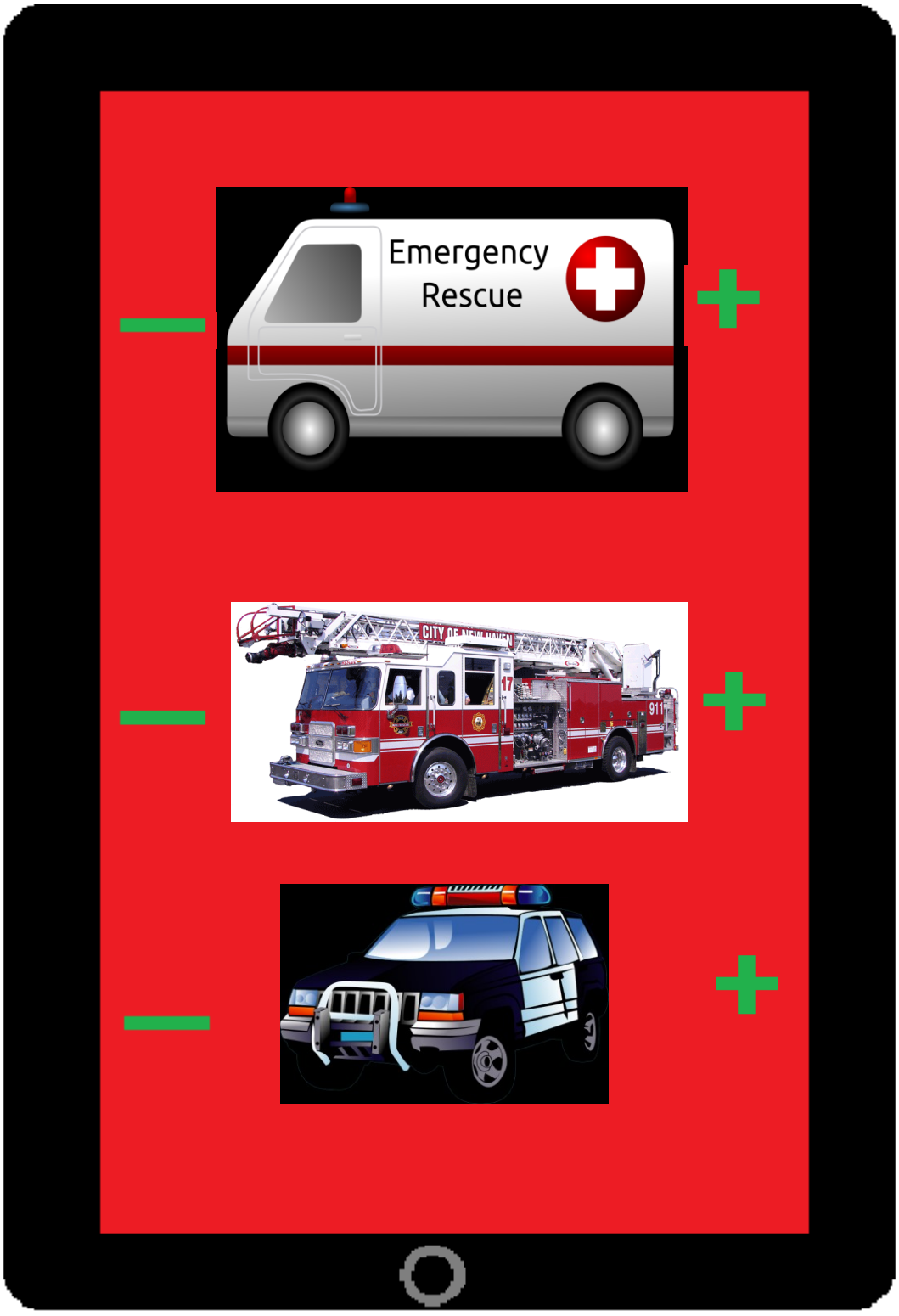
1) Typ objektu/zásahu
2) Počet osob v objektu/při zásahu
3) Nebezpečné materiály v objektu
4) Rozložení objektu
5) Rozsah požáru/zásahu
6) Okolí objektu/zásahu
7) Je třeba dalších složek IZS ?
8) Je třeba letecká pomoc při zásahu ?
9) Je třeba speciálních pomocných prvků při zásahu ?
10) Je třeba vyhlásit krizovou situaci nebo jinak rozšířit pomoc při zásahu ?
11) Jaké další okolnosti je třeba brát v potaz při zásahu ?
12) Kolik členů/posádek již na zásahu je ?
13) Využití GISu, čili zmapování daného zásahu
14) Rozlišné možnosti pro různé velitele/členy zásahu
15) Hrubý nákres situace pomocí jednoduchého editoru
16) Nebezpečné prostředí ?
17) Hořlaviny/výbušniny ?
18) Ostatní/Přidat další

