Bezpečnost informací ve vztahu k ochraně obyvatelstva

Gabriela Chovancová

Bakalářská práce
2018

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: 2017/2018

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

Jméno a příjmení:	**Gabriela Chovancová**
Osobní číslo:	**L16134**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**prezenční**

Téma práce: **Bezpečnost informací ve vztahu k ochraně obyvatelstva**

Zásady pro vypracování:

1. **Zpracujte rešerši s důrazem na monografie, studie, analýzy a další vztažné materiály.**
2. **Analyzujte bezpečnost informací vybraného subjektu ochrany obyvatelstva.**
3. **Na základě zjištěných skutečností navrhněte případná doporučení směřující ke zvýšení bezpečnosti informací vybraného subjektu.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] LAND, Michael, Truett A. RICKS a Bobby E. RICKS. Security management: a critical thinking approach. Boca Raton: CRC Press, Taylor & Francis Group, 2014, xiv, 188. Occupational safety & health guide series. ISBN 978-1-4665-6177-9.

[2] DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

[3] Ochrana obyvatelstva a krizové řízení: skripta. Praha: Ministerstvo vnitra – generální ředitelství Hasičského záchranného sboru ČR, 2015. ISBN 978-80-86466-62-0.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce:	**Ing. Petr Svoboda** Ústav ochrany obyvatelstva
Datum zadání bakalářské práce:	**3. listopadu 2017**
Termín odevzdání bakalářské práce:	**15. května 2018**

V Uherském Hradišti dne 10. listopadu 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 / DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- odevzdáním bakalářské/diplomové 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/diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou/diplomovou 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/diplomovou 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/diplomové 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/diplomové práce využít ke komerčním účelům;
- pokud je výstupem bakalářské/diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti 15. 5. 2018

Chovancová

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, již 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

Tato bakalářská práce se zabývá zabezpečením informací v organizaci. Je představena problematika ochrany informací a nastíněny návrhy na zlepšení bezpečnosti informací při zpracování a uchovávání informací v organizaci.

Klíčová slova: bezpečnost informací, bezpečnostní politika, hrozby, rizika, ochrana obyvatelstva

ABSTRACT

This bachelor work is concerning safety of organization´s information. It is presented the issue of the protection of information and outlined proposals for improving the security of information in the process

Keywords: information security, security policy, threats, risks, protection of the population

Chtěla bych poděkovat Ing. Petru Svobodovi, za odborné vedení mojí bakalářské práce a věnovaný čas. Dále bych chtěla poděkovat mé rodině za jejich podporu po dobu mého studia.

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

OBSAH

ÚVOD

Vzhledem k rozvoji informačních a komunikačních technologií, je problematika bezpečnosti informací v současné době důležitou oblastí. Dochází k nárůstu citlivých informací, která mohou být terčem útoků, čímž se zvyšují rizika informační bezpečnosti. Nové technologie pro zpracování informací, s sebou přináší i vyšší nároky na jejich zabezpečení.

Využívání informačních a komunikačních technologií je nezbytnou součástí pro efektivní provoz organizace. Technologie obsahují veškeré informace organizace a jakékoliv ohrožení těchto technologií má nepříznivé dopady. Proto by každá organizace měla dodržovat určitá bezpečnostní pravidla, která vedou k zajištění ochrany informací. Tato pravidla jsou formulována v dokumentu Bezpečnostní politika organizace, který obsahuje všechny principy, zásady, omezení, pravidla a postup pro řízení aktiv v organizaci.

Cílem mé bakalářské práce je představit problematiku bezpečnosti informací ve vztahu k ochraně obyvatelstva. Vypracovala jsem plán zabezpečení informační bezpečnosti v konkrétní organizaci, kdy jsem zjistila nedostatky a problémy, které dále slouží jako podklad pro vytvoření návrhu na jejich odstranění.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST INFORMACÍ

V dnešní době je bezpečnost informací nedílnou součástí každé organizace. Bezpečnost je součástí každodenního řízení a vnitřní kultury organizace.

1.1 Definice

Bezpečnost informačních systémů zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informací. Uplatnění obecných bezpečnostních opatření slouží k ochraně informací před jejich ztrátou nebo kompromitací, případně k jejich zjištění a přijetí nápravných opatření. Opatření zahrnuje bezpečnost počítačů, přenosu, emisí a šifrovací bezpečnost a odhalování ohrožení skutečností a systémů a jeho předcházení. Před neautorizovaným přístupem nebo porušením integrity dat vypomáhá **ochrana dat**, která zahrnuje technické, administrativní, procedurální, personální nebo fyzická opatření. Opatření znamená řízení rizika, včetně politik, postupů, směrnic, obvyklých postupů nebo organizačních struktur, které mohou být administrativní, technické, řídící nebo právní povahy. [1]

*,,**Informační systém** je funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracování, uchování a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy.*‘‘ [1]

Pojem **informace** je široký a mnohoznačný pojem a využívá se v různých významech. Informace obecně je chápána jako údaj o reálném prostředí, o stavu a procesech, které v něm probíhají. V informatice tvoří informaci kódovaná data, která lze vysílat, zpracovávat a uchovávat pomocí technických prostředků. Pojem informace se často zaměňuje s pojmem **data**, která spíše představují fakta, měření, obraz, zvuk či video v kontextu sledovaného procesu nebo situace. Data jsou vstupem či výstupem počítačového programu a jsou nezávislá na uživateli a většinou odráží současný stav reality. [1],[2]

Kybernetická bezpečnost je souhrn právních, organizačních, technických a vzdělávacích prostředků směřující k zajištění bezpečnosti kybernetického prostoru. Ochranu proti kybernetickému útoku a zmírňování následků nazýváme **kybernetická obrana**, která posiluje schopnost se účinně bránit. Pomocí **kybernetické strategie** dosahujeme rozvoje a využití schopností pracovat v kybernetickém prostoru, integrovaného a koordinovaného

s ostatními oblastmi k dosažení stanovených cílů pomocí identifikovaných prostředků a metod. [2]

Počítačová bezpečnost je obor informatiky, který se zabývá zabezpečením informací v počítačích. Zahrnuje zabezpečení ochrany před neoprávněným manipulování se zařízením, ochranu před neoprávněnou manipulací s daty, ochranu informací před krádeží nebo poškozením, bezpečnou komunikaci a přenos dat, bezpečné uložení dat a dostupnost. [2]

Jako komunikační prostředí pak většinou funguje **internet**, který představuje nechráněný informatický prostor, ve kterém během přenosu dat může docházet k narušování integrity, dostupnosti a důvěryhodnosti sdílených informací. Jednotlivé informační systémy mohou být prostřednictvím internetu cílem určitých útoků. Je nutno si uvědomit, že přístup do sítě internetu má jak uživatel, tak útočník. [1],[2]

1.2 Legislativa

Při zpracování bezpečnostní politiky je nutné pracovat s požadavky a povinnostmi vyplývajících z legislativních úprav ve státě. V této kapitole jsou uvedeny pouze vybrané základní legislativní předpisy. [3]

Zákon o Kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Tento zákon upravuje práva a povinnosti osob a působnost, ale také pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zákon se zabývá kybernetickým prostorem digitálního prostředí umožňující vznik, zpracování a výměnu informací, tvořené systémy, a službami a sítěmi elektronických komunikací. Dále se v tomto zákoně rozumí kritickou infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací a významným informačním systémem informační systém spravovaný orgánem veřejné moci, u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

Bezpečnostním opatření se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v IS a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru. Bezpečnostními opatřeními jsou:

a) organizační opatření,
b) technická opatření. [4]

ISO (International Organization for Standartization)

Mezinárodní organizace pro standardizaci si rezervovala sérii ISO 27000 pro normy z oblasti bezpečnosti informací. ISO/IEC 27000:2014 je soubor mezinárodních standardů zaměřená na řízení informační bezpečnosti v organizacích. Jednotlivé standardy cílí na různé aspekty informační bezpečnosti v organizacích. Poskytují praktické nástroje pro ty organizace, které chtějí identifikovat a řídit environmentální dopad svého chování a trvale udržovat a zlepšovat environmentální výkonnost. [5]

Organizace mohou použitím norem ISMS vyvinout a implementovat rámec pro řízení bezpečnosti svých informačních aktiv zahrnující finanční informace, informace o zaměstnancích, nebo informace, které jim byly svěřeny třetími stranami. Tyto normy mohou být také použity pro přípravu na posouzení jejich ISMS, týkající se ochrany dat. [5]

ČSN ISO/IEC 27001 a ISO/IEC 27002 jsou základním kamenem pro vytvoření bezpečných IS a jsou z nich odvozeny prakticky všechny zásadní postupy při vytváření a hodnocení bezpečnosti informací. Umožňují snadné ověření stavu bezpečnosti výměny informací mezi institucí a obchodními partnery. Současně platné normy, které se týkají bezpečnosti informací, vychází z ISO/IEC 27000. Tato řada ISO/IEC 27000 je klíčová pro bezpečnost informací státu. Tato mezinárodní norma specifikuje požadavky na ustanovení, realizaci, udržování a neustálé zlepšování systému řízení informační bezpečnosti v rámci rizik organizace. Požadavky této normy jsou používány ve všech organizacích, bez ohledu na jejich typ, činnost či velikost. [5]

1.3 Metodiky

Nezbytným předpokladem pro dříve popsané nové koncepce řízení informatiky je jejich podpora ve formě různých standardů, nejlepší zkušeností nebo metodik. [6]