Tyto možnosti by se také dělily, aby mezi nimi byla snadná navigace. Dělení by bylo na různé potřeby nebo také úplně základní dělení by bylo podle velmi běžných MU nebo velmi běžných výjezdů/zásahů. Dále by bylo dělení na potřeby jednotek nebo velitelů zásahu, potřebují-li další vůz nebo nějaké speciální vybavení. Potřebuje-li se například ještě výpomoc armády. Toto dělení by se také dalo přizpůsobit samozřejmě potřebám složek IZS.

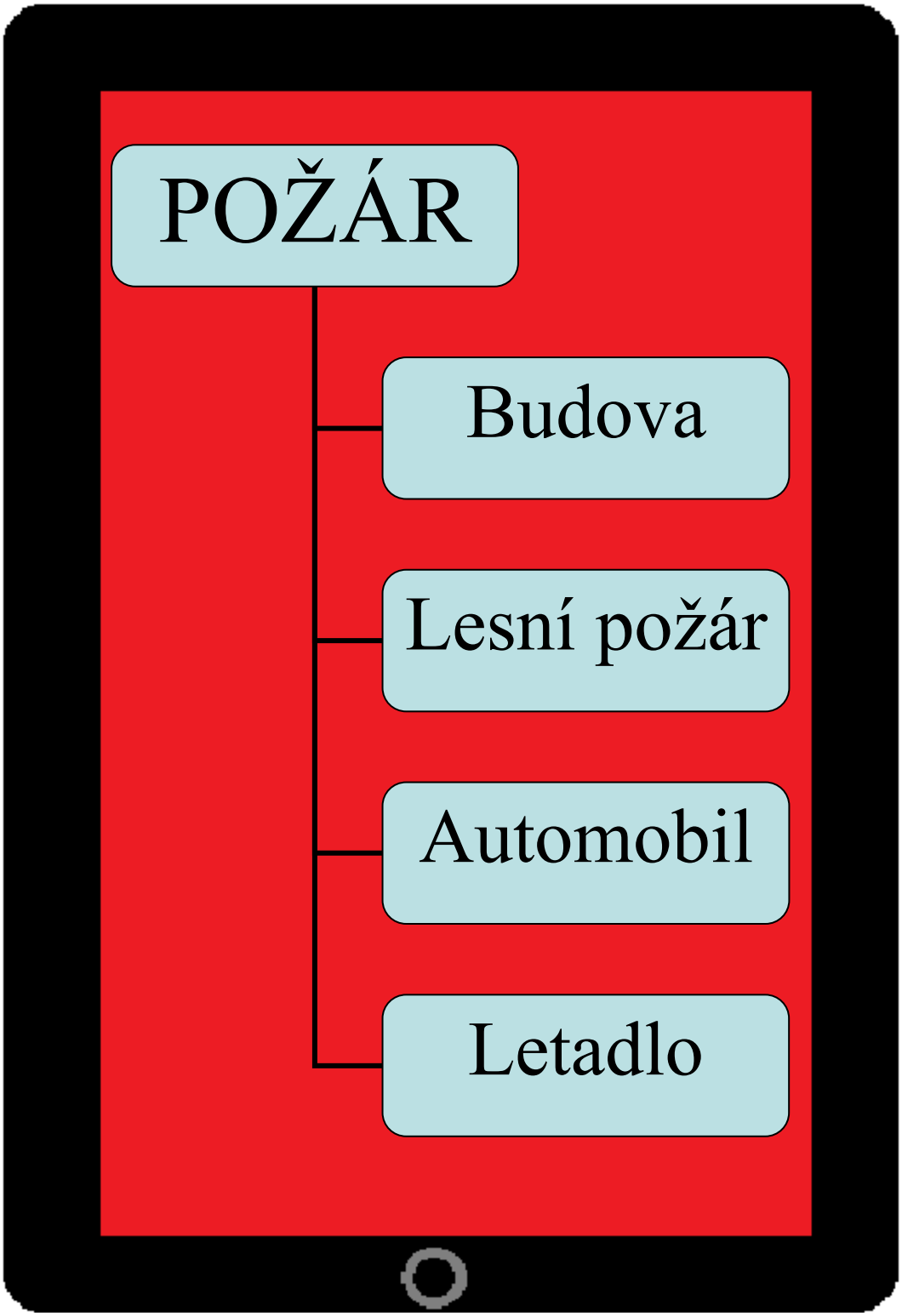
8.2 Grafický návrh

Má představa toho, jak by mohl takový jednoduchý webový klient vypadat. Rozhodně bych volil možnost rozlišit malé a velké displeje neboli tablet/notebook a mobilní telefon nebo nějaké jiné menší zařízení. U větších zařízení by bylo více možností, určení by bylo hlavně pro velitele zásahů nebo pro koordinátory. Mobilní zařízení by byly pro jednotlivé členy. Dalo by se také určitě rozlišit i při větších MU přímo pro obyvatele, to je však již také trochu jiné téma a pro jinou, respektive další práci. V grafickém rozhraní by bylo jednoduché, velmi intuitivní ovládání, které by bylo rozlišené do několika částí a v několika různých vrstvách. Vrstvy by byly děleny podle klasického dělení velení od koordinátora celé krize až případně po jednotlivé členy zásahu. Koordinátor celého zásahu nebo MU by měl k dispozici všechny složky IZS kterým by mohl přidělovat jednotlivé úkoly nebo s nimi jinak pracovat. Dále velitelé jednotlivých složek IZS by měli samozřejmě pod sebou své jednotky. A v neposlední řadě by pak byli velitele jednotlivých skupin. Všechno by tito velitelé měli na pouhých pár kliknutí, jednotky by se přesunovaly stylem drag-and-drop podle toho jak by bylo potřeba. Jednotky HZS by pak měly jednoduché check boxy, kde by si rychle mohly navolit jaký druh požáru například probíhá nebo co přesně hoří a co by například mohlo být v daném prostoru. Dále připadají v úvahu možnosti co sem již zmínil v kapitole 8.1.1. Grafický návrh je jen samozřejmě hrubý náhled toho, jak by to mohlo vypadat. Realita by se dala jistě přizpůsobit na míru, třeba i jednotlivým složkám IZS.

Obrázek 4Příklad návrhu volby jednotky



Obrázek 5Návrh přidávání složek IZS



Obrázek 6Příkladné možnosti požáru

8.3 Využití implementace cloudu u obyvatelstva

Využití je nasnadě. Cloudové úložiště se využije pro uložení nejaktuálnějších dat pro obyvatelstvo, které může danou MU sledovat v reálném čase. Velitelé IZS mohou tak přímo obyvatelstvu sdělit, co mohou udělat v jakém případě MU. Jako největší výhodu u tohoto stylu sdělování důležitých informací obyvatelstvu vidím využití GISu jako pomocného nástroje. Členové IZS mohou tak jednoduše označit různá důležitá místa pro obyvatele, jako jsou například nebezpečné zóny nebo naopak zóny pro potřebu úkrytu nebo zóny pro vyzvednutí potravin nebo pitné vody.