1.3.1 COBIT

Metodika COBIT (Control Objectives for Information and Related Technology) je pevně spojena s organizací ISACA (Asociace pro audit a řízení informačních systémů). Jedná se o sadu všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, která má za cíl pomoci organizaci maximalizovat užitek plynoucí z informačních technologií. Metodika COBIT je jedním ze základních nástrojů podporující IT Governance v organizacích. [6],[7]

Základní princip metodiky COBIT je postaven na cílech organizace (strategických požadavcích), zdrojích informačních technologií a procesech. Tyto tři komponenty využívá tzv. COBIT kostka. Současně nejlépe ukazuje základní koncepci metodiky: zdroje informatiky jsou řízeny procesy tak, aby bylo dosaženo stanovených cílů, které odpovídají strategickým požadavkům. [6],[7]

1.3.2 ITIL

ITIL (Information Technology Infrastructure Library) představuje soubor knih, který obsahuje popis způsobů procesního řízení služeb včetně infrastruktury IT, které jsou jejím prostřednictvím poskytovány. ITIL se koncentruje na plánování, vytváření, modifikaci, dodávku, správu, analýzu a použití služeb IT. Cílem metodiky ITIL je poskytnout ucelený soubor tzv. nejlepších zkušeností pro oblast řízení služeb IT a souvisejících procesů. [6],[7]

Pro metodiku ITIL jsou charakteristické:

- Procesní přístupy – procesně orientovaný přístup k řízení informatiky a informatických služeb je považován za jeden z jejích primárních znaků.
- Best Practise – hlavním důvodem oblíbenosti metodiky ITIL je jistě to, že obsahuje shrnutí nejlepších zkušeností z praxe.
- Respektování individuality – metodika ITIL poskytuje návod, co by se mělo udělat, ale nikoli jak se to mělo udělat. [6],[7]

1.4 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Národní úřad pro kybernetickou a informační bezpečnost je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Vznikl 1. srpna 2017 na základě

zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). [8]

Hlavní činnosti NÚKIB:

- provozovat Vládní CERT České republiky (GovCERT.cz),
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy,
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy,
- příprava bezpečnostních standardů pro informační systémy KII a VIS,
- osvěta a podpora vzdělání v oblasti kybernetické bezpečnosti,
- výzkum a vývoj v oblasti kybernetické bezpečnosti,
- ochrana utajovaných informací v oblasti informačních komunikačních systémů,
- kryptografická ochrana. [8]

Administrativní bezpečnost

Administrativní bezpečnost tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi.

Pravidla administrativní bezpečnosti jsou uvedeny ve vyhlášce č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utahovaných informací. [8]

Personální bezpečnost

Personální bezpečnost je základním druhem, jak zajistit ochranu utajovaných informací. Kromě ověřování podmínek, které musí fyzická osoba splnit, aby jí byl umožněn přístup k utajované informaci, zahrnuje personální bezpečnost i výchovu osob. Za zajištění proškolení fyzických osob, které jsou v přímém styku s utajovanou informací, ručí odpovědná osoba. Proškolení se koná jednou ročně a odpovědná osoba musí vést o těchto proškoleních přehledy. [9]

Fyzická bezpečnost

Fyzická bezpečnost zahrnuje technické prostředky a další prvky fyzické bezpečnosti a jejich certifikaci. Je druhem zajištění ochrany utajovaných informací. Fyzickou bezpečnost, tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím. Pro zabezpečení ochrany utajovaných informací v rámci fyzické bezpečnosti se určují objekty, zabezpečené oblasti a jednací oblasti. Objektem je budova nebo jiný ohraničený prostor, v kterém se zpravidla nachází zabezpečená oblast nebo jednací oblast. Objekt slouží ke zpracování a manipulaci s utajovanou informací. Zabezpečená oblast slouží k ukládání utajované informace, která se ukládá v zabezpečené oblasti v trezoru nebo jiné uzamykatelné schránce. [10]

Průmyslová bezpečnost

Podnikateli, který nezbytně k výkonu své činnosti potřebuje přístup utajované informaci stupně utajení Důvěrné a vyšší, lze umožnit tento přístup, pokud je držitelem platného osvědčení podnikatele příslušného stupně utajení nebo vyššího, pokud zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, nestanoví jinak.

Osvědčení podnikatele vydává Úřad podnikatelů, který splňuje podmínky pro jeho vydání stanovené v zákoně, po provedeném bezpečnostním řízení. [11]

1.5 Cíle bezpečnosti informací

Eliminace informatických útoků, eliminace hrozeb a rizik plynoucích z možných bezpečnostních incidentů, dosažení prokazatelné míry bezpečnosti IS a tím i jeho důvěryhodnosti.

Bezpečnosti se dosahuje cílenou aplikací bezpečnostních protiopatření v oblasti objektové, personální a technické. Tato protiopatření ve všech těchto oblastech jsou ve vzájemné provázanosti a nelze je oslabovat. [1]

Důležité je bezpečnost informací dostatečně řídit, hlavně při pořizování nového software, hardware, nebo při přijímání nových pracovníků. Proces řízení bezpečnosti informací představuje implementaci osvědčených modelů, postupů a bezpečnostních prvků. [2]

Základní atributy cíle bezpečnosti informací:

- Důvěrnost – zajištění bezpečného zacházení s informacemi.

- Celistvost – zajištění, že informace nemohou být neoprávněně zničeny, nebo pozměněny.
- Dostupnost – zajištění, že oprávněné osoby mají nerušený přístup k informacím, nebo službám.
- Autentizace – ověření, že subjekt je tím, za koho se vydává.
- Autorizace – ověření, zda má subjekt právo provést operaci.
- Nepopiratelnost – zajištění, že subjekt, který inicioval operaci, nebude moci tuto skutečnost popřít.[2]

Základním cílem BI je ochrana a snížení hrozeb a jejich dopadů. Hrozby mohou být např.:

- kompromitace,
- nedovolená změna hodnot,
- zničení informačního systému,
- zneužití citlivých informací,
- použití klamných dat,
- špatná interpretace hodnot,
- neoprávněný přístup k hmotným i nehmotným hodnotám,
- únik informací (krádež, kopie apod.). [7]

1.6 Důvody útoků

Během příprav bezpečnostní politik a krizových plánů je nezbytné pozorně zvážit a generický popsat možný průběh útoků v informatickém prostoru, stanovit pravděpodobnosti jejich výskytu a odhadnout rizika, která jsou na ně vázána. [1],[7]

Útočník může být limitován svými ekonomickými a technickými možnostmi, při čemž náklady na kvalifikovaně vedený informatický útok jsou vysoké a rostou s jeho složitostí. Proto nelze ze strany teroristických organizací vyloučit příklon k využívání relativně lacinějšího a snazšího útoku, vedeného hrubou silou proti fyzické integritě informačních systémů. Navíc tento způsob může být velmi účinný a odpovídá lépe mentalitě některých teroristických skupin a hnutí, které takto vedeným útokem sledují současně i své ‚politické zviditelnění'. [1],[7]

V dnešní době neexistuje žádná větší společnost nebo stát, který by nebyl závislý na připojení do kyberprostoru. V případě, že se hackerům podaří v tomto prostoru realizovat rozsáhlý útok, jsou důsledky katastrofické. Hrozby útoků v kyberprostoru neustále rostou. Ve většině případů je obtížné určit, kdo je útočníkem. Zkušení hackeři se umí v kyberprostoru velmi dobře orientovat. [7]

1.7 Prevence bezpečnosti informací

Na základě analýzy příčin a podmínek zločinnosti v této oblasti lze předem nebo v průběhu informačních procesů předejít zneužití, poškození, odcizení nebo zničení informací.

Cílem prevence je především předejít vzniku příčin a podmínek zločinnosti a kriminality, nebo odvrátit toto nebezpečí pokud vznikají náznaky ohrožení a překazit, zabránit procesům, které mají nežádoucí a kriminogenní účinky. [2]

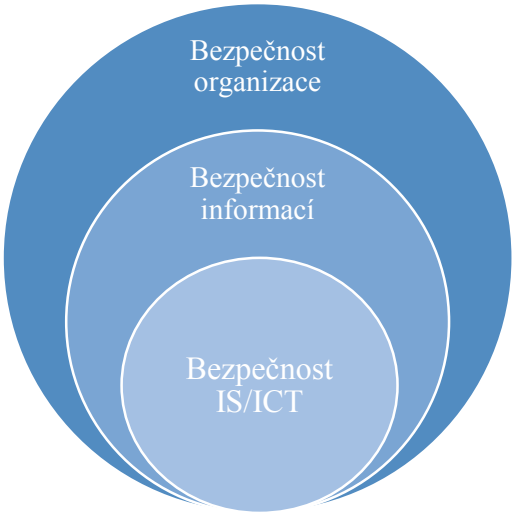
Subjekty prevence jsou nositelé i příjemci informací jako manažeři, organizátoři, pracovníci pracující v této oblasti, nebo také speciální orgány a organizace zaměřující se na informační bezpečnost. [2]

Objektem prevence budou vlastní informace jako duševní vlastnictví, tedy vlastnictví nehmotných statků, informační procesy a systémy, a to jako celek, tak i jejich části, nosiče, i nositelé. [2]

1.7.1 Řízení bezpečnosti informací

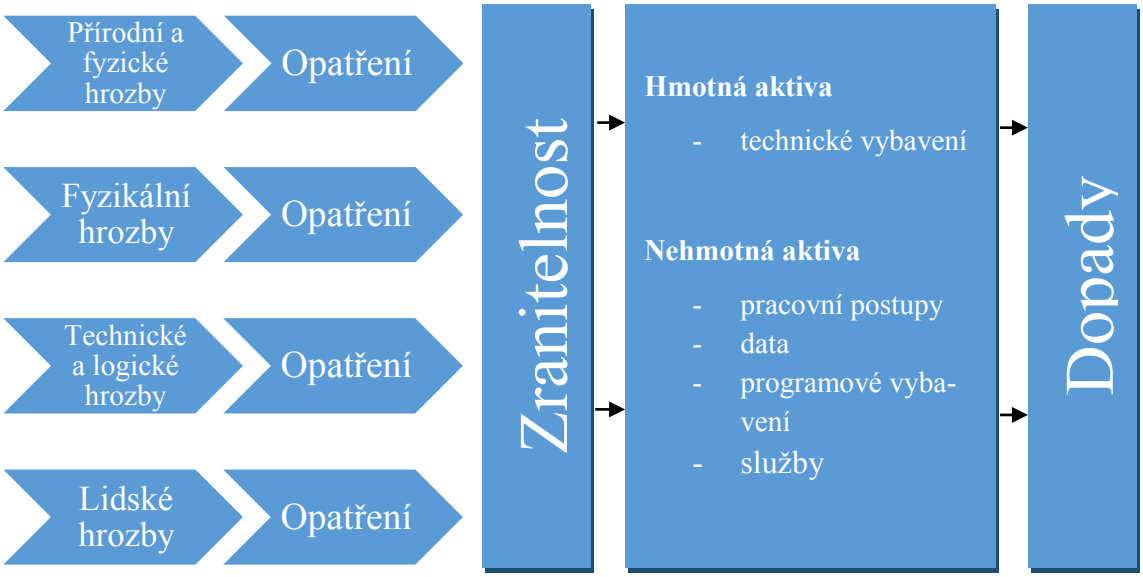
Jednou z kategorií bezpečností informací je bezpečnost organizace, jejíž součástí je zajištění bezpečnosti objektu, majetku organizace, jako je kontrola přístupů do objektu, strážní služba apod. Některé z těchto činností napomáhají zároveň k zajištění bezpečnosti IS/ICT, jako např. kontrola oprávnění fyzického přístupu do budov. [2],[6]

Bezpečnost IS/ICT má za úkol chránit ta aktiva, která jsou součástí informačního systému organizace podporovaného informačními a komunikačními technologiemi. Pracuje s „neviditelnými“ daty, informacemi a službami. V organizaci nepředstavuje fyzické médium, ale data jsou na něm nahraná. Jde např. o pravidla pro zadávání a správu přístupových hesel, pravidla provozu informačního systému organizace, pravidla pro krytování dat apod. [2]



Obrázek 1 - Vztah úrovní bezpečnosti v organizaci [zdroj: upraveno dle [2]]

Následující schéma zobrazuje vztahy mezi aktivy organizace a hrozbami které na ně potencionálně působit prostřednictvím zranitelnosti, možnost ochrany aktiv organizace formou opatření a dopady reálných hrozeb. [2]



Obrázek 2 - Zajištění bezpečnosti IS/ICT v organizaci [zdroj: upraveno dle [2]]

Formalizace řízení bezpečnosti informací slouží ke snížení pravděpodobnosti bezpečnostního selhání a vytváří strukturu dokumentů, která obsahuje jednotlivé plány řízení bezpečnosti:

- bezpečnostní politika,
- bezpečnostní standardy,
- bezpečnostní normy,
- bezpečnostní postupy,
- bezpečnostní procedury. [12]

Tvoří se jako separované dokumenty, jejichž výhodou je, že uživatel nemusí znát všechny standardy, politiky, normy a postupy a v případě změny, se mění pouze příslušný dokument. [12]

Bezpečnostní politika

Bezpečnostní politika je jedním ze základních pilířů, na kterém stojí systém řízení informační bezpečnosti. Musí být jasně definovány základní parametry, jinak nemůže být systém budován efektivně a účelně. jde o strategický plán implementace bezpečnosti v organizaci. [13],[14]

Bezpečnostní standardy

Bezpečnostní standardy vymezují povinné požadavky na užití hardwaru, softwaru, technologií a bezpečnostní kontrolu. Standardy poskytují průběh činností, kterým jsou procedury a technologie uskutečňovány uvnitř organizace. Představují také taktické dokumenty, které definují metody a postupy, díky kterým bude dosaženo cílů vymezených v bezpečnostních politikách. [13],[14]

Bezpečnostní normy

Bezpečnostní normy zahrnují minimální míru bezpečnosti, které by měl daný informační systém dosáhnout v rámci organizace. [13]

Bezpečnostní postupy

Bezpečnostní postupy obsahují pokyny, jak implementovat a zajišťovat bezpečnostní standardy a normy. Tyto postupy jsou přizpůsobeny každému informačnímu systému a podmínkám. Definují, jaké bezpečnostní mechanismy mají být použity, ale neurčují konkrétní produkt, nebo výrobce. [13],[14]

Bezpečnostní procedury

Bezpečnostní procedury se zabývají detailními návody popisující konkrétní akce, které jsou důležité pro implementaci bezpečnostních mechanismů, kontrol apod. Můžou se zaměřovat ne celý systém, nebo na konkrétní produkt. Bezpečnostní procedury se aktualizují při aktualizaci hardwaru nebo softwaru. [13],[14]

1.7.2 Oblasti informační bezpečnosti

Řízení bezpečnosti v organizaci se zabývá několika oblastmi. Jednotlivé části obsahují:

- Bezpečnostní politiku – stanovuje základní pravidla informační bezpečnosti.
- Řízení aktiv – přehled aktiv organizace a zajištění ochrany jednotlivých aktiv.
- Řízení přístupu – představují pravidla pro získávání přístupu ke všem informacím a komunikačním systémům.
- Organizace bezpečnosti informací – stanovení organizačních struktur.
- Bezpečnost z hlediska lidských zdrojů – definuje povinnosti pracovníků, které se vztahují na ochranu informací.
- Fyzická bezpečnost – vymezení pravidel pro přístup osob do objetu a ochrana zařízení ICT.
- Řízení komunikací a řízení provozu – zavedení opatření, které souvisejí se spolehlivým chodem informačních a komunikačních systémů organizace.
- Vývoj a údržba informačních systémů – zavedení principů informační bezpečnosti do rozvoje ICT.
- Zvládání bezpečnostních incidentů – pravidla pro řešení bezpečnostních incidentů.
- Soulad s požadavky – organizace se zavazuje k naplnění požadavků vyplývajících z právních závazků. [2]

1.7.3 Bezpečnostní politika

Každá společnost musí dodržovat bezpečnostní pravidla, která jsou nejčastěji formulována v bezpečnostní politice organizace. Bezpečnostní politika je dokument celkového zabezpečení organizace, který obsahuje principy, zásady, omezení, pravidla a postupy, podle kterých jsou v organizaci řízena veškerá aktiva firmy. [7],[13],[15]

Hlavním cílem je chránit interní sítě a data. Na bezpečnostní politiku navazují ostatní bezpečnostní dokumentace. Obsahuje souhrn bezpečnostních požadavků pro řešení informační

bezpečnosti na fyzické, personální administrativní a počítačové úrovni. Bezpečnostní politika je důležitá pro snižování rizik v organizaci a definuje, co je třeba chránit, proti čemu a jakým způsobem. [7],[15]

Při tvorbě dokumentu bezpečnostní politiky se musíme držet následujících kroků:

1. Posouzení vstupních vlivů.
2. Analýza rizik.
3. Zpracování bezpečnostní politiky.
4. Implementace bezpečnostní politiky.
5. Kontrola účinnosti bezpečnostní politiky a vyslovení závěrů. [15]

1.7.3.1 Tvorba bezpečnostní politiky

Posouzení vstupních vlivů

Posouzení vstupním vlivů je první krok při tvorbě bezpečnostní politiky. Nejprve dochází k rozhodnutí vedení zabývat se bezpečnostní politikou. Jde o určení zásadních cílů, strategií a politik pro bezpečnost informací v organizaci. Definuje klíčové problémy v oblasti bezpečnosti informací a vychází z aktuálního stavu organizace. [15]

Analýza rizik

Pro správné vyhodnocení rizik v organizaci je zapotřebí pojmenovat možné hrozby, kterým je organizace vystavena a provést analýzu rizik. Cílem analýzy rizik je identifikovat riziko a vyhodnotit tak, aby bylo možné rozhodnout, zda je přijatelné pro organizaci, či nikoli. [15],[16]

Vypracování bezpečnostní politiky

Pro vypracování bezpečnostní politiky je účinné využít vlastních zdrojů v organizaci, tudíž zaměstnance. Výhodou jsou nižší náklady a vyšší spojení tvůrce s organizací. Zaměstnanci mohou mít nedostatek znalostí a zkušeností, proto je spolehlivější pověřit externí firmu. [15]

Při tvorbě bezpečnostní politiky musí být pokryty všechny významné oblasti informační bezpečnosti. Bezpečnostní politika obsahuje metody a podmínky řešení informačního bezpečnosti. Návrh BP je zapotřebí provádět s ohledem na delší časové období, ne pouze na

aktuální stav a postupy je nutno ověřit a popsat jejich realizaci. Způsoby zabezpečení by se měli neustále kontrolovat a případně zdokonalovat. [15]

Dokument bezpečnostní politiky by měl obsahovat:

- definici, cíle, rozsah a důležitost bezpečnostní politiky,
- prohlášení vedení organizace o záměru podporovat cíle BI,
- výklad bezpečnostních zásad, principů a norem,
- stanovení obecných odpovědností pro oblast BI, a také vyhlášení bezpečnostních incidentů,
- odkazy na dokumentaci, která může BP podporovat. [16]

Implementace bezpečnostní politiky

Zde dochází k postupnému řešení dílčích kroků a projektů. Chybou v tomto kroku, může být například provádění kompromisů, nebo nedostatečná propagace bezpečnostní politiky. Obsah schvaluje vedení organizace a tato konečná verze BP je závazná pro všechny zaměstnance organizace. [16],[17]

Pokud bezpečnostní politika není sepsána v písemné formě, mohou nastat různé problémy. Každý zaměstnanec může pochopit BP po svém, na základě čeho můžou vznikat nejasnosti. Písemná forma napomáhá k přehlednosti bezpečnostní politiky. BP shrnuje veškerá aktiva a poukazuje na nebezpečí, která jim hrozí. [17]

S bezpečnostní politikou, by měl být seznámen každý zaměstnanec, například i uklízečka, která sice nemá přímý kontakt v informacemi, ale má neomezený přístup do všech prostor organizace a tím se dostává do vztahu k bezpečnostní politice prostřednictvím fyzické bezpečnosti. [16]

Kontrola účinnosti bezpečnostní politiky a vyslovení závěrů

Hodnocení, audit a monitoring stavu bezpečnosti informací v organizaci je nedílnou součástí bezpečnostní politiky. Velké a některé střední firmy by měli mít speciálního bezpečnostního technika, který bude zodpovídat za dodržování všeho, co souvisí s bezpečnostní politikou organizace a bude provádět přezkoumání stanovených pravidel (součástí přezkoumání by mělo být zhodnocení možností pro zlepšení a změny v přístupu k bezpečnosti). Pokud není prováděna kontrola účinnosti bezpečnostní politiky, může dojít

k neodhalení bezpečnostních incidentů a škody potom mohou být vyšší než při včas odhalených incidentech. [17]

1.7.3.2 Typy bezpečnostních politik

Dělení bezpečnostní politiky podle účelu:

- Regulační bezpečnostní politika – je požadována, pokud se organizace týkají jakékoliv průmyslové, nebo národní standardy a normy.
- Poradní bezpečnostní politika – tento typ BP vymezuje chování a aktivity, které jsou přijatelné a definuje následky jejich nedodržení. Jde o formulaci vrcholového managamentu.
- Informativní bezpečnostní politika – obsahuje informace o konkrétních subjektech. Jde např. o cíle společnosti, jaký způsobem firma komunikuje se svými partnery, zákazníky apod. [13]

Dělení bezpečnostní politiky podle formulace:

- Promiskuitní bezpečnostní politika – povoluje každému dělat vše, tedy i to, co by dělat neměl. Není obvykle provozně nákladná, důvodem použití této politiky je ekonomická nenáročnost řešení. Zaručuje pouze minimální bezpečnost (např. nenutí své zaměstnance používat hesla)
- Liberální bezpečnostní politika – povoluje každému dělat vše, až na věci, které jsou explicitně zakázané. Požadavkem je nízká ekonomická náročnost řešení. Tato politika je uplatňována, když jsou hrozby málo až průměrně závažné.
- Racionální bezpečnostní politika – zakazuje každému dělat to, co není explicitně povoleno. Tato politika je na zavedení nákladnější, ale zaručuje větší stupeň bezpečnosti. Požaduje provedení klasifikace objektů a subjektů podle jejich citlivosti a schopnosti.
- Paranoidní bezpečnostní politika – zakazuje každému dělat vše, co by mohlo být potencionálně nebezpečné. Zpravidla vede k maximální izolaci systému, díky čemu zaručuje nejvyšší stupeň bezpečnosti (např. zakazuje používat internetové služby, které by se daly zneužít). [13],[14]

2 OCHRANA OBYVATELSTVA

Ochrana obyvatelstva je širokou disciplínou, kterou nelze vysvětlovat a řešit jako plnění úkolů civilní obrany, nýbrž jakou soubor činností a úkolů odpovědných orgánů veřejné správy a také občanů, které vedou k zabezpečení ochrany života, zdraví, majetku a životního prostředí, v souladu s právními předpisy.

Tato problematika je v České republice obsažena jak v právních předpisech, tak na bázi dokumentů nelegislativního charakteru. Koncepce ochrany obyvatelstva představuje základní strategický plánovací dokument. Výchozím podkladem pro její zpracování je zejména **Bezpečnostní strategie ČR** a v ní identifikované bezpečnostní hrozby a zájmy ČR. [18]

Ochrana obyvatelstva je širokou disciplínou, kterou nelze vysvětlovat a řešit jako plnění úkolů civilní obrany, nýbrž jakou soubor činností a úkolů odpovědných orgánů veřejné správy a také občanů, které vedou k zabezpečení ochrany života, zdraví, majetku a životního prostředí, v souladu s právními předpisy.

Tato problematika je v České republice obsažena jak v právních předpisech, tak na bázi dokumentů nelegislativního charakteru. Koncepce ochrany obyvatelstva představuje základní strategický plánovací dokument. Výchozím podkladem pro její zpracování je zejména **Bezpečnostní strategie ČR** a v ní identifikované bezpečnostní hrozby a zájmy ČR. [18],[19]

2.1 Historie ochrany obyvatelstva

Již po 1. světové válce v Československé republice byla věnována pozornost ochrany obyvatelstva. Hlavními důvody byly napjaté vztahy mezi zeměmi, hrozba válečného konfliktu, vývoj leteckého průmyslu a možné použití chemických zbraní. V roce 1935 se přijal zákon č. 82/1935 Sb., o ochraně a obraně proti leteckým útokům a byla zřízena civilní protiletecká ochrana. Mezi hlavní úkoly civilní protiletecké ochrany patřilo – zabezpečit obyvatelstvo plynovými maskami a zařídit dostatečný počet veřejných úkrytů. V roce 1938 byl přijat zákon č. 75/1938 Sb. jako reakce na agresi a hrozbu Třetí říše. K 1. lednu 1976 byla civilní ochrana převedena z působnosti ministerstva vnitra do působnosti ministerstva obrany. Po vzniku samostatné ČR roku 1993 se začal používat termín civilní ochrana, která se soustředila především na opatření k ochraně životů a k omezení materiálních škod při mimořádných událostech. [18],[19]

2.2 Legislativa ochrany obyvatelstva

Roku 2000 vznikl tzv. balíček krizových zákonů:

- zákon č. 238/2000 Sb., o hasičském záchranném sboru ČR,
- zákon č. 239/2000 Sb., o integrovaném záchranném systému ČR,
- zákon č. 240/2000 Sb., o krizovém řízení,
- zákon č. 241/2000 Sb., o hospodářských opatření pro krizové stavy.

Ve stejné roce se zavedl pojem **ochrana obyvatelstva** a používá se dodnes a jejím garantem se stalo ministerstvo vnitra. [18]

2.3 Definice

Integrovaný záchranný systém – je koordinovaný postup jeho složek při přípravě na mimořádnou událost nebo při provádění záchranných a likvidačních prací.[18]

Krizová situace – krizová situace je narušení krizové infrastruktury nebo jiní nebezpečí, při nichž je vyhlášen stav nebezpeční, nouzový stav nebo stav ohrožení státu. [18]

Likvidační práce – jsou to činnosti vedoucí k odstranění následků způsobených mimořádnou událostí. [18]

Mimořádná událost – je škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují životy, zdraví, majetek nebo životní prostředí. [18],[19]

Ochrana obyvatelstva – rozumíme tím plnění úkolů civilní obrany, jedná se zejména o varování, evakuaci, nouzové přežití a ukrytí obyvatelstva a další opatření k zajištění ochrany jeho života, majetku a zdraví. [18],[19]

Riziko – situace, že s nějakou pravděpodobností vznikne událost, která může ohrozit životy lidí, zdraví, majetek a životní prostředí. Riziko je odvoditelné z konkrétní hrozby. [20]

Záchranné práce – jde o činnost k odvrácení nebo alespoň omezení bezprostředního působení rizik vzniklých mimořádnou událostí, která ohrožuje životy, zdraví, majetek nebo životní prostředí. [18],[20]

2.4 Současné bezpečnostní hrozby

Na základě analýzy bezpečnostního prostředí v České republice, lze identifikovat konkrétní hrozby pro její bezpečnost. Česká republika je členem mezinárodních organizací, zejména NATO a Evropské unie, zahrnují bezpečnostní hrozby i ty, které ohrožují i její spojence. Jde o tyto hrozby:

- Terorismus – mezi příčiny terorismu, patří v méně bohatých zemích stále přetrvávající chudoba, nedostatečný přístup ke vzdělání a zdravotní péče.
- Šíření zbraní hromadného ničení – jeden z hlavních problémů je prevence. V rozvojovém světě je absence účinné kontroly exportu zbraní a jiného vojenského materiálu.
- Kybernetické útoky – ke kybernetickým útokům dochází zejména kvůli rostoucí závislosti na informačních technologiích. Může dojít k úniku strategických informací, zásahům do informačních systémů státních institucí, které zajišťují základní funkci státu.
- Negativní dopad migrace – může způsobovat sociální napětí, napojení na organizovaný zločin.
- Organizovaný zločin a korupce – mezi nejdůležitější fenomény patří – ilegální organizovaná migrace, sexuální zneužívání dětí, prostituce, obchod s vojenským materiálem a globální obchod s narkotiky.
- Ohrožení funkčnosti kritické infrastruktury – narušení nebo nefunkčnost kritické infrastruktury má důležitý dopad na bezpečnost státu a zabezpečení základních životních potřeb pro obyvatelstvo, nebo ekonomiku státu.
- Pohromy přírodního nebo antropogenního původu – tytu mimořádné události, mají negativní vliv na zdraví a majetek obyvatel, životní prostředí, ale také na ekonomiku státu, např. zásobování surovinami, nebo pitnou vodou či poškození infrastruktury. [19],[21],[22]

3 CÍLE A POUŽITÉ METODIKY

Cílem této bakalářské práce je analyzovat a zhodnotit bezpečnost informací ve vztahu k ochraně obyvatel. Subjektem ochrany obyvatelstva byl vybrán konkrétní městský úřad.

V praktické části byly použity metody sběru dat a informací v podobě odborných konzultací se starostou obce a zaměstnanci městského úřadu. Dále byl popsán návrh bezpečnostní politiky městského úřadu a poté posouzení rizik pomocí SWOT analýzy.

SWOT analýza je komplexní metodou kvalitativního hodnocení. Hlavním účelem metody je klasifikace a hodnocení jednotlivých faktorů, které jsou rozděleny do základní čtyř skupin. Cílem této analýzy je získat přehled o možnosti jak snížit pravděpodobnosti hrozeb a zvýšit pravděpodobnosti příležitostí. Po vyhodnocení SWOT analýzy byla navržena možná opatření.

II. PRAKTICKÁ ČÁST

4 ANALÝZA SOUČASNÉHO STAVU BEZPEČNOSTI INFORMACÍ MĚSTSKÉHO ÚŘADU

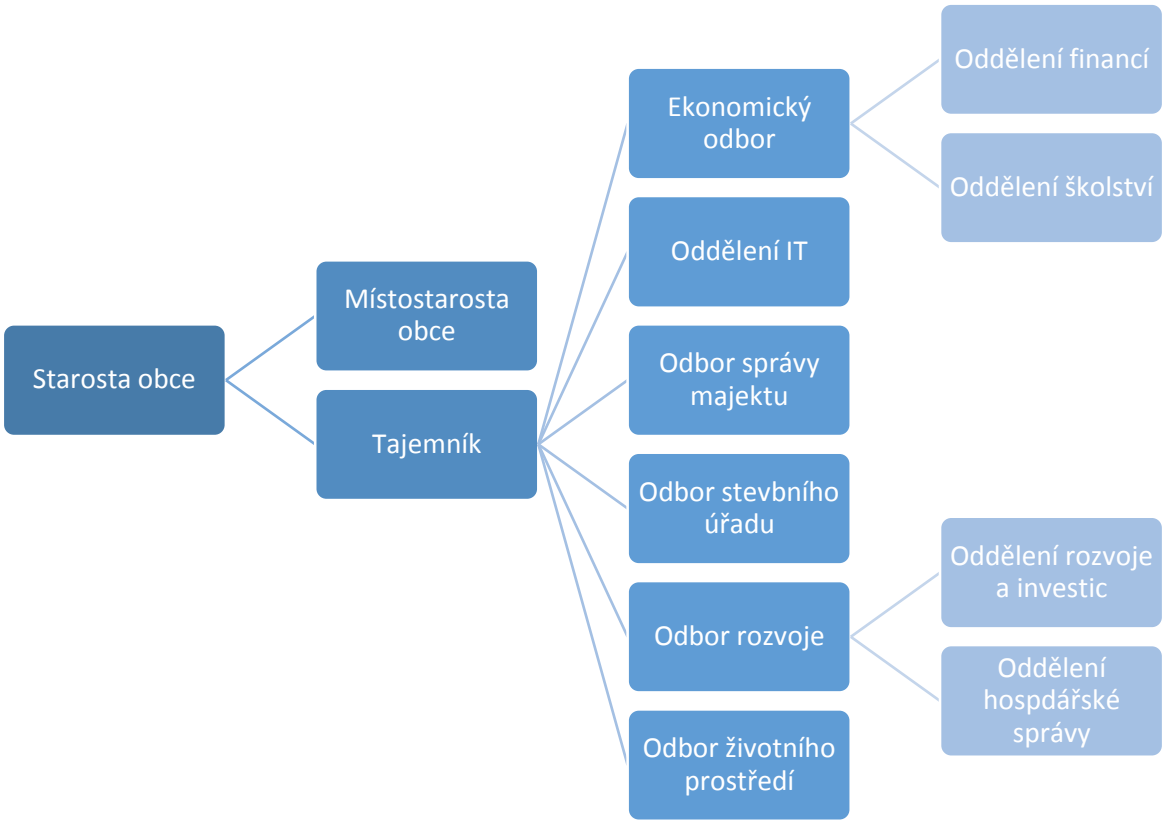
Tato část bakalářské práce se bude zabývat rozborem bezpečnosti informací konkrétního městského úřadu[1].

4.1 Organizační struktura městského úřadu

Podle zákona tvoří městský úřad starosta, místostarostové, tajemník městského úřadu a ostatní odbory. V organizaci je zaměstnáno přibližně 50 zaměstnanců. Městská rada může zřizovat odbory a oddělení pro jednotlivé druhy činností, které vedou zaměstnanci městského úřadu. Zkoumaná obec má více než 16 000 obyvatel.

Městský úřad zajišťuje úkoly a činnosti v oblasti samostatné a přenesené působnosti. V rámci této činnosti také zpracovává množství informací v elektronické i listinné podobě. Kromě informací přístupných veřejnosti jsou zpracovávány také informace o krizovém řízení a informace, které jsou určeny pouze pro interní potřebu organizace.

[1] Městský úřad si z důvodu povahy zjišťovaných skutečností nepřeje být konkrétně jmenován.



Obrázek 3 - Organizační struktura městského úřadu [zdroj: vlastní]

4.2 Popis současného stavu zabezpečení

Tento rozbor stavu zabezpečení městského úřadu slouží k zjištění, jaké úrovně bezpečnosti informací se zde dosahuje, což souvisí s informační, fyzickou, administrativní a personální ochranou. Získané informace byly získány prostřednictvím konzultace se starostou obce a zaměstnankyní městského úřadu.

Z analýzy současného stavu byly zjištěny následující závěry:

- Městský úřad má zpracovaný dokument, který určuje rámec bezpečnosti informací městského úřadu. Jsou zde definovány cíle a postoje k bezpečnosti informací.
- Zaměstnanci jsou obeznámeni s tím, co informace znamenají a proč je důležité je chránit.
- Městský úřad má zavedeny bezpečnostní mechanismy, s kterými jsou zaměstnanci seznámeni, což je důležité pro bezpečnost informací v organizaci. Je žádoucí,

aby účinnost bezpečnostních mechanismů byla v souladu s bezpečnostní politikou organizace a byla přiměřená odpovídajícím hrozbám.

Bezpečnostním mechanismem můžeme rozumět např. určitý algoritmus, který softwarově nebo hardwarově realizuje bezpečnostní funkci. Jsou to následující mechanismy:

- ochrana před hackery,
- ochrana před amatéry,
- ochrana proti útočníkům s vysokou úrovní znalostí,
- ochrana pro zachování důvěrnosti, integrity a autenticity zpráv.

— Městský úřad je střežen kamerovým systémem.

4.2.1 IT zabezpečení

Pracovní počítače: 13

Operační systém: Microsoft Office 7, Microsoft Office 10 a Citrix

Připojení k internetu: pomocí modemu o rychlosti 20 Mbps

V oblasti zabezpečení sítě a počítačů jsem dospěla k těmto výsledkům:

Operační systém

Operační systém je základním vybavením každého počítače. Stará se o správnou komunikaci mezi jednotlivými komponenty. Operační systém Microsoft Windows 7 je nejrozšířenějším operačním systémem. Je rychlý a spolehlivý. Je určen pro běžnou kancelářskou činnost. Zatímco Microsoft Windows 10 je určen spíše pro běžné uživatele, domácnost a studenty. Citrix umožňuje centrálně spustit Windows 10 stovkám i tisícům zaměstnanců současně a vyhnout se tak procesu aktualizace jednotlivých zařízení, proto je ideální pro zkoumanou organizaci.

Při zkoumání IT bezpečnosti bylo zjištěno, že správci sítě městského úřadu denně aktualizují operační systém.

Antivirová ochrana

Městský úřad používá antivirovou ochranu Eset, která je nainstalována na všech počítačích. Antivirový software musí být stále zapnutý, aby hlídal a kontroloval prováděné operace. Eset NOD 32 je antivirový program slovenské firmy ESET a nabízí vyváženou ochranu proti hrozbám, které ohrožují počítač a firemní systémy. Antivirus Eset patří mezi

nejlepší antivirový program. Antivirové programy mají za úkol chránit počítač před všemi škodlivými viry, jakou jsou např. červi, trojský kůň apod.

Mezi hlavní specifika programu patří:

- jednoduchá instalace a ovládání,
- nezatěžuje operační systém,
- automatické aktualizace virové databáze,
- kontrola příchozí a odchozí pošty.

Správci sítě zkoumané organizace správně aktualizují antivirovou ochranu, díky čemu snižují riziko napadení počítače viry.

Tabulka 1 – Porovnání antivirových programů ESET [zdroj: vlastní]

	ESET NOD32 Antivirus	ESET Smart Security	ESET Family Security Pack	ESET Smart Security Premium
Ochrana před viry	Ano	Ano	Ano	Ano
Podpora v českém jazyce	Ano	Ano	Ano	Ano
Ochrana internetového bankovnictví	Ne	Ano	Ano	Ano
Ochrana před hackery	Ne	Ano	Ano	Ano
Zabezpečená webkamera	Ne	Ano	Ano	Ano
Ochrana naší sítě	Ne	Ano	Ano	Ano
Rodičovská kontrola	Ne	Ano	Ano	Ano
Šifrování dat	Ne	Ne	Ne	Ano
Správce hesel	Ne	Ne	Ne	Ano
Mobilní ochrana	Ne	Ne	Ano	Ne

Zálohování dat:

Zálohování dat je běžnou prevencí rizika poškození pevného disku. Při zálohování většího množství dat se obvykle používá specializovaný program (např.: i v systému Microsoft Windows je součástí instalace), který celý proces zálohování usnadňuje. Pro zálohování většího množství dat je možné použít také specializovaná zařízení (hardware). Zálohování může probíhat mezi počítači propojených počítačovou sítí ve dvou základních režimech – online a offline.

MěÚ zálohuje data pomocí zálohovacího softwaru a vzdálenou zálohovací službou. Vzdálená zálohovací služba patří v dnešní době k nejpopulárnějším způsobu zálohování. Tato varianta zálohování zabraňuje poškození dat v důsledku požárů, povodní, či jiných mimořádných událostí. Nevýhodou může být pomalejší průběh zálohování, a také zneužití citlivých dat ze záloh třetí osobou. Mezi nejznámější zálohovací služby patří:

- Dropbox,
- Humyo,
- ADrive,
- Windows Live Mesh.

Typy záloh:

- Nestrukturované – jde o nejjednodušší způsob zálohování. Úložištěm mohou být např. diskety, CD, nebo DVD.
- Úplné a inkrementální – nejprve se provede úplná záloha a poté inkrementální záloha, kdy se zálohují pouze soubory, které se změnili od předešlé zálohy.
- Úplná a rozdílová – nejprve se provede úplná záloha a poté každá záloha zachytí všechny soubory, které jsou nově vytvořené nebo změněné.
- Zrcadlová a rezervně přírůstková – tato záloha obsahuje stav po poslední záloze, a také přírůstkové zálohy. Ukládáme pouze historii změn.
- Průběžná ochrana dat – provádí okamžitý zápis změny do žurnálu změn. Průběžné záznamy umožňují získat obraz dat v minulosti.
- Úplná záloha systému – zálohuje celý počítač i OS.

Používání internetu:

Ve zkoumané organizaci se nepoužívají nástroje k filtrování obsahu internetu. Bezpečné použití internetu záleží na každém zaměstnanci.

Politika hesel:

Jednou z nejdůležitějších věcí při dodržování bezpečnostních informačních podmínek jsou silná hesla. Silné heslo se vyznačuje následujícími vlastnostmi:

- Heslo by se mělo skládat nejméně ze sedmi znaků.
- Obsahuje znaky z nejméně tří ze čtyř skupin – velká písmena, malá písmeny, číslice a symboly.
- Výrazně se liší od předchozích hesel.
- Neobsahuje jméno nebo uživatelské jméno.
- Nejedená se o běžné slovo nebo jméno.

Heslo může být nejslabším místem v zabezpečení počítače. Silná hesla jsou důležitá, protože nástroje k odhalení hesel jsou v dnešní době zlepšovány. Z důvodu zabezpečení je třeba používat hesla obezřetně. Dodržováním následujících zásad můžeme hesla chránit:

- Heslo by se nemělo nikam zapisovat.
- Heslo by nemělo být sdělováno jiným osobám.
- Heslo pro přihlášení k síti, by se nemělo používat k jinému účelu.
- Heslo by se mělo měnit každých 60-90 dní.

Mezi nejčastější chyby, kterých se uživatel dopouští, při používání hesla patří:

- používání hesla jako vlastní jméno, jméno dítěte,
- používání hesla typu: „heslo“ nebo „1234“,
- používání stejného hesla příliš dlouho.

Zabezpečení počítače:

Zaměstnanci městského úřadu mají počítač zabezpečený pouze heslem, ale správci sítě mají v plánu zavedení bitlockeru. Bitlocket je nástroj Microsoftu, který je součástí vybraných edic Windows (např.: Windows Vista, Windows 7, Windows 10 Pro a Enterprise). Pomocí Bitlockerů můžeme zvýšit ochranu svých dat na pevném disku. Bitlocker může zabránit získání neoprávněného přístupu k systémovým souborům, nebo získání přístupu k datům na disku jeho odebráním z počítače pomocí šifrování systémových disků.

4.2.2 Fyzické a personální zabezpečení

Fyzické zabezpečení – vstup do budovy není nijak kontrolován či evidován. Zaměstnanci nemají identifikační karty. Budova je otevřena od 8:00 do odpoledních hodin, a je volně přístupná veřejnosti. Z vnější strany je budova monitorována kamerovým systémem. Pracovní počítače jsou zabezpečeny hesly. Městský úřad splňuje všechny požadavky v oblasti požární ochrany podle zákona č. 133/1985 Sb., o požární ochraně.

Účelem fyzické bezpečnosti je předcházet neoprávněnému přístupu k informacím, či poškození informací.

Při vstupu do budovy by měla být proveden kontrola, zda může osoba vstoupit do budovy. Tato kontrola bývá většinou zajištěna vrátným, který kontroluje vstup osob do budovy. Dále může být tato kontrola zajištěna v podobě čipových karet. Abychom zvýšili bezpečnost, je dobré po budově rozmístit kamery.

Personální bezpečnost – v této oblasti na MěÚ není téměř žádné zabezpečení. Zaměstnanci jsou pouze proškoleni o významu bezpečnosti informací. Všichni zaměstnanci by měli používat dostačující hesla na svých pracovních počítačích. O správné volbě hesla se zabývá politika hesel. Účelem personální bezpečnosti je snížit rizika lidské chyby, podvodu, krádeže, či zneužití prostředků organizace. Seznámení zaměstnanců s bezpečnostní politikou je součást vstupního školení.

Zaměstnanci mají zakázáno:

- Sdílet účty nebo hesla s jinými osobami.
- Ukládat hesla.
- Používat nedostačující hesla.
- Pořizovat kopie citlivých informací.
- Odnášet citlivé informace z prostor městského úřadu.
- Používat firemní email pro soukromé účely a naopak.
- Stahovat soubory z internetu.
- Instalovat programové vybavení.
- Kopírovat nelicencovaný operační systém.

Zaměstnanci jsou povinni:

- Používat pouze informace, které jsou nezbytné k plnění jejich pracovní činnosti.
- Chránit hardware a software.
- Nakládat s informacemi tak, aby byla zachována bezpečnost informací, a aby nedocházelo k bezpečnostním incidentům.
- Chránit průnik škodlivého programového vybavení do IT systémů.
- Okamžitě oznámit bezpečnostní incident, který se v systému objevil bezpečnostnímu manažerovi, nebo vedení organizace a učinit všechna opatření k minimalizaci následků.
- Dodržovat zásadu čistého stolu a čisté obrazovky.

Při nedodržení bezpečnostních zásad může být zaměstnanec postihnut za porušení povinnosti, nebo pracovní kázně dle zákona č. 262/2006 Sb., zákoník práce.
Školení zaměstnanců by se mělo provádět pravidelně v určitých intervalech. Nejčastěji by se měli školit nový zaměstnanci a poté by školení mělo probíhat jednou ročně.
Zásady zaměstnanců po absolvování školení:

- Zabezpečovat dokumenty, se kterými právě nepracují.
- Pokud si tisknou důležité dokumenty, nesmí je nechat ležet bez dohledu.
- Na pracovním počítači nesmí používat programy, které nejsou určené k jejich práci.
- Při odchodu z kanceláře se musí odhlásit z počítače.
- Po ukončení práce musí veškerá data uložit a zálohovat.
- Evidovat příchod a odchod do práce.

4.3 Proces tvorby návrhu bezpečnostní politiky

V této části jsem vytvořila návrh bezpečnostní politiky, neboli plán zabezpečení informací, kdy je nutné provést analýzu rizik, pro zjištění možných hrozeb. Poté jsem se zaměřila na bezpečnostní politiku městského úřadu, kde budou specifikovány hlavní cíle a požadavky na informační bezpečnost a také bezpečnostní opatření.

Cíle zabezpečení městského úřadu

MěÚ připouští, že jejich zabezpečení není ideální, z čehož vyplývá, že organizaci hrozí různá rizika a proto se budu zabývat tvorbou plánu zabezpečení. Cílem bude dosáhnout kvalitního zabezpečení, aniž by bylo třeba vynaložit větší sumy na jeho realizaci. Mezi hlavní cíle patří:

- identifikovat rizika,
- zdokonalit prevenci,
- navrhnout plány na opatření.

4.4 Analýza rizik bezpečnosti informací městského úřadu

Analýza rizik může být vypracována různými způsoby. Já jsem si vybrala jednoduchou neformální analýzu rizik. Znalosti potřebné k provedení analýzy jsem získala na základě rozhovorů se starostou a zaměstnankyní městského úřadu. Analýza rizik může sloužit jako podklad pro vytvoření bezpečnostní politiky.

4.4.1 Specifikace aktiv

Všechna aktiva musí být identifikována. Aktivum je cokoliv hmotného pro organizaci, co může být ohroženo působením hrozby. Dělí se do následujících kategorií:

- fyzická aktiva – hardwarové vybavení, počítače, technická zařízení, dodávky energie, vody, tepla, osvětlení,
- softwarová aktiva – operační systémy, technologie, informační systémy,
- informační aktiva – veškerá data, informace a údaje,
- lidské zdroje.

Informační aktiva mají různé požadavky na zajištění informační bezpečnosti. Za účelem přijetí opatření jsou stanoveny klasifikace informací:

- osobní údaje,
- interní údaje – informace, které nejsou určené pro veřejnost, ale pouze pro zaměstnance příslušného městského úřadu,
- externí údaje – informace, které jsou určené pro veřejnost.

4.4.2 Specifikace hrozeb

Pro vyhodnocení rizik je důležité pojmenovat hrozby, kterým je městský úřad vystaven.

Hrozby útoků

Jedná se o nebezpečí spojené s používáním internet. Každý zaměstnanec, který je připojený k internetu je potencionálním terčem útoku v podobě virů, spyware, spamů apod. Zranitelným místem může být opět zaměstnanec, který může útok umožnit třeba otevřením nevyžádané pošty, nebo nedostatky v systému zabezpečení sítě.

Mezi nejčastější slabiny v systému zabezpečení sítě patří:

- nedostatečné filtrování nevyžádané pošty,
- nedostatečné nástroje k filtrování obsahu webu,
- slabá hesla,
- poučení zaměstnanců o zásadách používání internetu.

Bezpečnostním opatřením může být zakoupení, instalace a pravidelné aktualizace programového vybavení a také školení zaměstnanců.

Hrozba vyzrazení informací zaměstnancem

Tento únik informací může být neúmyslný, ale také úmyslný. Tato hrozba může vyplývat z nedbalosti, nebo neznalosti zaměstnanců v oblasti informační bezpečnosti. Mezi formy vyzrazení informací patří:

- pořízení kopie dat,
- ústní sdělení neoprávněné osobě,
- předání dat neoprávněné osobě za úplatu,
- předání dat neoprávněné osobě za použití násilí nebo výhružkou.

Bezpečnostním opatřením může být častější proškolování zaměstnanců, aby si byli vědomi důležitosti informací. Míra naplnění tohoto rizika je na střední úrovni.

Hrozba nakládání s informacemi, ztráty nebo úniku informací

V tomto případě jsou nejčastějšími útočníky například bývalý nespokojení zaměstnanci. Jde o cílené útoky se záměrem poškodit informace. Útočníci mohou získané informace využít k vydírání. Nejčastější formy útoku jsou spojeny s užíváním internetu. Vzdělání zaměstnanců v oblasti informační bezpečnosti je důležité i v souvislosti s touto hrozbou.

Hrozba poškození informací živelnou pohromou

Informace mohou být poškozeny různými živelnými pohromami. Hrozbou může být:

- požár, může vzniknout selháním lidského faktoru, při kouření apod.,
- povodně,
- přívalové deště, větrná bouře s následným poškozením budovy,
- poruchy elektrické sítě následkem živelné pohromy.

Bezpečnostním opatřením proti těmto hrozbám můžou být důsledné kontroly při dodržování požárních předpisů, provádění pravidelných revizí hromosvodů a hasících prostředků, nebo školení zaměstnanců. Míra naplnění tohoto rizika je středně vysoká.

4.4.3 Návrh opatření

Opatření pro eliminaci hrozeb byly zajištěny za pomoci návrhu bezpečnostní politiky.

V této části práce budu navrhovat bezpečnostní politiku městského úřadu, která udává, co má být chráněno a stanovuje, jakým způsobem toho dosáhnout.

Politika bezpečnosti informací by se měla skládat s cílů a zásad bezpečnosti informací a následků pro porušení informační politiky.

Úvodní ustanovení

Politika bezpečnosti informací definuje základní strategie a zásady pro bezpečnost městského úřadu, určuje základní bezpečnostní pravidla pro používání a údržbu informací a informačních prostředků s cílem zajistit požadovanou úroveň ochrany informací.

Dodržování bezpečnostní politiky je vyžadováno od všech interních i externím zaměstnanců, bez rozdílu funkce.

Tato politika stanovuje přístup k řízení bezpečnosti informací, aby zajistila ochranu informací aktiv před hrozbami, ať už jde o hrozby přírodního charakteru, nebo lidského.

Aby bylo dosaženo ochrany informací, musí být v pravidelných ročních intervalech prováděny analýzy rizik, kterým jsou aktiva organizace vystaveny. Za revizi dokumentu bezpečnostní politiky odpovídá bezpečnostní manažer, který kontroluje efektivnost působení tohoto dokumentu.

Odpovědnost

Politika bezpečnosti informací je důležitý dokument, se kterým musí být seznámeni všichni zaměstnanci města. Tento dokument může být veřejně přístupný na internetových stránkách města.

Vedení městského úřadu by mělo:

- Pravidelně monitorovat a vyhodnocovat rizika vztahující se k informacím.
- Zabezpečit zneužití nebo ztráty informací.
- Dbát na to, aby náklady na bezpečnostní opatření byly vynakládány efektivně.

Každý zaměstnanec, který má přístup k informacím, přebírá odpovědnost za bezpečné nakládání s těmito prostředky a za ochranu informací ve své působnosti. Bezpečnostní politika je závazná pro všechny uživatele, bez ohledu na funkci, či pozici v úřadu. Každý uživatel nese odpovědnost za porušení pravidel v souladu s předpisy, s nimiž byli seznámeni.

Zásady práce s informacemi a způsob jejich zabezpečení:

- vytvářet a prosazovat systém přístupu k informacím,
- provádět stálou identifikaci bezpečnostních incidentů a přijímat opatření pro zlepšení bezpečnosti informací,
- zajistit ochranu osobních údajů v souladu s legislativou,

- zabezpečovat informační systémy, elektronickou poštu a internet,
- zabezpečit fyzickou bezpečnost,
- zajišťovat dostupnost, spolehlivost a integritu dat,
- monitorovat nebo kontrolovat stav bezpečnostních prvků,
- prosazovat politiku bezpečného pracoviště,
- zajišťovat kontrolu interní sítě,
- spolehlivě zálohovat informační systémy,
- zajistit kvalitu informací a služeb v souladu s legislativou a interní požadavky organizace.

Následky za porušení bezpečnostní politiky

Porušení zásad politiky bezpečnosti informací je chápáno jako bezpečnostní incident, a musí být řešen. Porušení zásad se musí analyzovat a přijímat účinná opatření a cílem je se učit z těchto událostí.

Dokument bezpečnostní politiky musí být schválen a projednán Radou města.

S dokumentem bezpečnostní politiky souvisí legislativa:

- zákon č. 101/2000 Sb., o ochraně osobních údajů,
- zákon č. 111/2009 Sb., o základních registrech.

Bezpečnostní komise

Bezpečnostní komise se skládá z tajemníka úřadu a vedoucího útvaru informatiky úřadu. Tato komise formuluje zásady bezpečnostní politiky, definuje bezpečnostní cíle a jejich zavádění, schvaluje hlavní kroky, které vedou ke zvýšení bezpečnosti dat a prostředků v informačním systému a schvaluje a podporuje iniciativy týkající se bezpečnosti informačních systémů. Dále také řeší disciplinární problémy vůči bezpečnosti, hodnotí účinnost bezpečnostní politiky, prosazuje, aby podpora bezpečnostní politiky ze strany vedení byla viditelná v celém úřadě.

4.5 SWOT Analýza

SWOT analýza slouží k posouzení připravenosti městského úřadu na daná rizika. Tato analýza z hlediska názvu znamená počáteční anglická slova: S – strenght jako silné stránky, W – weaknesses jako slabé stránky, O – opportunities jako příleţitosti a T – threats jako hrozby. SWOT analýza je organizačně snadná, levná a nevyžaduje žádné těžké výpočty a poskytuje rychlou odpověď.

Tabulka 2 – SWOT analýza [zdroj: vlastní]

	Silné stránky	Slabé stránky
Vnitřní prostředí	Zpracovaný dokument bezpečnostní politiky.	Nedostačující znalost bezpečnostní politiky.
	Vyčleněné finanční prostředky.	Orientace v dokumentu bezpečnostní politiky.
	Fungující městský úřad s odpovídajícím technickým vybavením.	Nedostačující fyzické zabezpečení městského úřadu.
	Vypracované postupy k řešení rizik.	Provádění analýzy rizik.
	Komunikace mezi organizačními složkami (vedení/oddělení).	

	Příležitosti	Ohrožení
Vnější prostředí	Zavedení kontroly na prověřovací cvičení pro zaměstnance.	Vyzrazení citlivých informací zaměstnancem.
	Zlepšení orientace v dokumentu bezpečnostní politiky.	Napadení hackery.
	Školení zaměstnanců městského úřadu.	Poškození informací živelnou pohromou.
		Nesprávné zacházení s informacemi, nebo jejich ztráta.
		Slabá hesla.

Tabulka 3 – SWOT analýza [zdroj: vlastní]

Silné stránky	**Váha**	**Hodnocení**	**Bilance**
Zpracování dokumentu bezpečnostní politiky.	0,3	5	1,5
Vyčleněné finanční prostředky.	0,2	4	0,8
Fungující MěÚ s odpovídajícím technickým vybavením.	0,2	4	0,8
Vypracované postupy k řešení rizik.	0,2	4	0,8
Komunikace mezi organizačními složkami.	0,1	4	0,4
Součet	**1**	**21**	**4,3**
Slabé stránky			
Nedostačující znalost bezpečnostní politiky.	0,3	-5	-1,5
Orientace v dokumentu bezpečnostní politiky.	0,3	-4	-1,2
Nedostačující fyzické zabezpečení MěÚ.	0,2	-2	-0,4
Provádění analýz rizik.	0,2	-3	-0,6
Součet	**1**	**-14**	**-3,7**
Příležitosti			
Zavedení kontroly na prověřovací cvičení pro zaměstnance.	0,3	4	1,2
Zlepšení orientace v dokumentu bezpečnostní politiky.	0,3	4	1,2
Školení zaměstnanců městského úřadu.	0,4	5	2
Součet	**1**	**13**	**4,4**
Ohrožení			
Vyzrazení citlivých informací zaměstnancem.	0,2	-4	-0,8
Napadení hackery.	0,1	-2	-0,2
Poškození informací živelnou pohromou.	0,2	-2	-0,4
Nesprávné zacházení s informacemi, nebo jejich ztráta.	0,2	-2	-0,4
Slabá hesla.	0,3	-5	-1,5
Součet	**1**	**-15**	**-3,3**

Vyhodnocení SWOT analýzy

Tabulka 4 – Vyhodnocení SWOT analýzy [zdroj: vlastní]

Vnitřní prostřední	0,6
Vnější prostředí	1,1
Celkem	**1,7**

Hodnoty SWOT analýzy jsou hodnoceny následovně:

- U silných stránek a příležitostí od 1 do 5, s tím, že 1 znamená nejnižší spokojenost, naopak 5 značí nejvyšší spokojenost.
- U slabých stránek a ohrožení od -1 do -5, s tím, že -1 znamená nejnižší nespokojenost, a naopak -5 nejvyšší nespokojenost.

Dále je hodnocena váha, kterou je vyjádřena důležitost jednotlivých problémů. Následně je vynásobena váha položky s hodnotou položky a vše se sečte. Poté jsou výsledné hodnoty vnějšího prostředí a vnitřního prostředí sečteny a vyjde nám výsledná hodnota bilance.

Při analýze bylo zjištěno, že je městský úřad dobře připraven na daná rizika. Vyplývá to také z celkové bilance, kde vnější část převládá nad vnitřní částí. Městský úřad by se měl více zaměřit na vnější rizika.

Silné stránky

K Silným stránkám městského úřadu patří dobře zpracovaný dokument bezpečnostní politiky. Tento dokument definuje základní strategie a zásady pro bezpečnost městského úřadu, určuje bezpečnostní pravidla pro používání a údržbu informací a informačních prostředků s cílem zajistit požadovanou úroveň ochrany informací. Dále jsou v dokumentu bezpečnostní politiky uvedeny směrnice, vyhlášky a zákony, kterými se musí zaměstnanci řídit. Mezi další Silné stránky patří vyčleněné finanční prostředky, odpovídající technické vybavení a dobrá komunikace mezi organizačními složkami (mezi vedením a odbory, či komunikace mezi jednotlivými odbory navzájem).

Slabé stránky

K Slabým stránkám městského úřadu patří neznalost zaměstnanců bezpečnostní politiky. Jak už je zmíněno, zaměstnanci se musí řídit směrnicemi a zákony, které by měla bezpečnostní politika obsahovat. Městský úřad musí dohlédnout nato, aby byli zaměstnanci v tomto ohledu dostatečně proškoleni a porušení zásad by mělo být řešeno. Mezi další Slabé stránky patří špatná orientace v dokumentu BP, provádění analýz rizik a nedostačují fyzické zabezpečení MěÚ, čímž je míněna např. absence vrátnice a vrátného, čímž by se zlepšila kontrola vstupu osob do budovy.

Příležitosti

U stránky Příležitostí je třeba věnovat největší pozornost položce školení zaměstnanců městského úřadu. Zaměstnanci by měli být řádně proškoleni o bezpečnosti informací v organizaci. Každý zaměstnanec by si měl být vědom, s jak citlivými informacemi pracuje a jak důležitá je bezpečnost těchto informací. Mezi další Příležitosti patří zavedení kontroly na prověřovací cvičení pro zaměstnance a zlepšení orientace v bezpečnostní politice.

Ohrožení

Hrozby, které mohou ohrožovat městský úřad, jsou zapříčiněné lidským, nebo přírodním faktorem. Větší pravděpodobnost je u hrozeb zapříčiněných lidským faktorem, ale je možné tyto hrozby eliminovat pomocí směrnic a zákonů. Mezi hrozby způsobené člověkem můžeme zařadit vyzrazení citlivých informací zaměstnancem, špatná volba hesla na pracovním počítači, nebo nesprávné zacházení s informacemi, či jejich poškození. Mezi hrozby způsobené živelnou pohromou můžeme řadit např. poškození informací způsobené požárem, povodněmi apod. Pravděpodobnost u hrozeb přírodního charakteru se eliminuje stěží, jelikož nelze přesně určit, kdy k hrozbě dojde.

ZÁVĚR

Cílem mé bakalářské práce bylo objasnění pojmů ochrany obyvatelstva a bezpečnosti informací a s ní související oblast informační bezpečnosti. V úvodní kapitole práce byly definovány základní pojmy, které jsou v práci zmiňovány.

V další části jsem se zabývala cílem bezpečnosti informací, prevencí a možnými důvody útoku. Bezpečné informace lze chápat jako ty informace, které splňují tři základní požadavky, tj. důvěrnost, integrita a dostupnost informací. Dále jsou popsány bezpečnostní mechanismy, které se používají k dosažení požadavků na informační bezpečnost.

Dále jsem popsala základní oblasti informační bezpečnosti, které je třeba zahrnout do bezpečnostní politiky a stanovit určité požadavky a pravidla. Při zpracování bezpečnostní politiky je nutno mít na zřeteli legislativní požadavky. V kapitole Bezpečnostní politika byl vysvětlen význam pojmu a dále popsány jednotlivé fáze tvorby, na základě kterých jsem vytvořila návrh bezpečnostní politiky pro městský úřad. Vychází se z aktuálního bezpečnostního stavu organizace a definují se klíčové oblasti, které se musí řešit. Pro správné vyhodnocení rizik je nutné pojmenovat hrozby, kterým jsou informace vystaveny.

Vyhodnocením stávajícího stavu bezpečnostních opatření v oblasti bezpečnosti informací v organizaci, byli zjištěny určité nedostatky a rizika, které organizaci hrozí. Hlavní rezervy byly nalezeny v nedostatečném školení zaměstnanců o informační bezpečnosti a v nezpracovaném dokumentu bezpečnostní politiky. Bakalářská práce slouží pouze jako informační materiál, tudíž žádné z uvedených doporučení nebylo aplikováno. Všechna rizika nemůžeme nikdy plně eliminovat, ale je důležité jejich zmírnění.

SEZNAM POUŽITÉ LITERATURY

[1] FEREBAUEROVÁ, Růžena a Oldřich PEKÁREK. *Aplikovaná informatika*. 1. České Budějovice: Vysoká škola evropských a regionálních studií, 2014. ISBN 978-80-87472-74-3.

[2] POŽÁR, J. *Informační bezpečnost*. 1. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

[3] ČSN ISO/IEC 17799 Informační technologie - Soubor postupů pro řízení informační bezpečnosti. Český normalizační institut. 2006

[4] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - v působnosti NÚKIB. Národní bezpečnostní úřad [online]. Praha, 2017 [cit. 2018-02-14]. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/1091-zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/

[5] Risk Analysis Consultans [online]. Praha: RCA, 2017 [cit. 2018-02-13]. Dostupné z: http://www.iso27000.cz/

[6] DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: Bezpečnost. 2. vydání. Praha: Computer Press, 2003. ISBN 80-7226-849-X.

[7] DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

[8] NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Praha [cit. 2018-02-04]. Dostupné z: https://www.govcert.cz/

[9] Personální bezpečnost. *Národní bezpečnostní úřad* [online]. Praha: NBÚ, 2015 [cit. 2018-02-11]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1043-obecne-k-personalni-bezpecnosti/

[10] Fyzická bezpečnost. *NBÚ* [online]. Praha: NBÚ, 2015 [cit. 2018-02-11]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/1014-informace/

[11] Průmyslová bezpečnost. *Národní bezpečnostní úřad* [online]. Praha: NBÚ, 2015 [cit. 2018-02-11]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-

informaci/prumyslova-bezpecnost-osvedceni-podnikatele-certifikaty/1061-obecne-k-prumyslove-bezpecnosti/

[12] STŘÍŽOVÁ, V. a kol. Organizace v podmínkách informační společnosti. Praha: Vysoká škola ekonomická v Praze, Nakladatelství Oeconomica, 2014. ISBN 978-80-245-2072-8.

[13] HANÁČEK, P, STAUDEK, J. Bezpečnost informačních systémů. 1 vyd. Praha: Úřad pro státní informační systém, 2000. 127 s. ISBN 80-238-5400-3.

[14] ČERMÁK, Miroslav. Clever and Smart. Bezpečnostní politika a související dokumenty. [online]. 2010 [cit. 2018-03-27]. Dostupné z: http://www.cleverandsmart.cz/bezpecnostni-politika-a-souvisejici-dokumenty/

[15] SMEJKAL, V, RAIS, K. Řízení rizik ve firmách a jiných organizacích. Praha: Grada, 2013. ISBN 978-80-247-4644-9.

[16] DOSEDĚL, Tomáš, Počítačová bezpečnost a ochrana dat, Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[17] HUB, Miloslav. Bezpečnost a ochrana informací v prostředí internetu. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

[18] Ochrana obyvatelstva a krizové řízení: skripta. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2015. ISBN 978-80-86466-62-0.

[19] KRATOCHVÍLOVÁ, Danuše, Danuše KRATOCHVÍLOVÁ ML. a Libor. Ochrana obyvatesltva. 2. aktualizované vydání. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2013. ISBN 978-80-7385-134-7.

[20] zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů

[21] ZEMAN, Petr a kolektiv. Česká bezpečnostní terminologie. 1.vyd. Brno: Masarykova univerzita. 2013, s. 12 13. ISBN 80-210-3037-2. 186 s.

[22] Bezpečnostní strategie ČR. Praha: Kolektiv autorů pod vedením Ministerstva zahraničních věcí ČR, 2015. ISBN 978-80-7441-005-5.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Apod. A podobně

Atd. A tak dál

BI Bezpečnost informací

BP Bezpečnostní politika

CD Kompaktní disk

CERT Computer Emergency Response Team

DVD Digitální víceúčelový disk

IS Informační systémy

ISMS Information Security Management Systém

IT Informační technologie

Např. Například

OS operační systém

SEZNAM OBRÁZKŮ

SEZNAM TABULEK