Obrázek 7Příklad únikové cesty [10]

ZÁVĚR

Moji bakalářskou práci jsem věnoval především studii implementace cloudových technologií pro krizové řízení. V teoretické části jsem definoval jednotlivé dílčí věci v rámci cloudových technologií, kde jsou nutné znalosti pro následnou praktickou část. Ty obsahují také důležitá fakta ze světových zdrojů, která jsou velmi důležitá pro moji práci, jelikož jde z velké části také o využití v celosvětovém a nadnárodním měřítku. Použil jsem všechny možné cloudové technologie a zvážil jsem taktéž bezpečnost, která je velmi důležitá. Obzvlášť v době, kdy se navyšuje útoků kybernetických na všemožné servery, tak pokud jde o bezpečnost obyvatel, tak se musí samozřejmě také jednat o nejvyšší bezpečnost technologických sítí, čili cloudů.

V praktické části jsem již zohledňoval konkrétní případ části krizového řízení a to sice Integrovaný záchranný systém. Implementoval jsem případný cloudový systém pro IZS a vyčlenil jsem možnosti pro tento systém. Také jsem nastínil, jak by mohla vypadat jedna z jeho podob.

SEZNAM POUŽITÉ LITERATURY

[1] Lenovoblog, dostupné z <http://www.lenovoblog.cz/2014/05/co-je-to-cloud-patri-mu-budoucnost-dat.html>

[2] Ministerstvo vnitra ČR, dostupné z <http://www.mvcr.cz/>

[3] Cloud.cz, dostupné z <http://www.cloud.cz/cloud/158-cloud-computingco-ty-pojmy-znamenaji.html>

[4] Ministerstvo vnitra ČR, dostupné z <http:// http://www.mvcr.cz/clanek/organy-krizoveho-rizeni.aspx>

[5] T-systems, dostupné z <http://www.t-systems.cz/produkty-a-reseni/cloud-computing/677144_1/blobBinary/pdf5-ps.pdf>

[6] T-systems, dostupné z <http://www.t-systems.cz/produkty-a-reseni/cloud-computing/677144_1/blobBinary/pdf5-ps.pdf>

[7] CAD.cz, dostupné z https://www.cad.cz/gis/80-gis/3001-informacni-system-krizoveho-rizeni-hlavniho-mesta-prahy.html

[8] HZS ČR, dostupné z http://www.hzscr.cz/clanek/integrovany-zachranny-system.aspx

[9] JČU ČB, dostupný obrázek z https://www.zsf.jcu.cz/cs/katedra/katedra-radiologie-toxikologie-a-ochrany-obyvatelstva/informace-katedry/informace-pro-studenty/ucebni_texty/ochrana-obyvatelstva-se-zamerenim-na-cbrne-aplikovana-radiobiologie-a-toxikologie-krizova-radiobiologie-a-toxikologie/struktura-a-legislativa-izs-koordinace-a-navaznost-cinnosti-slozek-izs-mu-a-ks

[10] County of Haliburton, dostupný obrázek z https://haliburtoncounty.ca/services/planning-and-gis/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IZS Integrovaný záchranný systém

MU Mimořádná událost.

IT Internet technology

NAS Network attached storage

NIST National Institute of Standards and Technology

ITIL Information Technology Infrastructure Library

SaaS Software as a Service

PaaS Platfrom as a Service

IaaS Infrastructure as a Service

ICT Information and communication technology

USB Universal seriál bus

GIS Geographical information system

HMP Hlavní město praha

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH