Stanovení požadavků na bezpečnost desktopových systémů a mobilních zařízení malé obce

Libor Janoušek

Bakalářská práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Libor Janoušek**
Osobní číslo:	**A14575**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Stanovení požadavků na bezpečnost desktopových systémů a mobilních zařízení malé obce**
Téma anglicky:	**Establishing the Safety Requirements of Desktop Systems and Mobile Devices in a Small Village**

Zásady pro vypracování:

1. **Proveďte literární rešerši oblasti specifických požadavků na bezpečnost informačních systémů malé obce.**
2. **Stanovte rizika, kterým jsou informační systémy vystaveny.**
3. **Vyberte možná opatření pro zvýšení úrovně bezpečnosti informačních technologií ve specifickém prostředí malé obce.**
4. **Navrhněte způsoby implementace, zdůvodněte význam jejich použití a dle možností uvedené realizujte.**
5. **Vyhodnoťte výsledky své práce s ohledem na její využitelnost v praxi.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 80-251-0106-1**
2. **DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.**
3. **KOCMAN, Rostislav a Jakub LOHNISKÝ. Jak se bránit virům, spamu, dialerům a spyware. Brno: CP Books, 2005. ISBN 80-251-0793-0**
4. **LACKO, Ľuboslav. Vývoj aplikací pro Android. Brno: Computer Press, 2015. ISBN 978-80-251-4347-6**
5. **LACKO, Luboslav. Osobní cloud pro domácí podnikání a malé firmy. Brno: Computer Press, 2012, 270 s. ISBN 978-80-251-3744-4**
6. **Moderní správa IT ve firmě. In: Http://www.businessit.cz/ [online]. Praha: Bispiral, 2011 [cit. 2016-12-20]. Dostupné z: http://www.businessit.cz/ebooks/moderni_sprava_IT_ve_firme.pdf**

Vedoucí bakalářské práce:	**prof. Mgr. Roman Jašek, Ph.D.** Ústav informatiky a umělé inteligence
Datum zadání bakalářské práce:	**20. července 2017**
Termín odevzdání bakalářské práce:	**29. srpna 2017**

Ve Zlíně dne 20. července 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

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

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Jméno, příjmení: Libor Janoušek

Název bakalářské práce: Stanovení požadavků na bezpečnost desktopových systému a mobilních zařízení malé obce

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 28. 8. 2017

.....
podpis diplomanta

ABSTRAKT

Předkládaná bakalářská práce se zabývá bezpečnostními riziky, kterým je informační systém malé obce vystaven, jejich analýzou a následným návrhem možných opatření pro zvýšení úrovně bezpečnosti informačních technologií ve specifickém prostředí malé obce. Práce se dále zabývá návrhem implementace doporučených opatření. Cílem této práce je seznámení s riziky, kterým je informační systém malé obce vystaven. Je důležité si uvědomit riziko vstupu neoprávněných osob do systému. Teoretická část seznámí čtenáře s úvodem do informační bezpečnosti a definicí základních pojmů z oblasti bezpečnosti a ochrany dat. Součástí je i legislativa týkající se informačních systémů veřejné správy. Praktická část definuje pojmy a doporučuje postupy a opatření pro zvýšení bezpečnosti informačního systému ve specifickém prostředí malé obce. V závěrečné části práce je provedena analýza Městského úřadu Veselí nad Moravou a Obecního úřadu Těmice.

Klíčová slova: informační systém, datová bezpečnost, analýza rizik, antivirové zabezpečení, fyzická bezpečnost

ABSTRACT

This bachelor work is concerned with security risks affecting the information system used by villages, its analysis and subsequent suggestions of possible measures increasing the level of information security in the specific area of villages. What is more, the thesis furthermore deals with implements of recommended security measures. The purpose of this bachelor thesis is to introduce the main risks affecting information systems of villages. It must be remembered that the risk of entry by an unauthorized person is very high. The theoretical part provides the reader with an insight into information security. Moreover, this part also defines basic terms in the field of data security and protection, including legislation of information systems used in public administration. The empirical part contains definitions of the aforementioned terms as well as recommended steps and preventive measures that help to increase information system security in the very specific area of villages. The last part of this work is dedicated to the analysis in the town halls Veselí nad Moravou and Těmice.

Keywords: Information system, data security, risk analysis, antivirus security, physical security

Děkuji vedoucímu své bakalářské práce panu prof. Mgr. Romanu Jaškovi, Ph.D. za jeho věnovaný čas, odborné rady a vedení bakalářské práce.

Také bych chtěl hlavně poděkovat starostovi obce Těmice, panu Karlu Královi, za ochotu a poskytnuté informace o procesech chodu informačního systému malé obce a v neposlední řadě své rodině, která mě podporovala po celou dobu studia.

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

OBSAH

ÚVOD

V dnešní době je bezpečnost čím dál více používané slovo. Informace jsou klíčovým zdrojem obecního úřadu. Pomocí informací můžeme provádět statistiky a dohledat spoustu jiných informací. Z tohoto důvodu vznikl informační systém. Kvalita informačního systému může být posuzována z mnoha různých pohledů. Jedním z nejdůležitějších požadavků informačního systému je kvalita zabezpečení informací, protože jakákoliv hrozba může mít negativní dopad na celkový chod systému a může tak způsobit nevyčíslitelné škody, které mohou vést až k zneužití dat a informací. Neustálý vývoj informačních technologií a větší množství informací, které je potřeba zpracovávat, znamená i rostoucí složitost informačních systému. Zavedení kvalitního informačního systému je v mnoha případech pro vedení obecního úřadu těžkým úkolem. Abychom zabránili hrozbám při zavádění informačního systému je dobré pro zavedení najmout specializovanou firmu. Všechny tyto technologie mohou správně fungovat, pokud jsou vytvořeny podmínky pro jejich správné zavedení a používání, hlavně personální používání.

Za cíl mé práce, která má název „Stanovení požadavků na bezpečnost desktopových systémů a mobilních zařízení malé obce“, považuji stanovení postupů bezpečnosti informačních systémů a mobilních aplikací. Tyto postupy stanovuji v oblasti malé obce, kde je důležité mít kvalitní informační systém, protože se zde pracuje neustále s informacemi.

Teoretická část je věnována dané problematice a definicím základních pojmů z oblasti bezpečnosti informačních systémů. Dále je zde popsána analýza rizik a pojmy, které se analýzy týkají. Nejdůležitější kapitolou této časti je ochrana dat, která je rozdělena na tři oblasti. První oblastí je fyzická bezpečnost, kde jsou definovány zejména přírodní katastrofy, které mohou informační systém ohrozit. Druhou oblastí je datová bezpečnost, kde jsou popsány nástroje pro zvýšení bezpečnosti dat. Poslední oblastí je personální bezpečnost, která je jednou z nejdůležitějších a bývá podceňovanou oblastí z hlediska bezpečnosti.

Praktická část obsahuje analýzu současného stavu Obecního úřadu Těmice. Podle analýzy jsou dále rozvinuty jednotlitvé postupy a doporučení pro bezpečnost informačního systému a informačních technologií. Většina definovaných situací se týká procesního zabezpečení informací a dat.

V závěrečné části práce je uvedeno srovnání Obecního úřadu Těmice s Městským úřadem Veselí nad Moravou.

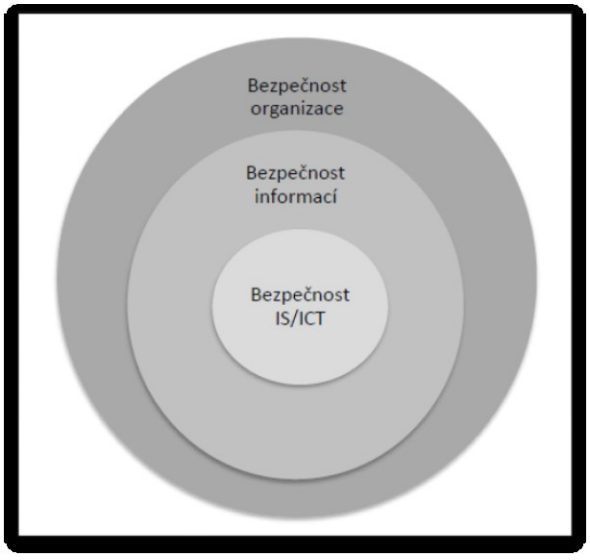
I. TEORETICKÁ ČÁST

1 ÚVOD BEZPEČNOSTI INFORMAČNÍCH SYSTÉMU

Informačním systémem obvykle rozumíme odpovídající ochranu informačního systému a informací, které jsou během jejich vstupu zpracovány, uloženy a přenášeny. Součástí bezpečnosti IS je i komunikační bezpečnost tj. ochrana informací přenášená mezi počítači, fyzická bezpečnost tj. ochrana před přírodními katastrofami a personální bezpečnost tj. ochrana před vnitřními útočníky. [1]

Informační systém je bezpečný, pokud je zajištěn fyzicky, administrativně, logicky, ale také technicky. IS musíme zabezpečit, protože se jedná o ochranu našich dat a informací. Základními požadavky na bezpečnost informačních systémů jsou:[1]

- **důvěrnost** – k údajům mají přístup pouze oprávněné osoby. Jedná se o ochranu před prozrazením informací,
- **integrita** – data, software a hardware můžou modifikovat pouze oprávněné osoby. Jedná se o ochranu přesnosti a úplnosti aktiv,
- **dostupnost** – data nebo služby jsou dostupná pouze oprávněným osobám v okamžiku, kdy ji potřebují. [3]



Obrázek 1: Vztah úrovní bezpečnosti v organizaci. [3]

Na obrázku č. 1 vidíme:

Bezpečnost IS/ICT chrání pouze aktiva, která jsou součástí informačního systému organizace podporovaného ICT. Z toho důvodu je bezpečnost IS/ICT nejužší a komplikovanou oblastí řízení bezpečnosti.

Informační bezpečnost je součástí bezpečnosti organizace. Cílem je řízení informační bezpečnosti a shrnout zásady bezpečné práce s informacemi. Oproti IS/ICT zahrnuje navíc způsob zpracování uložení a správu archivu nedigitálních dat, zásady skartace materiálu, nakládání s informacemi během transportu na jiná místa atd.

Bezpečnost organizace nebo firmy je nejvyšší kategorií bezpečnosti. Jedná se o zajištění bezpečnosti objektu, majetku organizace jako ostraha přístupu atd. Některé činnosti pomáhají k zajištění bezpečnosti IS/ICT jako např. fyzický přístup do budov. [48]

1.1 Základní princip bezpečnosti při použití IS

Informační systémy zpracovávají stále více informací s velkou hodnotou, které můžou být při jejich vstupu zpracovány, uloženy, přenášeny i prezentovány. Jedná se převážně o informace s důležitými hodnotami např.: zdravotní záznamy, daňová přiznání, bankovní účty, obchodní záměry atd. Abychom tyhle informace zabezpečili, musíme zajistit takovou ochranu, aby k těmto informacím měly přístup pouze oprávněné osoby, které zpracovávají nefalšované informace, aby bylo snadné zjistit, kdo tyhle informace vytvořil, změnil nebo odstranil a aby byly dostupné, když budou potřebné. [1]

1.2 Motivace zabezpečení IS

Organizace propojují informační a komunikační systémy na bázi IS jak uvnitř organizace (intranet), tak i s ostatními organizacemi (extranet). Díky tomu se organizace stávají velmi závislé na službách IS. Při ztrátě důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IS má na chod organizace nepříznivý dopad. Řešením je uplatnění zásad bezpečnosti IT. [1]

Informační systém může být neautorizovaný, a to může vést např. ke zničení systému nebo porušení soukromí jiných osob, nebo lze používat IS i oprávněnými zaměstnanci k nepracovní činnosti, ať již osobní, nebo výdělečné.[1]

Hlavními důvody pro zabezpečení informačního systému organizace patří následující body, které určují způsoby narušení bezpečnosti zpracovávání informací:

- narušení soukromí či utajení informací,
- vydávání se za jinou oprávněnou osobu a zneužíváním jejích privilegií,
- distancování se od odpovědnosti nebo od závazků plynoucích z manipulace s informacemi,

- tvrzení, že se nějaká informace někam poslala a toto se nikdy nestalo,
- tvrzení, že se informace získala od nějakého podvodníka,
- neoprávněné zvýšení svých privilegií přístupu k informacím,
- modifikací privilegií ostatních osob,
- zatajení výskytu důvěrné informace v jiných informacích,
- zjišťování, kdo a kdy si zpřístupňuje které informace,
- zařazení se jako skrytý mezičlánek v konverzaci jiných subjektů,
- pokažení funkcionality softwaru doplněním skrytých funkcí,
- narušení protokolu činností jiných subjektů zavedením nesprávných, nekorektních informací,
- podkopání důvěryhodnosti protokolu způsobenými zjevnými, byť možná jen zdánlivými – poruchami,
- bránění jiným uživatelům legitimně komunikovat.[1]

1.3 Základní pojmy z oblasti bezpečnosti IS

Informační systém je tvořen čtyřmi hlavními komponenty:

- **hardware** – technické vybavení počítače, např.: procesor, paměti,
- **software** – sada všech počítačových programů, které provádějí určitou činnost, např.: aplikační programy, operační systém,
- **data** – vyjádření informace tak, aby je bylo možné přenášet a zpracovávat počítačem, např.: data uložená v databázi, výstupní sestavy,
- **lidé** – jsou to uživatelé, personál a osoby, které pracují s IS.

Další pojmy a názvosloví:

- **aktivum** – jsou to všechny hmotné a nehmotné věci, které mají pro majitele nějakou hodnotu. Hmotná aktiva představují uživatelskou technologii, zejména výpočetní technikou. Nehmotná aktiva jsou programové vybavení a data, jako je operační systém, aplikační programy atd.,
- **autentizace** – jedná se o ověření identity uživatele,
- **autorizace** – jedná se o určitou činnost danou přístupovými daty a také příslušným oprávněním,

- **bezpečnostní analýza IS** – patří sem analýza rizik, hrozeb, které představují odbornou analýzu IS za účelem zjistit rizika a navrhnout vhodné protiopatření, aby byla zvýšena bezpečnost IS,
- **bezpečnostní audit** - nezávislé zkoumání systému zpracování dat a činností pro testování systémových kontrol. Cílem je zjistit zda kontroly jsou odpovídající a existuje shoda s bezpečnostní politikou.,
- **bezpečnostní incident** – jedná se o porušení bezpečnostních politik, zásad a pravidel provozu informační a komunikační technologie,
- **bezpečnostní politika** - soubor postupů pro řízení bezpečnosti informací,
- **citlivá data** – data, které vyžadují ochranu před zneužitím,
- **citlivé informace** – informace, které se musí chránit před neoprávněnou změnou, ztrátou nebo zničením,
- **dostupnost** - data nebo služby jsou dostupná pouze oprávněným osobám,
- **hrozba** – příčina nechtěného incidentu, kdy výsledkem může být poškození systému,
- **informační technologie** – veškerá technika, která zpracovává data a informace,
- **integrita** - jedná se o ochranu přesnosti a úplnosti aktiv,
- **ochrana aktiv** – zabezpečení aktiv před způsobením rizik,
- **protiopatření** - činnost, která chrání IS a jeho aktiva před určitou hrozbou,
- **riziko** - pravděpodobnost používání zranitelného místa IS,
- **útočník** – osoba, která se snaží nabourat do IS za účelem krádeže, poškození dat nebo celého systému,
- **zranitelnost** - slabina IS využitelná k útoku na informační systém. [23]

1.4 Zranitelné místo

Jedná se o slabinu IS využitelnou k útoku na informační systém a poté ke způsobení škod nebo ztrát. Zranitelná místa jsou důsledkem chyb, selhání analýz, v návrhu, popřípadě v implementaci IS, důsledek vysoké hustoty uložených informací, složitostí softwaru apod. [5]

Základními zranitelnými místy mohou být:

- **fyzická zranitelnost** – IS je snadno dostupný pro případný lidský útok např.: výpadek proudu,

- **přírodní zranitelnost** – IS se nemůže vyrovnat s přírodními faktory např.: blesk, záplava, zemětřesení,
- **fyzikální zranitelnost** – IS pracuje na fyzikálních principech, které mohou způsobit jejich zneužití např.: odposlech,
- **lidská zranitelnost** – způsobuje největší zranitelnost např.: nezaškolení zaměstnanci.

Zranitelná místa mohou vznikat jako důsledek selhání v návrhu nebo ve specifikaci požadavků. IS plní všechny funkce a vykazuje všechny bezpečnostní vlastnosti, které se po něm vyžadují, ale i přesto obsahuje zranitelná místa, díky kterým se stává z hlediska bezpečnosti nevhodným. [5]

Další zranitelná místa mohou vznikat při řešení nebo konstrukci. IS nesplňuje svoje požadavky, protože do něj byla zavlečena zranitelná místa použitím špatných standardů nebo nesprávným rozhodnutím pří jeho návrhu a implementaci. [5]

Zranitelné místo může vzniknout i při jeho používání. IS může být správně zkonstruován, ale zranitelná místa byla do něj zavlečena prostřednictvím nevhodných nástrojů.[5]

1.5 Hrozba a riziko

Zranitelná místa jsou vlastnostmi IS, jejichž výskyt způsobuje, že tato místa mohou být napadena mnoha různými vlivy a to může mít dopad na celkový chod systému. Hrozbou označujeme zranitelné místo IS, na kterém dochází k útoku a ke způsobení škod na aktivech. Hrozby rozdělujeme do dvou kategorií: objektivní a subjektivní. Do objektivní kategorie můžeme zařadit nepředvídatelné události týkající se například přírodních katastrof a s nimi související fyzické poškození např. požár, únik vody. Subjektivní hrozby plynou převážně z lidského faktoru. Dále je můžeme rozdělit na neúmyslné, např. způsobeno nezaškolením uživatele nebo správce, a na úmyslné, které můžeme charakterizovat vnějšími útočníky (špioni, teroristi, konkurenti, hackeři), ale i vnitřními útočníky (většina útoku na IS je vedena zevnitř, útočníkem, který může být propuštěn, vydírán anebo chamtivým zaměstnancem). Proto je velmi efektivní z hlediska vedení útoku součinnost obou typů útočníků. [6]

Hrozba je charakterizována zdrojem, který může být vnější nebo vnitřní, potenciálním útočníkem, frekvencí a kritičností uplatnění hrozby. K neoprávněnému přístupu k informacím může útočník využít např. škodlivý software. [6]

Existence hrozby představuje určité riziko. Riziko definuje pravděpodobnost používání zranitelného místa IS a charakterizuje pravděpodobnost výskytu bezpečnostního incidentu i potenciálně způsobenou škodu. Riziko nám tedy udává uplatnění s určitou mírou pravděpodobnosti.[1]

1.6 Útok

Útokem nazýváme bezpečnostní incident, při kterém dochází k úmyslnému použití zranitelného místa, tj. využití zranitelného místa ke způsobení škod nebo ztrát na aktivech IS. Při analýze rozeznáváme formy útoků a musíme je řešit podle typu problému. Měli bychom převážně řešit typy jako: jak se projevuje počítačová kriminalita, jaké jsou možné formy útoků, kdo útočí, kdo může páchat počítačový zločin, jaká rizika souvisí s používáním informačního systému a v neposlední řadě jak se chránit před útoky. Následně bychom měli řešit: jak útok detektovat, jak zjistit bezpečnostní incident, jak reagovat na útok, co dělat, když dojde k bezpečnostnímu incidentu. [6]

1.6.1 Druhy útoků

- **Útok opakováním** – jedná se o útok odposlechem mezi dvěma stranami, kdy útočník odposlouchává část komunikace a později ji zopakuje. Nejjednodušší příklad spočívá v odposlechu jedné zprávy,
- **Útok ze středu** – přítomnost útočníka je mezi oběma stranami a má tedy kontrolu nad celou komunikací. Princip spočívá v odposlechu a navazování spojení mezi oběma stranami A a B a to způsobem, že pro stranu A se identifikuje jako strana B a naopak,
- **Útok na hesla** – útočník získá uživatelské informace,
- **Útok na integritu zpráv** – souvisí s nedokonalým návrhem IS.[4]

Před odposlechem je vhodné se chránit formou prevence, kdy detekce odposlechu je velmi obtížná. Avšak absolutní prevenci útoků zajistit nelze, proto je typická ochrana zejména pro aktivní formy útoků založena na detekci útoků a následné obnově činnosti. Musíme si vzít také ponaučení ze zjištěných skutečností a získávané zkušenosti uplatnit při vylepšování ochrany. [1]

1.6.2 Kdo může útočit?

Útok lze provést z vnějšku, ale často se na informační systém útočí i z vnitřku.

- **amatéři, náhodný útočník** – objeví náhodně zranitelná místa při běžné práci, kdy se jedná o náhodné až často neúmyslné útoky. Tito útočníci nemají velké znalosti ani finanční prostředky. Proto proti nim stačí slabá bezpečnostní opatření,
- **hackeři** – provádí běžné útoky, kdy mají hodně znalostí, ale obvykle nemají vhodné příležitosti k útokům a mívají omezené finanční prostředky,
- **profesionální útočníci** – mají vysokou úroveň znalostí, obvykle disponují s dostatkem finančních prostředků i s dostatkem času k provedení útoku. [4]

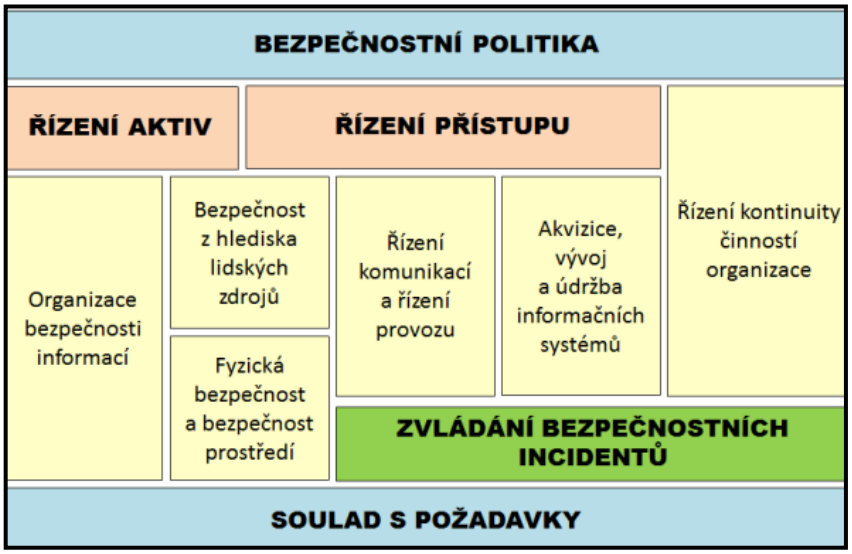
1.7 Bezpečnostní politika

Bezpečnostní politika je soubor postupů pro řízení bezpečnosti informací, který obsahuje nejlepší zkušenosti řízení bezpečnosti informací. Jedná se o normy ISO/IEC 27001:2005 a specificky ISO/IEC 27002:2005 a obsahuje 133 bezpečnostních norem opatření, které jsou rozděleny do 11 oblastí. Jedná se o dokument, který by neměl být statický, protože informační systém se čas od času mění a musíme tak čelit různým hrozbám a chránit jiná aktiva. Z toho plyne, že lepší bezpečnostní politika by se měla čas od času aktualizovat. Pro realizaci jsou definována dvě opatření. Prvním opatřením je dokument, ve kterém vedení organizace formuluje: [22]

- vyjádření cíle a význam bezpečnosti informací,
- upřesnění základních bezpečnostních zásad a pravidel,
- odpovědnost a pravomoc týkající se bezpečnosti informací v organizaci,
- vyjádření zájmu prohlubovat bezpečnost informací.[22]

Bezpečnostní politika musí obsahovat všechny principy, omezení, požadavky, pravidla a postupy.

Druhé opatření zajišťuje pravidelnou revizi. Dále by mělo obsahovat prohlášení týkající se: rozsahu, legislativní a regulační povinnosti, role a odpovědnosti, strategického přístupu a principu, přístup k řízení rizik. Tato politika musí být schválena nejvyšší organizační úrovní např. generálním ředitelem.[22]



Obrázek 2: Rozdělení bezpečnostní politiky. [22]

Na obrázku č. 2 vidíme charakteristiku jednotlivých kategorií:

- **bezpečnostní politika** – jak už bylo řečeno, jedná se dokument, který popisuje strategii zajišťující informační bezpečnost,
- **řízení aktiv** – stanovuje zásady fungování jak uvnitř organizace, tak i mimo ní,
- **řízení přístupu** – řídí přístup k aktivům,
- **organizace bezpečnosti informací** – definuje aktiva a důležitost ochrany,
- **bezpečnost lidských zdrojů** – zajišťuje bezpečnost informací lidských zdrojů např. školení zaměstnanců,
- **fyzická bezpečnost a bezpečnost prostředí** – provádí se zde ochrana pro zamezení přístupu neoprávněných osob,
- **řízení komunikace a řízní provozu** – zajištění bezpečného provozu pro zálohování dat a monitoring sítě,
- **nákup, vývoj a údržba IS** – dodržování bezpečnosti informací a pořizování nových informačních technologií,
- **řízení kontinuity činností organizace** – stanovení postupů pro zajištění nepřetržitého provozu organizace a opatření pro minimalizaci škod,
- **zvládání bezpečnostních incidentů** – pravidla pro hlášení bezpečnostních incidentů a postupů pro jejich opravu,
- **soulad s požadavky** – zajištění souladu s legislativními a smluvními závazky. [22]

2 INFORMAČNÍ SYSTÉM VEŘEJNÉ SPRÁVY

Jedná se o soubor informačních systémů, který veřejná správa používá pro výkon svých služeb.

2.1 Ministerstvo vnitra

Ministerstvo vnitra pomocí atestace dlouhodobého řízení ISVS, atestace způsobilosti k realizaci vazeb ISVS a prostřednictvím referenčního rozhraní uskutečňuje zpětnou vazbu na metodiky týkající se zákonu č. 365/2000 Sb., o ISVS, ve znění pozdějších předpisů a jejich následného dodržování v praxi. Dále omezuje vznik duplicit provozování ISVS pomocí projektového přístupu a zabezpečuje skutečné požadavky na čerpání financí z veřejného rozpočtu. Také připravuje technologické podmínky pro efektivnější výkon veřejné moci. [30]

2.2 e-Government

e-Governmentem se rozumí správa veřejných věcí, které využívají moderních elektronických nástrojů. Veřejná správa se tak stává občanům bližší, dostupnější, efektivnější, rychlejší a hlavně levnější. [25]

Budování e-Governmentu probíhalo v letech 2007 – 2013. Jako první vznikl Czech POINT, který je již dnes skoro v každé obci. Díky tomu mohou občané na jednom místě získat mnoho dokumentů, využít služby a tím ušetřit spoustu času. Poté byl spuštěn systém datových schránek, které zaručují elektronickou komunikaci se státem. Datové schránky nahradily klasické posílání obálek s popruhem. Vznikl také systém základních registrů, kde jsou uloženy aktuální platební údaje, které úředníci ve většině případů nemusí opakovaně žádat od občanů. [25]

Aby mohly tyto systémy fungovat, je důležité pro ně vytvořit bezpečnou infrastrukturu.

2.2.1 Czech POINT

Czech POINT je univerzální kontaktní místo veřejné správy, které poskytuje občanům ověřené výpisy z centrálních registrů, jako jsou rejstřík trestů, veřejný rejstřík nebo registr živnostenského podnikání. [26]

Služby Czech POINTU jsou dostupné na více než 7100 místech převážně v České republice.

Přehled nabízených služeb:

- Výpis z Katastru nemovitostí
- Výpis z Veřejného rejstříku
- Výpis z Rejstříku trestů
- Přijetí podání podle živnostenského zákona
- Výpis z bodového hodnocení řidiče
- Podání do registru účastníků provozu
- Datové schránky
- Centrální úložiště ověřovacích doložek
- Výpisy ze Základních registrů [26]

2.2.2 Datové schránky

Datové schránky slouží jako komunikační nástroje a nahrazují klasické doporučené dopisy. Pomocí nich můžeme komunikovat s orgány veřejné moci. Všechny úřady v České republice komunikují prostřednictvím datových schránek s každým, kdo ji má zřízenou. Datovou schránku musí mít povinně zřízenou orgány veřejné moci, právnické osoby, advokáti a daňoví poradci. Ostatní si ji můžou dobrovolně zřídit. [27]

Abychom nemuseli chodit pro obálky na poštu, můžeme si zdarma založit datovou schránku a komunikovat s úřady online. Datové schránky nám poskytují jistotu, že se naše zpráva dostala na správný úřad. Zprávu, kterou odešleme pomocí datové schránky, si můžeme uložit, abychom v případě potřeby mohli prokázat obsah zprávy. [27]

2.2.3 Základní registry

Základní registry jsou jeden ze základních pilířů e-Governmentu, které fungují od roku 2012 bez problémů. Díky nim se zrychlila a zjednodušila spousta agend, občané a firmy získali plnou kontrolu nad svými osobními údaji. K osobním údajům má přístup pouze zákonná oprávněná osoba. Každý přístup je zaznamenáván, takže jsou naše údaje pod důkladnou kontrolou. [28]

Rozdělení základních registrů:

- **registr osob** – obsahuje pouze základní údaje o subjektech, které mají IČO a také jejich provozovnách,

- **registr obyvatel** – obsahuje údaje o fyzických osobách, žijících na území České republiky. U fyzických osob eviduje jméno, příjmení, datum a místo narození, adresa trvalého bydliště, státní občanství, čísla dokladů a ID datové schránky,
- **registr práv a povinností** – obsahuje údaje o agendách a o přístupu oprávněných osob k údajům, které se nachází v ostatních registrech,
- **registr územní identifikace, adres a nemovitostí** – eviduje územní členění státu a obsahuje údaje o pozemcích, ulicích a katastrálních území. [28]

2.3 Legislativa

- **Zákon č. 365/2000 Sb., o informačních systémech veřejné správy**
  - zákon byl přijat dne 23. 10. 2000 a posléze novelizován zákonem č. 18/2012Sb.,
  - definuje práva a povinnosti správců ISVS a dalších osob, kteří se podílejí na vytváření, užívání a provozování informačních systémů veřejné správy,
  - vytváří podmínky, aby kvalitní informační systém byl co nejlepším nástrojem a pomocníkem pro výkon veřejné správy,
  - upravuje atestace a postavení atestačních středisek z důvodu doručování zpráv orgánům veřejné moci prostřednictvím portálu veřejné správy,
  - poskytuje ověřený výstup z informačního systému veřejné správy. [31]
- **Vyhláška č. 64/2008 Sb., uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením**
  - Vyhláška se týká přístupnosti a byla přijata dne 28. 2 2008
  - definuje povinnosti orgánů veřejné správy, aby informace, které se týkají veřejné správy, byly uveřejňovány tak, aby se k těmto informacím dostali i osoby se zdravotním postižením pomocí dálkového přístupu.[32]
- **Vyhláška č. 53/2007 Sb., o referenčním rozhraní**
  - přijata dne 22. 3. 2007,
- jedná se o stanovení technických a funkčních náležitostí, které se realizují mezi vazbami informačního systému veřejné správy prostřednictvím referenčního rozhraní ISVS. [33]

- **Vyhláška č. 52/2007 Sb., o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb ISVS prostřednictvím referenčního rozhraní**
  - přijata dne 22. 3. 2007
  - definuje postupy, díky kterým atestační střediska provádí posuzování způsobilosti a uskutečňují vazby ISVS na základě referenčního rozhraní.
  - posuzování se skládá ze zkoušky a poté se stanoví výsledek zkoušky. [34]
- **Vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení ISVS**
  - přijata dne 6. 12. 2006 a je podobná vyhlášce č. 52/2007 Sb.,
  - definuje postupy, které využívají atestační střediska k posuzování dlouhodobého řízení ISVS. [35]
- **Vyhláška č. 529/2006 Sb., o dlouhodobém řízení ISVS**
  - přijata dne 6. 12. 2006,
  - stanovuje postupy, které využívají orgány veřejné správy při vytváření, vydávání vyhodnocení a následně jejich dodržování,
  - také vytváří požadavky na bezpečný a kvalitní informační systém veřejné správy. [36]
- **Vyhláška č. 528/2006 Sb., o informačním systému o informačních systémech veřejné správy**
  - přijata dne 6. 12. 2006,
  - stanovuje technické náležitosti pro předání údajů do veřejného informačního systému,
  - systém obsahuje informace jako dostupnost a obsah zpřístupněných ISVS. [37]
- **Vyhláška č. 469/2006 Sb., o informačním systému o datových prvcích**
  - přijata dne 24. 10. 2006,
  - stejně jako vyhláška č. 528/2006 Sb., stanovuje technické náležitosti pro předání údajů do informačního systému,
  - definuje postupy Ministerstva informatiky a orgánů veřejné správy, které informační systémy využívají při vedení, zápisu a vyhlašování datových prvků. [38]

2.4 Atestace

Předmětem atestace je dlouhodobé řízení informačních systémů veřejné správy tak, jak ji stanovuje zákon č. 365/2000 Sb., o informačních systémech veřejné správy. Jedná se o informační koncepci, provozní dokumentaci a způsobilost k realizaci vazeb informačního systému veřejné správy s jinými informačními systémy, prostřednictvím referenčního rozhraní.[40]

Ministerstvo vnitra udělilo pověření k provádění atestací následujícím atestačním střediskům:

Atestační středisko	Pověření vydáno
RELSIE spol. s. r. o. Na stárce 1201/12 Praha 5 PSČ 150 00 IČ: 624 17 339	Na základě rozhodnutí č.j.: MV- 41547-7/OKK-2008 ze dne 28. května 2008 na období 5 let s podmínkou platného „Osvědčení o akreditaci". Na základě rozhodnutí č.j.: MV- 47689-10/OKK-2011 ze dne 26. dubna 2011 bylo prodlouženo období, na které bylo vydáno pověření k provádění atestací, o dalších 5 let. Na základě rozhodnutí č.j.: MV-66271-2/EG-2016 ze dne 29. dubna 2016 bylo vydáno pověření k provádění atestací na období 5 let s podmínkou platného „Osvědčení o akreditaci".
Elektrotechnický zkušební ústav, s. p. Pod Lisem 129 Praha 8 - Troja PSČ 171 02 IČ: 00001481	Na základě rozhodnutí č.j.: MV- 3629/11-OKK/2009 ze dne 27. ledna 2009 na období 5 let s podmínkou platného „Osvědčení o akreditaci". Na základě rozhodnutí č.j.: MV-13209-9/VEG-2014 ze dne 3. února 2014, s nabytím právní moci dne 21. února 2014, bylo vydáno pověření na období dalších 5 let s podmínkou platného „Osvědčení o akreditaci".
Equica, a. s. Rubeška 215/1 Praha 9 – Vysočany PSČ 190 00 IČ: 264 90 951	Na základě rozhodnutí č.j.: MV-132335-8/AEG-2011 ze dne 12. prosince 2011 na období 5 let s podmínkou platného „Osvědčení o akreditaci".
AYLLOR & COX s.r.o. Na Florenci 1055/35 Praha 1 - Nové město PSČ 110 00 IČ: 279 02 587	Na základě rozhodnutí č.j.: MV-109979-8/VEG-2013 ze dne 30. září 2013, s nabytím právní moci dne 18. října 2013, na období 5 let s podmínkou platného „Osvědčení o akreditaci

Obrázek 3: Atestační střediska. [41]

V obrázku č. 3 jsou uvedena atestační střediska s pověřením, které každé atestační středisko v určitém rozsahu vydává. Se společností RELSIE s. r. o. pracuje i laboratoř penetračních testů Fakulta aplikované informatiky.

2.5 Akreditace

Ministerstvo vnitra vydává povolení k provádění akreditací právnické osobě, která je členem mezinárodních sdružení zabývajících se akreditací a splňuje podmínky podle zákona 365/2000 Sb., o ISVS. [42]

Od roku 2007 provádí akreditaci Český institut pro akreditaci, o. p. s. Český institut pro akreditaci je národní akreditační orgán založený vládou České republiky, který poskytuje služby v souladu s platnými právními předpisy ve všech oblastech, jak státních, tak privátních. V souladu s požadavky mezinárodních norem a dokumentů ČIA provádí nestranné, objektivní a nezávislé posouzení způsobilosti pro:

- Zkušební laboratoře (ČSN EN ISO/IEC 17025:2005)
- Zdravotnické laboratoře (ČSN EN ISO 15189:2013)
- Kalibrační laboratoře (ČSN EN ISO/IEC 17025:2005)
- Certifikační orgány provádějící certifikaci systémů jakosti, systémů environmentálního managementu, systémů managementu bezpečnosti a ochrany zdraví při práci, systémů managementu bezpečnosti informací, systémů managementu bezpečnosti potravin a systému trvale udržitelného hospodaření v lesích (ČSN EN ISO/IEC 17021:2011, ČSN EN ISO/IEC 17021-1:2016)
- Certifikační orgány certifikující produkty (ČSN EN ISO/IEC 17065:2013)
- Ověřovatelé emisí skleníkových plynů (ČSN EN ISO 14065:2013, nařízení Komise (EU) č. 600/2012)
- Certifikační orgány provádějící certifikaci osob (ČSN EN ISO/IEC 17024:2013)
- Inspekční orgány (ČSN EN ISO/IEC 17020:2012)
- Poskytovatele zkoušení způsobilosti (ČSN EN ISO/IEC 17043:2010)
- Environmentální ověřovatele programů EMAS a dohled nad zahraničními environmentálními ověřovateli (nařízení ES č. 1221/2009)
- Výrobce referenčních materiálů (ČSN EN ISO/IEC 17025:2005 a TNI Pokyn ISO 34:2013).[43]

2.6 Informační systém o datových prvcích

Aplikace poskytuje oficiální informace o datových prvcích ISVS a také slouží k poskytnutí datových prvků a zveřejňování číselníků. Poskytnuté datové prvky v ISDP jsou pro orgány

veřejné správy a vazby jejich informačních systémů závazné. Systém byl vyvinut podle zákona č. 365/2000 Sb., o ISVS a vyhláškou Ministerstva informatiky ČR č. 469/2006 Sb. o informačním systému, o datových prvcích. Tento systém je provozován od 1. ledna 2007. [44]

V ISDP existují role:

- **průzkumník** – je automaticky přihlášen do ISDP po spuštění aplikace. Může vytvářet a podávat náměty, vyhledávat vyhlášené datové prvky, využívat XML schémata a PDF dokumentaci k vyhlášeným datovým slovníkům,
- **komentátor** – je přihlášen podepsáním věty na vstupu, s využitím zaručeného elektronického podpisu. Může vytvářet a podávat náměty, podněty na zápis, změnu datového prvku,
- **osoby jednající za správce -** je přihlášen podepsáním věty na vstupu, s využitím zaručeného elektronického podpisu. Zapisuje ke všem podnětům stanovisko, na základě kterého se administrátor ISDP rozhoduje o vyhlášení nebo nevyhlášení podnětu OS,
- **osoby jednající za správce číselníku -** je přihlášen podepsáním věty na vstupu, s využitím zaručeného elektronického podpisu. Zodpovídá za správu číselníků pro jednoduché datové prvky a může připravovat nové číselníky.

Pro výkon všech uživatelských rolí, kromě role průzkumníka, je potřeba se do ISDP přihlásit za použití kvalifikovaného certifikátu (QC), vydaného akreditovaným poskytovatelem certifikačních služeb podle zákona č. 227/2000 Sb., o elektronickém podpisu.[44]

2.7 Informační systém o informačních systémech veřejné správy

Aplikace slouží k poskytnutí informací o ISVS. Jedná se o základní informace jako informace o ISVS a dostupnosti ISVS. Systém byl vytvořen podle zákona č. 365/2000 Sb., o ISVS a vyhláškou Ministerstva informatiky č. 528/2006 Sb. Systém je provozován od 1. ledna 2007. V IS o ISVS lze vkládat záznamy o nových ISVS, měnit záznamy ISVS nebo vkládat záznamy o ukončení činnosti ISVS.[45]

V IS o ISVS existují role:

- **průzkumník –** nemá právo vkládat do IS o ISVS záznamy a je pouze oprávněn číst záznamy vložené ostatními uživateli a tvořit vstupní sestavy

- **osoby jednající za správce –** do systému se přihlašuje pomocí kvalifikovaného certifikátu (QC). Uživatel má právo vkládat záznamy o nových ISVS, měnit záznamy ISVS a vkládat záznamy o ukončení činnosti ISVS. Nový záznam uživatel vyplní, podepíše kvalifikovaným certifikátem (QC) a předloží administrátorovi.
- **administrátor –** je pracovník Ministerstva informatiky, který má za úkol kontrolu předložených záznamů. Po kontrole může zveřejnit záznam o nové, změněné, ukončené činnosti ISVS, nebo záznam vrátí osobě jednající za správce k dopracování. [45]

2.8 Kybernetické bezpečnosti

Od 1. ledna 2015 nabyl zákon č. 181/2014 Sb., o kybernetické bezpečnosti účinnosti. Zákon sjednává práva a povinnosti osob týkající se v oblasti kybernetické bezpečnosti. Také dne 1. ledna 2015 nabyla vyhláška č. 315/2014 Sb. účinnost. Tahle vyhláška stanovuje bezpečnostní incidenty a relativní opatření v oblasti kybernetické bezpečnosti. Předmětem vyhlášky je stanovení obsahu a struktury bezpečnostní dokumentace pro IS. Vyhláška také definuje bezpečnostní opatření týkající se rozsahu, typu a kategorie bezpečnostních incidentů. [24]

V oblasti kybernetické bezpečnosti se nachází orgány a osoby, které jsou zodpovědné za kybernetickou bezpečnost. Těmito orgány a osobami jsou:

- poskytovatel služeb elektronických komunikací,
- osoba zajišťující síť,
- správce kritické informační infrastruktury,
- správce významného IS. [24]

Správci informačního, komunikačního a významného IS musí zajistit odborné školení osob, které provozují bezpečnostní role. Školení by se mělo provádět při přijetí zaměstnance do pracovního poměru, tzn. vstupní školení a poté v určitých cyklech tzn. pravidelná školení. [24]

Správce kritické informační infrastruktury a správce komunikačního systému kritické informační infrastruktury musí určit bezpečností role. [24]

Bezpečností role se rozdělují:

- **manažer kybernetické bezpečnosti –** odpovídá za systém řízení bezpečnosti, v praxi se jedná o mezistupeň mezi nejvyšším vedením a základní úrovní tzn. operativní úrovní,
- **architekt kybernetické bezpečnosti –** zajišťuje návrhy a implementaci bezpečnostních opatření,
- **auditor kybernetické bezpečnosti –** jedná se o osobu, která provádí audit kybernetické bezpečnosti. Tato osoba musí být nestranná a má fyzickou odpovědnost za rozvoj, použití a bezpečnostní aktiva,
- **garant aktiva –** jedná se o fyzickou osobu, kterou pověří organizace za účelem rozvoje, použití a zajištění důvěrnosti, dostupnosti a integrity aktiv. [24]

2.8.1 Pojmy kybernetické bezpečnosti

- **Kybernetický prostor** – virtuální oblast, kde pracují a komunikují informační systémy prostřednictvím elektronických komunikací, jednotlivá PC i PC sítě. Jsou zde zpracovány a vyměňovány informace a ukládána, sdílena nebo přenášena data v elektronické podobě.
- **Kritická informační infrastruktura** – rozšíření kritické infrastruktury, tak jak ji definuje vláda a krizový zákon. Pojem „informační“ se týká informačních a komunikačních systémů. Poškodit kritickou informační infrastrukturu může mít zásadní dopad např. na bezpečnost státu.
- **Významný informační systém** – má zásadní význam pro fungování veřejné správy (podle stávající vyhlášky např. informační systém základních registrů, samotné základní registry, informační systém datových schránek). Konkrétní systémy budou definovány připravovanou vyhláškou podle Ministerstva vnitra.
- **Významná síť** – jde o systémy, zařízení a další prostředky určené pro přenos signálu, bez ohledu na druh přenášené informace pomocí kybernetického prostoru.
- **Správce informačního a komunikačního systému** – jedná se o způsob zpracování informací a podmínky pro provozování informačního systému, jak to stanovuje zákon.
- **Bezpečnostní opatření** – bezpečnostní opatření se dělí do dvou skupin: technické a organizační. Cílem je eliminovat hrozby, kterými jsou ohroženy informační systémy. [46]

2.8.2 Legislativa týkající se kybernetické bezpečnosti

- **Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti**
  - přijata dne 15. 12. 2014,
  - vyhláška definuje obsah bezpečnostních opatření a strukturu bezpečnostních dokumentací pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém.
- **Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích**
- přijata dne 15. 12. 2014,
- vyhláška stanovuje kritéria pro významné informační systémy
- kritéria se člení na dopadová určující kritéria a oblastní určující kritéria,
- dopadovým kritériem je skutečnost, že úplná nebo částečná nefunkčnost informačního systému způsobena narušením bezpečnosti informací by mohla mít negativní vliv na fungování orgánu veřejné moci.[46]

3 ANALÝZA RIZIK

Jedná se o nejdůležitější etapu stanovení bezpečnostní politiky. Cílem analýzy rizik je:

- identifikování a odstranění událostí, které mají nežádoucí vlivy na aktiva,
- zjištění hrozeb a rizik, kterým je informační systém vystaven,
- určit, jaké škody mohou vzniknout při útoku,
- určit, která opatření mohou rizika odstranit nebo částečně minimalizovat.[1]

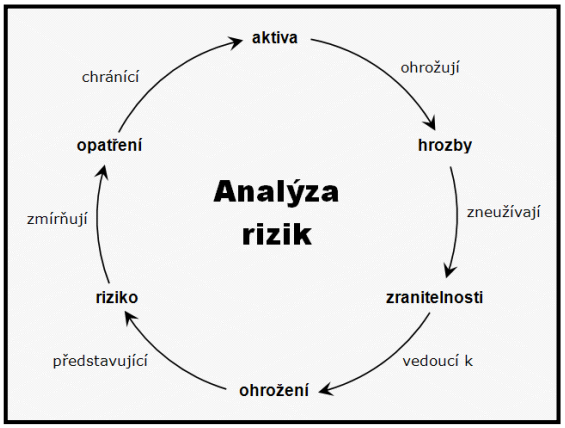
Při tvorbě vlastní bezpečnostní politiky musí být provedena analýza rizik, tedy musíme zjistit, co chceme chránit. Analýza rizik nám definuje hrozby, jakým je společnost vystavena, jaká je pravděpodobnost zneužití a jaký to bude mít dopad na společnost. [7]

3.1 Pojmy analýzy rizik

Zmíněné pojmy jsou popsány v předešlé kapitole, zde si je pouze vyjmenujeme, stručně popíšeme a doplníme o definici aktiv.

Pojmy, které se v analýze rizik používají:

- **aktivum** – je hmotný a nehmotný majetek, který má pro organizaci nějakou hodnotu. Aktivum by mělo být určitým způsobem chráněno před hrozbami, které je mohou měnit,
- **hrozba –** zranitelné místo IS, na které dochází k útoku a ke způsobení škod na aktivech,
- **zranitelnost** – slabina IS využitelná k útoku na informační systém a poté ke způsobení škod nebo ztrát,
- **riziko** – pravděpodobnost používání zranitelného místa IS a charakterizuje pravděpodobnost výskytu bezpečnostního incidentu i potenciálně způsobenou škodu,
- **opatření** – je vše, co bylo navrženo pro eliminování hrozeb, případně jejich zmírnění. [7]



Obrázek 3: Analýza rizik. [7]

Na obrázku č. 3 vidíme analýzu rizik. Musíme si uvědomit rozdíl mezi hrozbou a rizikem. Hrozby zneužívají zranitelnosti IS vedoucí k ohrožení, což je riziko, které zmírníme opatřeními a chráníme tak aktiva před působením hrozeb. [7]

Analýza rizik se skládá z několika fází: identifikace a kvalifikace aktiv, hrozeb, zranitelností a stanovení výsledného rizika za účelem vhodného opatření. V každé z těchto fází musíme provést následující kroky, které na sebe navazují:

- **identifikace respondentů** – osoby, na které se budeme obracet s žádostí o poskytnutí informací a se kterými budeme komunikovat,
- **získání informací** – zde budeme získávat informace od respondentů formou dotazníků,
- **analýza informací** – musíme analyzovat informace, které jsme získali,
- **interpretace informací** – jakmile jsme informace získali a poté analyzovali, musíme je pro respondenta srozumitelně interpretovat,
- **pravost informací** – pravdivost odpovědí bychom si měli nechat schválit jednotlivými respondenty,
- **dokumentace informací** – jediné co zákazníkovi zůstane, je dokumentace.[7]

V případě, že se jedná o vlastní analýzu, můžeme ji provést čtyřmi různými způsoby. První způsob se nazývá základní přístup, kdy jsou vybrány a realizovány základní nástroje opatření. Druhý způsob je neformální přístup, kdy se provádí orientační analýza rizik, která je založená na zkušenostech expertů. Také se zde vyhodnocují možné scénáře. Třetí formální způsob je založen na detailním provedení analýzy za účelem provedení hodnocení aktiv, hrozeb a zranitelností. Poslední přístup je kombinovaný, kdy se provádí orientační analýza, ale v případě identifikování hrozby se provede detailní analýza rizik. [7]

3.2 Škodlivý software

V souvislosti se škodlivým softwarem si většina uživatelů představí virus. Virus je schopen vlastní replikace, tedy množení a infikaci dalších systémů bez vědomí uživatele. Je zejména určen pro způsobování co největších škod a jeho hlavním úkolem je mazání. Virus se nejčastěji připojuje ke spustitelnému souboru. Jakmile se virus v počítači zdržuje delší dobu a rozšíří se, je jeho odstranění poměrně náročné. Počítač, který je napaden virem se projevuje např. zpomalením nebo zhroucením systému, snížením výkonu, zmenšením volného místa na disku, mazáním souborů, přeformátováním disků atd. [8]

V dnešní době se počítačový virus příliš často nevyskytuje. Mnohem častěji se vyskytují následující druhy škodlivého softwaru.

3.2.1 Trojský kůň

Je to počítačový program, který se jeví jako běžný uživatelský software, ale místo toho naruší celkové zabezpečení sytému. Trojský kůň se šíří tak, že uživatelé důvěřují určitému programu, protože si myslí, že pochází z legálního zdroje. Trojský kůň se na rozdíl od počítačového viru liší tím, že není schopen replikace a nepřipojí se ani k hostitelskému souboru. Nejčastěji se vyskytuje v jednom samostatném souboru. Často se vyskytuje v crackovacích programech. [8]

3.2.2 Adware

Adware se dostává do počítače legálně s naším souhlasem. Dostává se do počítače pomocí freewarových nebo sharewarových programů. Typickým příznakem jsou „vyskakující“ pop-up reklamní okna během surfování, společně s vnucováním stránek, o které nemá uživatel zájem. Pro ochranu můžeme použít některý z doplňků blokování reklam. [8]

3.2.3 Backdoor

Jedná se o speciální skupinu trojských koní, které vstupují do počítače a uživatel není schopen jejich vstup vypozorovat. Backdoors vyčekávají do chvíle, kdy se útočník připojí na PC. Poté s tímto počítačem můžou provádět prakticky vše, např. mazat soubory, snadno získávat data atd. Jako obranu proti backdoor je pochopitelně kvalitní antivirový program, ale také je důležité nespouštět programy, o kterých nevíme, co obsahují. [8]

3.2.4 Červ

Červ je situován tak, aby kopíroval sám sebe z jednoho počítače do druhého a to automaticky. Díky internetu se může sám aktualizovat a tím se může dále během síření zlepšovat. Nejdříve přejímá kontrolu nad funkcemi počítače, které mohou přenášet soubory a informace. Poté, jak je zaveden v systému, se může přenášet samostatně. Červ se dostává do počítače většinou elektronickou poštou jako je e-mail. Pokud odešle červ kopii sebe sama všem uživatelům v e-mailovém adresáři, může to mít dominantní efekt na zpomalení sítě a Internetu jako celek. Červ se vyskytuje převážně v příloze e-mailové zprávy. [9]

3.2.5 Spyware

Spyware je program, který sleduje, shromažďuje a odesílá informace o napadeném počítači bez vědomí uživatele. Na rozdíl od backdooru jsou odcizovány pouze „statistická“ data jako např. přehled navštívených stránek nebo nainstalovaných programů atd. Tahle činnost je odůvodněna snahou zjistit potřeby uživatele a tyto informace pak využít pro cílenou reklamu. Spyware se může šířit společně s několika sharewarovými programy a jejich autoři o této skutečnosti vědí. Naštěstí v počítači nedochází k jeho rozmnožení a uložená data nijak nepoškozuje. [9]

4 OCHRANA DAT

V dnešní době téměř všichni uživatelé nebo firmy používají ke své práci počítače a proto mají svá data uložena v podobě počítačových souborů na disku. Uložená data musíme chránit před zničením a zneužitím. Tuto část bychom neměli nijak podceňovat, protože uložená data jsou důležitá, abychom mohli naši práci provádět efektivně.

Z hlediska bezpečnosti ochrany dat rozlišujeme fyzickou bezpečnost, datovou bezpečnost a personální bezpečnost, které si dále charakterizujeme.

4.1 Fyzická bezpečnost

Fyzická bezpečnost ochrany dat před neoprávněnými osobami. Pokud neoprávněná osoba má fyzický přístup k nosičům, na kterých jsou uložena data, pak může tato data zničit. V oblasti fyzické bezpečnosti musíme chránit data také před přírodními katastrofami.[4]

4.1.1 Fyzický přístup

Už při vstupu do budovy by se měla provádět kontrola, zda může osoba vstoupit do budovy. Tato kontrola bývá obvykle zajištěna vrátným, který kontroluje vstup osob do objektu. Dále může být tato kontrola zajištěna v podobě automatického dveřního systému, který je založen na principu čipových karet. Důležité je vědět, jaká osoba se v objektu pohybuje. Abychom zvýšili bezpečnost, je dobré po budově rozmístit snímače pohybu a kamery. Díky takovému opatření budeme vědět o všem, co se bude v budově provádět.[4]

Zapomínat by se hlavně nemělo na to, v jakých místnostech jsou umístěny servery a běžné počítače. Servery mohou být umístěny za železnými dveřmi bez oken. Pro zvýšení kontroly je vhodné na určité dveře nainstalovat čtečky čipových karet. Tím docílíme, že budeme mít přehled, kdo například vstupuje do místnosti se servery.[4]

4.1.2 Přírodní katastrofy

Mezi přírodní katastrofy se řadí požáry, zemětřesení a voda. Tyto katastrofy nemůžeme předem předvídat.

Požáry

Požáry jsou velmi nebezpečné, jak pro lidi, tak i pro techniku. Proto důležitá data by měla být uložena v protipožárních skříních, které by ještě pro zvýšení bezpečnosti měly být vo-

dotěsné. Budova by měla vždy obsahovat protipožární opatření, mezi která patří hasicí přístroje a systémy. [4]

Zemětřesení

Při zemětřesení dochází k pádu budov a následnému zasypání disků, na kterých máme uloženy data. Důležitým opatřením je odolnost proti prachu a také skříň, ve které je disk nainstalován. Proti lehkým zemětřesením bude stačit pevné upevnění disku i skříně počítače, tím se zabrání pádu nebo nárazu. [4]

Voda

Důležitým faktorem před záplavami je dobrá poloha a instalace serverů v horních patrech budov. Místnosti, ve kterých jsou umístěny servery, by měly být izolovány. Neměly by se zde vyskytovat žádné kanály ani potrubí. Izolovat by se měly i počítačové skříně, ve kterých jsou disky s daty umístěny. [4]

4.2 Datová bezpečnost

4.2.1 Firewall

Firewall je technické vybavení, kterému se někdy říká také „ vstupní brána “, která slouží pro komunikaci mezi sítěmi, popřípadě mezi počítačem a sítí. Hlavní funkcí firewallu je bezpečnost dat vstupující směrem ven a směrem dovnitř. Také brání před neoprávněnými průniky do sítě. Principem je povolení komunikace, která je pro nás potřebná, a zároveň zakázání ostatních komunikací. [8]

Filtrující pakety zkoumají každou hlavičku a používají informace pro rozhodnutí, zda paket přijmout či odmítnou bez oznámení. Pokud paket příjme, směřuje jej k cíli a zabezpečuje komunikaci podle poskytnutých informací v hlavičce každého paketu. Výhoda filtrování paketů spočívá v rychlosti filtrování a průhlednosti, kdy zavedení nevyžaduje žádnou změnu v chování uživatele. Nevýhodou je nedůvěryhodné a důvěryhodné spojení hostitele, které je povoleno přímým spojením.[17]

Aplikační brány rozhodují o přístupu podle informací, které jsou uvnitř paketu ve všech vrstvách modelu OSI. Oproti filtrujícím paketům poskytuje vyšší úroveň zabezpečení. Brána vystupuje jako prostředek pro aplikace jako elektronická pošta, FTP, Telnet, http. To že firewall o aplikaci ví, znamená, že může provádět důkladnější ověření komunikace oproti filtrujícímu paketu. Brána aplikací ověřuje data, jestli jsou v přijatelném formátu,

může provádět rozšířené ověření a rozsáhlé protokolování informací. Mezi výhody zde patří značná úroveň zabezpečení, která je ovšem vykoupena vysokou náročností na použití hardware.[17]

Stavové paketové filtry povolují a zamítají pakety podle sady pravidel, které se podobají filtrujícím paketům. Brána, která je schopná kontrolovat stav se rozhoduje nejen podle IP adres a portů, ale také podle informací, které se nachází v hlavičce TCP. Firewall sleduje stav každé relace a může otevírat nebo zavírat porty příslušných požadavků dané relace. Kontrola stavu paketů byla vyvinuta za účelem rychlosti a flexibility filtrů paketů a zabezpečení úrovní aplikace na proxy serveru. Stavové paketové filtry nejsou tak rychlé jako filtrující pakety a nenabízí úroveň znalosti aplikace jako aplikační brána. Hlavní výhodou oproti filtrujícím paketům je schopnost nahlížet do dat určitého typu paketů. [17]

4.2.2 Autentizace a autorizace

Autentizace slouží k jednoznačnému určení uživatele, který přistupuje k systému. Cílem je zajistit jednoznačnou identifikaci uživatele, aby systém přesně věděl, s kým komunikuje. Aby byla zajištěna bezpečnost systému, měl by každý systém podporovat autentizaci uživatele. To se docílí pomocí mechanismů systému v podobě databázového serveru. V databázi jsou uložení uživatelé, kteří mají heslo, které je šifrováno. Uživatel se pak přihlašuje do systému pomocí svého uživatelského jména a hesla. Kromě toho můžou být k autentizaci i použity speciální aplikace, hardwarové zařízení nebo služby OS. [10]

Administrátor neboli bezpečnostní správce má možnost oprávnění pro připojení k systému přidělit, ale také může připojení odebrat a časově omezit v podobě počtu přihlášení za měsíc nebo omezit jeho platnost. Systém, který umožňuje definovat akce, které se mají vykonat, pokud nebudou splněny podmínky autentizace např. kontaktovat administrátora zasláním elektronické pošty, zablokovat uživatelský účet nebo odebrat oprávnění přístupu k citlivým datům. Nemělo by chybět vygenerování záznamu v podobě sledovacích protokolů z důvodu případného porušení bezpečnostních mechanismů. [10]

Navazující proces na autentizaci je autorizace, kdy jde o proces ověření přístupových oprávnění uživatele vstupující do informačního systému. Autorizace ověřuje konkrétního uživatele, zda má oprávnění provést určitou akci. Oprávnění na provedení určitých akcí jsou rozdělena mezi více uživatelů: mezi administrátory a běžné uživatele. [10]

4.2.3 Antivirový software

Antivirový program slouží k identifikaci, eliminaci a odstraňování počítačových virů nebo jiného škodlivého programu, kterým se říká malware. Antivirový program musí být stále zapnutý, aby hlídal a kontroloval správnost prováděných operací. Mezi nejzákladnějšími operacemi antivirových programů by nemělo chybět vyhledávání a skenování virů, analýza a kontrola integrity. Pro mnoho uživatelů je také důležitá cena těchto programů. U komerčních produktů platí, že nabízí vyšší úroveň zabezpečení a poskytování služeb. I přesto, jestli máme komerční nebo volně stažitelný antivirový program, nesmíme zapomínat na pravidelnou kontrolu počítače, stahovaných dat z internetu a veškerá data, které do počítače vkládáme.[11]

Jednoúčelové antiviry jsou určeny pro detekci, popřípadě i odstranění jednoho konkrétního viru nebo menší skupiny virů. Tyto antiviry nelze používat jako plnohodnotnou antivirovou ochranu. V případě, že uživatel zjistí, že jeho počítač je nakažen určitým virem, není nic jednoduššího, než využít jednoúčelové antiviry, které jsou obvykle zdarma. [11]

On-demand skener je nabízen některými společnostmi zdarma, popřípadě jako shareware. Spouštějí se přes OS DOS ovládané přes příkazový řádek a jsou určeny pro případ, že systém MS Windows není schopen provozu. [11]

Antivirové systémy mají za úkol chránit počítač před všemi škodlivými viry, jako jsou např. červi, trojský kůň atd. Jedná se tedy o komplexní řešení, které může být doplněno o osobní firewall a další specializované nástroje. [11]

4.2.4 Zálohování a archivace

Zálohování je proces, při němž vzniká kopie zdrojových dat. Kopie zdrojových dat bývá obvykle uložena na jiném místě, než se nachází zdrojová data. Při zálohování je kladen důraz na rychlou obnovu dat. Zálohují se data, která slouží převážně ke každodennímu použití. Proto je výhodné ukládat data na diskové pole, které jsou mnohem rychlejší než páskové mechaniky.

Oproti zálohování je archivace, kdy není kladen důraz na rychlou obnovu dat. Archivují se data, která nejsou pro každodenní použití, ale pro dlouhodobé uložení. Zde mohou být data uložena i na páskové mechaniky z důvodu, že není kladen důraz na obnovu dat.

Typy záloh:

- **nestrukturovaná** – jedná se o nejjednodušší způsob zálohování, který však není u větších firem oblíben. Úložištěm může být např. diskety, CD, DVD,
- **úplná + inkrementální** – nejprve se provede úplná záloha dat a poté je provedena inkrementální záloha, kdy se zálohují pouze soubory, které se změnili od předešlé zálohy. Tato záloha má za cíl vytvořit více kopií zálohovaných dat,
- **úplná + rozdílová** – nejprve se provede úplná záloha jako u předešlého typu a poté každá záloha zachytí všechny soubory, které jsou nově vytvořené nebo změněné od vytvoření úplné zálohy. Výhodou je, že se obnovuje pouze poslední úplná záloha a posléze její překrytí poslední rozdílovou zálohou,
- **zrcadlová + rezervně přírůstková** – tato záloha obsahuje reflektující stav po poslední záloze a také historii přírůstkové zálohy. I zde máme k dispozici neustále aktuální plnou zálohu a ukládáme pouze historii změn. Zálohování se automaticky promítá do zrcadla a změněné soubory jsou přesunuty do přírůstkové zálohy,
- **průběžná ochrana dat** – provádí okamžitý zápis každé změny do žurnálu změn. Ukládání se provádí změnou bajtů nebo celého bloku dat, místo ukládání celých změněných souborů. Průběžné záznamy umožňují získat obraz dat v minulosti,
- **úplná záloha systému** – zálohuje celý PC i s OS, je potřeba software, který nám vytvoří obraz disku. [18]

4.2.5 Aktualizace

Programy mohou obsahovat určité chyby, které útočník využívá, aby se dostal do operačního systému. Výrobci programů jsou si toho vědomi, a proto poskytují opravy, díky kterým můžeme tyto chyby eliminovat. Máme dva druhy oprav „ hotfixy“, opravují dílčí problémy a „ patche neboli service packy“ opravují více problémů zároveň. Tyto opravy poskytují výrobci zcela zdarma prostřednictvím internetu. Důležité je mít programy aktuální, především by se měl klást důraz na aktuálnost operačního systému, webových prohlížečů a antivirového programu. [8]

4.2.6 Šifrování dat

Šifrování převádí data z podoby otevřeného textu do podoby čitelné na základě speciální znalosti. Šifrování tvoří významný bezpečnostní prvek v informačním systému. Hlavním důvodem je ochrana důvěrných a osobních informací před neoprávněnými osobami. Je

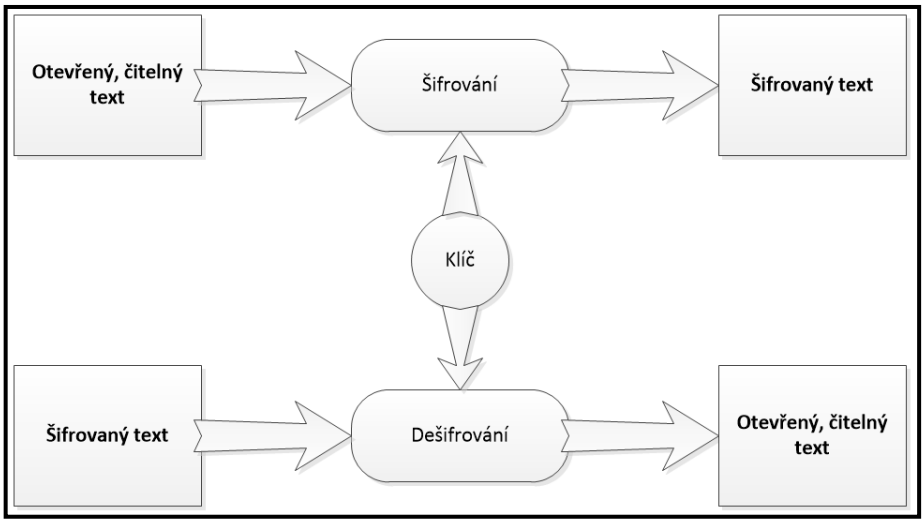
vhodné také jako ochrana před administrátory systémů, kteří nemusí mít přístup k našim datům. [2]

Opakem šifrování je dešifrování, kdy dochází k transformaci šifrovaných dat do původní podoby.[2]

Oba zmíněné postupy potřebují ke své funkci tajnou informaci. Obvykle je to klíč a nějaká z metod. Klíč si můžeme představit jako klasické heslo, které používáme denně např. jako přihlášení do počítače. V dnešní době můžeme použít jako klíč i biometrický klíč. Znamená to, že oprávněné osoby se můžou prokázat např. otiskem prstu.[2]

Rozeznáváme dva typy kryptografických algoritmů.

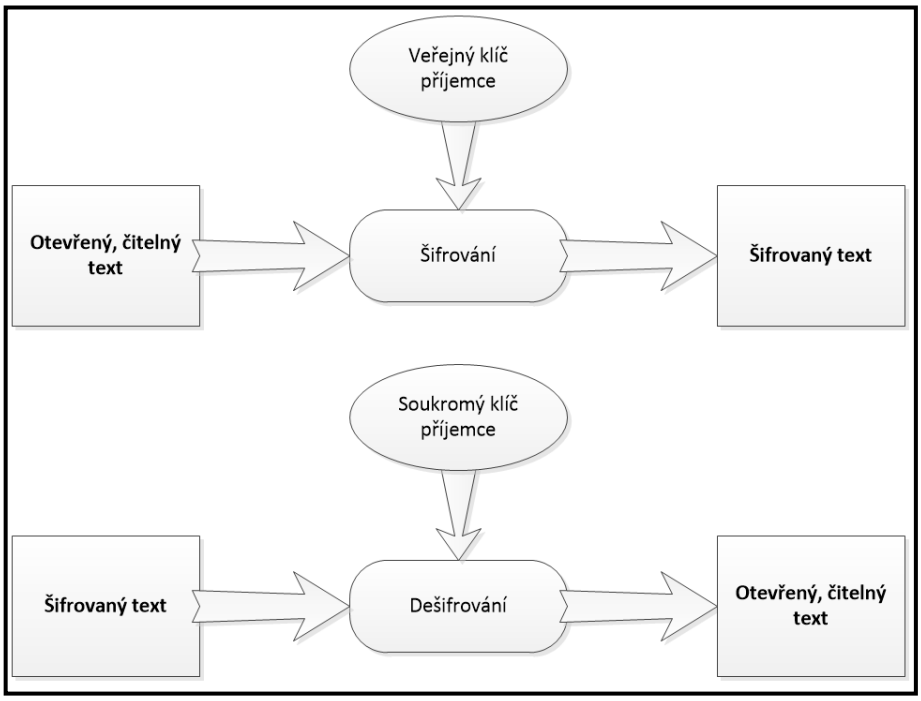
- **Symetrické šifry** – jedná se o algoritmus, který je velmi rychlý a pro šifrování a dešifrování používá stejný klíč. Rychlost vyplývá z malé výpočetní náročnosti, a proto jsou vhodné pro šifrování velkého množství dat. Dělíme je na blokové a proudové šifry. Proudové šifrují bit po bitech, ale blokové kódují celý daný blok. Mezi nejznámější algoritmy téhle šifry patří: DES, 3DES, IDEA, AES a Blowfish. Nejpoužívanějším algoritmem je AES, který se dočkal i HW akceleraci.[2]



Obrázek 5: Princip symetrické šifry. [2]

Na obrázku č. 4 vidíme princip symetrického šifrování, je velice jednoduchý. Odesílatel svou zprávu zakóduje jedinečným klíčem, který zná pouze on a jeho příjemce. Klíč nikdo nesmí nikomu dále sdělit, aby nebylo šifrování prolomeno. Poté můžeme odeslat zprávu příjemci, bez toho, aby se bál, že si zprávu přečte někdo jiný.

- **Asymetrické šifry** – jedná se o algoritmus, kde společný klíč je nahrazen párovým klíčem. Využívají se dva klíče, kdy jeden je veřejný a druhý soukromý klíč. Klíče spolu nijak nesouvisí a nelze jeden od druhého odvodit. Veřejný klíč se používá pro šifrování a soukromý klíč pro dešifrování zprávy do čitelné podoby. Pro použití asymetrického šifrování je důležité, aby soukromý klíč měl vždy jen vlastník. Při dodržování základních pravidel docílíme bezpečnosti: Je vhodné používat dostatečně dlouhé klíče alespoň 128b, ale raději256b. Dále konstruovat algoritmy s využitím matematického přístupu, které umožňují útok pouze hrubou silou.[2]



Obrázek 6: Princip asymetrické šifry. [2]

Na obrázku č. 5 vidíme princip asymetrické šifrování, které na rozdíl od symetrického využívá dvojici klíčů. Jeden klíč se používá pro šifrování a druhý pro dešifrování. Odesílatel si nechává svůj soukromý klíč, který nikomu nesmí sdělit, zatímco veřejný klíč může znát kdokoliv. Při použití tohoto šifrování se nemůže stát, že zprávu přečte cizí osoba.

4.2.7 Vícenásobné diskové pole

RAID je vícenásobné diskové pole nezávislých disků. Jde tedy o zabezpečení kontinuity činnosti v případě selhání jednoho, nebo více disků dle typu pole. Úroveň zabezpečení se liší podle zvoleného typu RAID pole. Mezi nejvyužívanější typy patří RAID 0, RAID 1, RAID 5, RAID 6 a RAID 10. [12]

RAID 0 v praxi znamená, pokud dojde k výpadku jednoho z disků, ztratí se všechna data. RAID 0 můžeme rozdělit na dva typy zřetězení a prokládání. Pokud použijeme první typ zřetězení, data se ukládají na jednotlivé disky až do vyčerpání kapacity na daném disku. Jakmile dojde místo na disku, ukládá se na další disk. V druhém typu prokládání jsou data ukládána střídavě na dva disky. Můžeme tím docílit rychlejšího čtení a zápisu.[12]

RAID 1 využívá zrcadlení. V praxi to znamená, že data jsou ukládána současně na oba disky. V případě poruchy jednoho z disku se pracuje s diskem druhým a tím pádem máme data pořád k dispozici. Nevýhodou je, že máme sice dva disky, ale kapacitu máme pouze jednoho z nich.[12]

RAID 5 vyžaduje minimálně tři disky. Pro ukládání dat využívá jeden disk redundantní informace tzv. paritní bity, které jsou rozmístěny po všech discích. V případě selhání jednoho z disků se dají data na tomto disku obnovit pomocí paritních bitů, které jsou uloženy na zbývajících discích a můžeme je zapsat na nový disk. [8]

RAID 6 je rozšíření RAIDU 5. Pro zvýšení odolnosti proti chybám používá ukládání druhé, nezávislé paritní informace. Díky tomu je spolehlivější a v případě výpadku dvou disků můžeme data znovu získat. Rychlost čtení je podobná jako u RAIDU 5, ale zápis je o něco pomalejší, protože musíme vypočítat a uložit dvě sady paritních informací. [51]

RAID 10 je kombinace RAID 0 a RAID 1, využívá zrcadlení disků. Poskytuje vysokou propustnost dat a úplnou redundanci. Data se prokládají přes všechny disky, protože je zrcadlen každý disk. Z důvodu, že se neprovádí žádný výpočet parity, nedochází tedy ke zpoždění. RAID 10 toleruje ztrátu několika jednotek, pokud tedy nedojde k selhání dvou stejných zrcadlených disků.[13]

4.2.8 Virtuální privátní síť

Virtuální privátní síť (VPN) je propojení mezi dvěma body pomocí privátní nebo veřejné sítě, většinou pomocí Internetu. Využívají se speciální protokoly, které jsou založené na TCP/IP a jsou označovány jako protokoly pro tunelová propojení. Data jsou směřována přes Internet jako jakýkoliv jiný paket. Při používání VPN zahajuje komunikaci klient přes Internet pomocí virtuálního propojení mezi dvěma body k serveru. Server vzdáleného přístupu přijme a ověří volajícího a následně přenese data mezi klientem VPN a organizací. [14]

Linka je vytvářena pomocí zapouzdření dat do hlavičky, které obsahují směrovací informace, díky kterým se data dostanou přes sdílenou nebo veřejnou síť až ke koncovému uživateli.[14]

4.2.9 Bezpečné heslo

Pomocí hesla se můžeme připojit ke službám na Internetu, jako např. přihlášení do emailové pošty, sociální sítě, bankovnictví a další webové aplikace. Heslo je převážně jediným způsobem, jak ověřit totožnost na internetu a díky tomu služby využívat. Proto musíme klást důraz na délku hesla, aby jej nebylo snadné odhalit. Mnoho uživatelů používá slabá hesla a tím zvyšují riziko, že jejich heslo někdo prolomí a bude moci používat jejich služby. [15]

Mezi nejznámější způsoby prolomení hesel patří sociální inženýrství, slovní útoky a útoky hrubou silou.[15]

Sociální inženýrství využívá manipulace uživatele k získání jeho hesla. Pro tento způsob se nejčastěji používá pretexting nebo phishing. Při použití pretextingu je uživatel žádán k heslu pomocí příběhu doplněného o reálný údaj např. datum narození. Phishing se používá převážně k údajům k bankovním službám, kdy uživatel na podvržené stránce sám zadá heslo a odešle útočníkovi. Podvržené stránky se můžou posílat i pomocí e-mailu. [15]

Slovní útok vychází z velmi jednoduchých hesel, které si uživatelé zvolí. Útočník vloží seznam možných hesel do speciálního programu a postupně tyto hesla zkouší, až získá přístupové heslo. [15]

Útok hrubou silou je velmi zdlouhavý, protože zkouší všechny možné kombinace. V případě použití krátkých hesel je velmi účinný.[15]

Při použití čísel od 0 – 9, heslo dlouhé 4 znaky znamená celkem 10 tisíc kombinací. V případě stejného použití, ale navíc doplněno a malé znaky abecedy představuje celkem 1,7 milionu kombinací. Avšak při tvorbě bezpečného hesla, které by mělo obsahovat zmíněná dvě použití, tedy číslo od 0 – 9 a malé i velké znaky abecedy, heslo dlouhé 4 znaky představuje celkem 15 milionů kombinací.[15]

4.3 Personální bezpečnost

Personální bezpečnost je velmi důležitou oblastí z hlediska lidských zdrojů, která sleduje životní cyklus pracovníka.[3]

První oblast, která rozděluje bezpečnostní opatření, je již před vznikem pracovního vztahu. Dochází zde ke stanovení a dokumentaci bezpečnostních rolí a odpovědností. Je vhodné nové pracovníky prověřit pomocí ověření identity, ověření dokladů, ověření nejvyššího dosaženého vzdělání. Také zde můžeme ověřit bezúhonnost na základě výpisu z trestního rejstříku. Všechny prověřovací aktivity musí být prováděny svědomitě a důsledně podle právních předpisů. V poslední fázi před vznikem pracovního vztahu je stanovení podmínek.[3]

Druhou oblastí je přijetí nového zaměstnance. Zde musíme dbát na to, aby vedoucí zaměstnanců své zaměstnance seznámil s bezpečnostními pravidly a aby je na základě motivace dodržovali. Bezpečnostní povědomí je prováděno různými školeními, semináři, tréninky a jinými aktivitami. Důvodem je, aby zaměstnanci respektovali předem stanovená pravidla. Pokud by tato pravidla nechtěli akceptovat, mohou být disciplinárně potrestáni. Drobné prohřešky mohou být slovně napomenuty, ale závaznější prohřešky mohou být řešeny finančně, ale i ukončením pracovní smlouvy.[3]

Třetí oblastí je ukončení pracovního vztahu. Hlavním opatřením je odpovědnost o ukončení pracovního vztahu. Jedná se hlavně o to, aby mezi personálním oddělením a manažery byly zabezpečeny vztahy. Je důležité upozornit zaměstnance, který se rozhodl odejít, „ o mlčenlivosti“, která platí i po jeho odchodu. Také by měl zaměstnanec vrátit všechny zapůjčené věci. Pokud v organizaci byly povoleny soukromé prostředky zaměstnance, musí zaměstnanec po skončení pracovního vztahu smazat všechna data na soukromých prostředcích. Zaměstnanci, kteří se starají o komunikační technologie, musí zajistit smazání všech přístupových údajů odcházejícího pracovníka.[3]

5 MOBILNÍ ZAŘÍZENÍ

O mobilní zařízení se musíme starat stejně jako o PC. Zajímáme se o to, jaké firemní data mají zaměstnanci na firemních smartphonech a jaké aplikace do nich instalují. Mezi nejrozšířenější operační systémy patří Android od Googlu a iOS od Applu. [16]

U Androidu je mnohem více verzí operačního systému, které nabízejí různé schopnosti, a díky tomu se stává komplikovanější vývoj mobilních aplikací. Operační systém iOS obsahuje nástroje, které dávají IT oddělením možnost snadno smartphony konfigurovat a sledovat jejich chování. V případě potřeby můžou také mobilní zařízení zamknout nebo úplně vymazat. V operačním systému iOS můžeme provádět mnoho nastavení, např. zakázat používání fotoaparátu, zakázat instalaci nových aplikací a zakázat používat vybraných aplikací. Rozšíření konfigurace operačního systému Android přišlo s příchodem verze 2.2. U této verze již mohou správci na dálku mazat data ze ztraceného zařízení, zamknout přístup k zařízení, vyžadovat hesla a nastavit jeho minimální délku. Zmíněné možnosti jsou k dispozici pouze tehdy, pokud je na zařízení nainstalována aplikace Google AppsDevicePolicy od firmy Google. Ve srovnání s operačním systémem iOS obsahuje operační systém Android méně možností pro vzdálený přístup. [16]

Na každém mobilním zařízení by měl být nainstalován antivirový program stejně jako na klasických PC. Mezi nejznámější antivirové programy mobilních zařízení patří firma AVG společně s firmami Avast a ESET Mobile Security. Antivirové programy kontrolují aplikace, stahování e-mailů, SMS a prohlížení webových stránek. V případě nalezení škodlivého softwaru může také antivirový program skenovat celé zařízení a nalezený vir odstranit. Některé programy nabízí i schopnost lokalizace ztraceného mobilního zařízení. [16]

5.1 BYOD

BYOD je využívání soukromých zařízení uživatele jako notebook, smartphone a tablet v práci a připojení do počítačové sítě v podniku. Jedná se o rozvíjející se trend posledních let, převážně v malých a středních firmách, díky cloud úložištím.[21]

Hlavní výhodou je zvýšení produktivity a spokojenosti zaměstnanců, protože zaměstnanci pracují se svými zařízeními, na které jsou zvyklí. Mnohdy zaměstnanci mají kvalitnější osobní zařízení, než jsou podnikové standardy. Díky tomu mohou na pracoviště přinášet různé inovace. Další výhodou může být snížení firemních nákladu, protože firma nemusí kupovat a obnovovat neustále daná zařízení. [21]

Mezi hlavní nevýhodu a také riziko patří přístup k citlivým datům a informacím. Pokud osobní zařízení zaměstnance nesplňuje bezpečnostní požadavky, může to pro firmu představovat riziko.[21]

Pokud chceme, aby BYOD byl zaveden ve firmě, je důležité, aby byla ošetřena práva a provedena zásadní změna pracovních smluv.[21]

5.1.1 Zásady pro zavedení BYOD u podnikatele

Jako první by měl podnikatel provést pečlivou přípravu, ve které je dobré si stanovit pravidla pro používání BYOD a identifikovat rizika.[20]

Základními pravidla jsou:

- Kontrola přístupu k BYOD zařízení,
- Ukončení činnosti při nečinnosti tedy „time-out“,
- Používání antivirů a firewall,
- Provádět aktualizace OS a SW,
- Souhlas vlastníka zařízení ke zpracování osobních údajů a souhlas k autorským právům.[20]

Pokud jsme provedli první fázi a určili si základní pravidla, můžeme přejít k uzavření dohody s pracovníkem, kde se zavazuje k dodržování uvedených pravidel. Tato dohoda může mít pak formu např. dodatek k pracovní smlouvě. [20]

Zavedením pravidel však není zajištěno, že budou tato pravidla od zaměstnanců dodržována. Proto je nejúčinnější metodou školení svých zaměstnanců. [20]

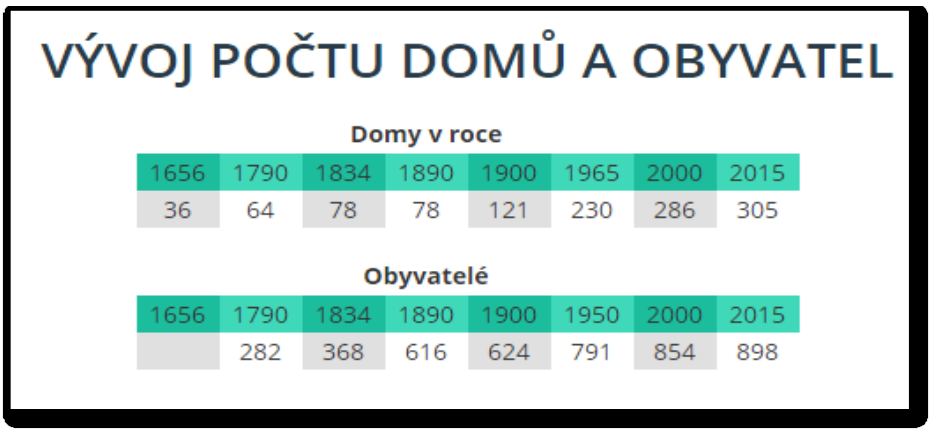
II. PRAKTICKÁ ČÁST

6 SPECIFIKACE OBCE TĚMICE

Oficiální název:	Obec Těmice
Adresa úřadu:	Těmice 176
	698 84 Těmice
Datová schránka:	ID: j8nba33
Elektronická podatelna:	E-mail: obec@temice.cz
Správce internetových stránek:	E-mail: info@ictmedia.cz

Těmice se nachází na jihovýchodní Moravě 15 km od Veselí nad Moravou v okrese Hodonín. První písemné zprávy o obci pocházejí z roku 1371. S 904 obyvateli patří mezi menší vesnice v regionu. Kraj okolí obce je známý vinařskou a zemědělskou výrobou. Vesnici obklopuje Domanínský kopec a Zadní díly. Obcí protéká potok Syrovínka, v nedávných letech zde byl vybudován menší rybník a místní koupaliště. Ve vesnici se také nachází obchod s potravinami, 2 hospody, kadeřnictví a stavebniny. Můžeme zde i naleznout poštu, mateřskou školu a obecní úřad.

V 90. letech byl vybudován místní vodovod, provedena plynofikace a položeny telefonní kabely. Občané tak mohou díky kabelové televizi získat všechny potřebné informace.



Obrázek 7: Vývoj počtu domů a obyvatel. [47]

Z obrázku č. 6. o vývoji počtu domů a obyvatel můžeme vidět, že i při postupném zvyšování počtu domů a obyvatel se Těmice řadí mezí menší vesnice v České republice. V současnosti k roku 2017 eviduje celkem 904 obyvatel.

6.1 Analýza současného stavu obecního úřadu Těmice

Obecní úřad v Těmicích se nachází uprostřed obce v malé přízemní budově. Přístup do budovy je možný pouze hlavními dveřmi, kterými se dostaneme do chodby vedoucí k informacím neboli zaměstnancům úřadu. Obecní úřad má celkem 4 místnosti, v nichž pracují 3 zaměstnanci. V první místnosti sídlí dvě ženy – matrikářka a účetní, které se starají o poskytnutí informací a vedení účetnictví, druhá místnost je pracovna pana starosty. Ostatní dvě místnosti slouží pro archivaci dokumentů a zálohovaných dat. Všechna PC jsou v přízemí. Vchod ani chodba nejsou nijak monitorovány.

Obrázek 8: Lokalizace obecního úřadu. [52]

Úřad má celkem 4 počítače, na kterých je nainstalován operační systém Windows 10. Přestože úřad pracuje s citlivými daty, tak počítače nejsou zabezpečeny. Nejsou uloženy do bezpečnostních boxů, které jsou izolovány proti vodě. Počítače jsou zabezpečeny pomocí Windows firewall. Dalším zabezpečením je antivirový software ESET Smart Security. I když úředníci pracují s citlivými údaji, tak žádná další zabezpečení počítačů nejsou prováděna. Veškerá data jsou uložena na externích pevných discích a zálohovací servery obecní úřad vůbec nepoužívá. Fyzická bezpečnost také není vhodně vyřešena. Zálohovaná data nejsou uložena v místnosti, která je opatřena izolací proti vodě a protipožárními čidly. Zabezpečení této místnosti není kladena žádná pozornost - zámkem ani pomocí klávesnice před dveřmi a přístupovým heslem. Vstoupit sem může každý zaměstnanec úřadu. V místnosti se také nacházejí dvě okna, která nejsou zabezpečena, takže hrozí i vniknutí zvenčí. Data, které spravuje starosta obce, si zálohuje sám, ale ostatní data, jako např. ve-

dení účetnictví, zálohuje firma Syscom Bzenec, která se rovněž stará o celkový chod počítačů a provádí veškeré aktualizace a nastavení. Počítače, které využívají sekretářky pro provádění účetnictví, jsou v samostatné síti z důvodu účetního programu. Počítač, který využívá pan starosta je oddělen od všech. Všichni zaměstnanci mají na svých počítačích oprávnění power user (využívají vstupní heslo do systému) a mohou s PC provádět prakticky cokoliv. Zaměstnancům je také povoleno používání osobních flash disků. Vzhledem k tomu, že zaměstnanci mají přístup ke všem informacím, tak nejsou nijak pravidelně školeni. Uvedená absence pravidelných školení může mít negativní dopad na celkovou bezpečnost informací úřadu. Úřad nijak neeviduje příchody ani odchody svých zaměstnanců a nepoužívá ani čipové karty pro vstup do jednotlivých místností. Pro práci na úřadě zaměstnanci nevyužívají svá osobní zařízení, ale pokud zaměstnanec chce používat osobní zařízení, starosta ani externí firma to nezakazuje.

Jeden PC úřad nevyužívá přímo pro práci na úřadě, ale používá ho pro úpravu a řízení vody. Tento PC se nachází v příspěvkové organizaci Vodovod Těmice, která má budovu na okraji obce.

Obrázek 9: Lokalizace příspěvkové organizace Vodovod Těmice. [52]

Jelikož je voda důležitá pro každého občana a Vodovod Těmice zajišťuje vodu obcím Domanín, Syrovín a Těmice, přistoupila obec i k důkladnějšímu zabezpečení počítače oproti počítačům, které používá na obecním úřadě. O zabezpečení PC se stará externí firma GDF, která se řídí směrnicí, kde jsou určeny pravidla použití výpočetní techniky. Tato firma se kromě jiného také stará o zabezpečení přenosů, internetu a hlášení poruch. Na PC je nain-

stalován operační systém Windows 10. Jako antivirový program je nainstalován ESET Smart Security Premium spolu s externím firewallem Sophos. U čisté vody se zálohování dat provádí automatickým snímkováním, duplicitními stroji a kompatibilním komunikačním protokolem. Vlastní příjem dat není po internetu, ale lze jej získat pouze spojením se zrcadleným archivem. Řízení je zcela automatické a odborně pověřená osoba řeší pouze nestandardní stavy. U špinavé vody (kanalizace) je zabezpečení dat provedeno archivací. Data jsou zálohována s frekvencí jednou za 14 dní v celkové záloze a denní přírůstkovou zálohou. Zálohy se vypalují na Blu-Ray média 25 GB a 50 GB a ukládají se do místnosti, kde se nachází server. Tato místnost je také vybavena protipožárním sejfem, kde jsou Blu-Ray média uložena. Když komunikace selže, řídí se systém autonomně dál. PC infrastruktura je zálohována jedním záložním zdrojem. K tomuto účelu jsou rozvody proudu z UPS v modrých zásuvkách. Zálohování v případě dlouhodobého výpadku elektřiny je řešeno pomocí záložního generátoru, který začne dodávat energii do dvou minut od výpadku síťového zdroje.

7 NÁVRH ŘEŠENÍ

Bezpečnost informačních systémů z hlediska opatření, by měla každá malá obec zajistit, aby kontinuálně udržela ochranu před nežádoucími vlivy. Bezpečnostní opatření zahrnuje jak ochranu zařízení a softwaru, tak i personální bezpečnost, která je pro obec velmi důležitá. Je třeba si hlavně uvědomit, že ideálně zabezpečený informační systém neexistuje a také to, že HW a SW nejsou největším rizikem. Hlavní rizikem je člověk, který pracuje s informačním systémem. Proto by každý uživatel informačního systému měl být řádně proškolen, aby se snížilo riziko. Proškolení zaměstnanců nemusí zabírat mnoho času a finančních nákladů. Mělo by jít hlavně o základní proškolení, aby zaměstnanci pochopili funkce programů, se kterými budou pracovat, jaká hesla používat pro přihlášení a také jaké stránky v pracovní době mohou navštěvovat. Za každý informační systém je zodpovědná pověřená osoba neboli správce informačního systému. Kromě správce informačního systému musí mít každý obecní úřad vedoucího jednotlivých oddělení, který kontroluje své podřízené. Každý správce by měl mít kontrolu, co zaměstnanci na daném zařízení instalují a zda jsou nainstalované programy aktuální. Aktualizace se musí týkat nejen operačních systémů a aplikačních programů, ale také systémů ochrany – antivirových programů. Odpovědnost nemůže být jen stanovena, ale musí být i vyžadována.

7.1 Identifikace nalezených nedostatků

V předešlé kapitole byla provedena analýza současného stavu obce Těmice. Na obecním úřadě v Těmicích byly identifikovány velké nedostatky týkající se zabezpečení informačního systému. Některé z nich byly méně závažné, ale naopak některé více. Nedostatky byly převážně v zabezpečení zálohovaných dat a taky chybělo školení zaměstnanců. Hlavním cílem této části práce bude navrhnout vhodná řešení pro jejich odstranění nebo alespoň částečné zmírnění.

Fyzická bezpečnost	Špatně	Správně
Firewall	Windows firewall	Externí firewall
Antivirový program	ESET Smart Security	ESET Smat Security Premium
Zálohování dat	Externí pevné disky (každý den)	Externí pevné disky (každý den)
Omezení oprávnění	Ne	Ano
Flash disky	Povoleno	Zakázat
Aktualizace	Provádí firma Syscom Bzenec	Firma Syscom + kontrola starosta (správce sítě)
Školení zaměstnanců	Ne	Ano

Tabulka 1: Identifikace nalezených nedostatků bezpečnosti dat. [Vlastní]

V tabulce č. 2 můžeme vidět identifikaci nalezených nedostatků ohledně bezpečnosti dat. Jelikož obecní úřad pracuje s velmi citlivými údaji, má špatně řešenu řadu bezpečnostních opatření. Jako nejrizikovější vyplynula fyzická bezpečnost. Zálohování se provádí na externí pevné disky, které nejsou uloženy v místnosti, která je opatřena izolací proti vodě, protipožárními čidly. Hlavní vstup není také monitorován ani hlídán. Za ne příliš vhodné a rizikové považuji neproškolování zaměstnanců a jejich volnost na PC, které používají pro danou práci. Školením můžeme zabránit mnoha incidentům. Jak již bylo zmíněno, úřad nechává spravovat počítače externí firmou Syscom Bzenec. Může se i stát, že starosta neboli správce sítě, nebude mít skutečný přehled o stavu na daném PC. V takovém případě je

lepší, aby správce sítě kontrolovat vše, co externí firma provedla. Získá tím přehled o všech počítačích, které se na úřadě nachází.

7.2 Fyzická bezpečnost

	Stávající stav	Doporučení
Bezpečnostní box	Ne	Ano
Zámek PC skříně	Ne	Ano
Mříže oken	Ne	Ano
Bezpečnostní dveře	Ne	Ano
Protipožární opatření	Ne	Ano
Izolace proti vodě	Ne	Ano

Tabulka 2: Fyzický bezpečnost. [Vlastní]

V tabulce č. 3 je provedena analýza fyzické bezpečnosti, kde je jasně vidět, že ji obecní úřad neřeší. V následujících částech této kapitoly je provedeno doporučení pro zajištění fyzické bezpečnosti.

7.2.1 Fyzické zabezpečení zálohovaných dat

Obecní úřad fyzickou bezpečnost neřeší vhodně. V případě zabezpečení zálohovaných dat, které obecní úřad zálohuje na externí pevné disky, doporučuji umístit disky a důležité dokumenty do místnosti, která bude izolována proti vodě a bude obsahovat protipožární čidla. Okna v této místnosti budou opatřena bezpečnostními mřížemi. Také by k minimální nápravě stavu stačilo opatřit vstup do místnosti dveřmi, které budou mít na jedné straně kulatou kliku. Již toto základní opatření může zamezit přístupu nechtěným osobám. Takové opatření vstupu do místnosti je spíše minimální a pořád ještě nedokonalé. V ideálním případě doporučuji současné dveře nahradit bezpečnostními dveřmi, které mají odolnost proti násilnému vniknutí, požáru a dokážou tlumit i hluk. Jako doplňující opatření pro ztížení přístupu doporučuji také před dveře umístit klávesnici pro vstup do místnosti.

V případě, kdy bude tato místnost dobře zabezpečena proti vstupu nechtěných osob, je potřeba také určit okruh lidí, kteří mohou do této místnosti vstupovat. Určit jejich pravomoci a také okolnosti, za kterých je jim přístup umožněn. Všechny tyto osoby musí být

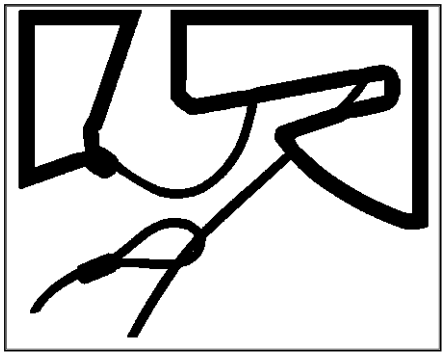
důkladně proškoleny, jak se v místnosti chovat, jak řešit krizové situace - převážně hlášení požáru.

7.2.2 Fyzické zabezpečení počítačů

Pro zvýšení fyzické bezpečnosti u PC jsem doporučoval umístění počítačů do skříněk, které jsou izolovány proti vodě. Také můžeme považovat za zvýšení bezpečnosti uzamčení počítačových skříní proti otevření. U některých z nich to není otázkou dodatečných nákladů, protože zámek je již součástí skříně. Pokud ale takovou skříň úřad nemá, může oslovit externí firmu pro dodání zámků do již existující skříně. Více viz obrázek níže.

Obrázek 10: Zámek PC skříně. [50]

Pokud chceme mít nejlepší fyzické zabezpečení, můžeme použít i zámky, které brání fyzickému přemístění hardwarového vybavení firmy. Většina z nich je již součástí počítačů, monitorů, tiskáren atd. a je vybavena stolem pro připojení zámku.



Obrázek 11: Zámek hardware. [49]

7.2.3 Fyzický přístup

Podstatnou součástí je také fyzický přístup, který obecní úřad nikterak neřeší. Neprovádí žádnou evidenci svých zaměstnanců a místnosti také nejsou nijak zabezpečeny. Pro zvýše-

ní bezpečnosti doporučuji, aby obecní úřad měl každou místnost opatřenou bezpečnostními zámky a nacházely se zde i alarmy. Jednotlivá zařízení označit. Je dobré také provádět evidenci zaměstnanců. Abychom ji zajistili, stačí jim zřídit čipovou kartu, pomocí které budou do jednotlivých místností vstupovat. Tak budeme vědět, kdo se v jednotlivých místnostech pohybuje a v jakém okamžiku.

7.2.4 Shrnutí fyzické bezpečnost

Dodržováním následujících bodů by mělo vést k nápravě fyzické bezpečnosti.

- Místnost se zálohovanými daty a důležitými dokumenty opatřit mřížemi, zámky, alarmy, protipožárním opatřením a izolací proti vodě,
- Všechny vstupy a výstupy evidovat,
- Minimalizovat osoby, které mají vstup do důležitých místností, jako jsou místnosti, kde jsou umístěny zálohovaná data nebo důležité dokumenty. Proto je dobré mít jednoho správce odpovídajícího za servery a druhého za dokumenty. Vstup jiného zaměstnance do těchto prostorů musí být jen za přítomnosti pověřené osoby,
- Místnosti s daty a důležitými dokumenty by neměly obsahovat žádná okna, v našem případě je opatřit bezpečnostními mřížemi
- Jednotlivá opatření pravidelně testovat alespoň jednou do měsíce,
- Evidovat sériová čísla PC a komponentů,
- Označit PC, jeho umístění a uživatele, který je za dané PC zodpovědný.

7.3 Firewall

Obecní úřad používá firewall, který je přímo zabudován v systému Windows. Nalezneme jej v ovládacích panelech v sekci systém a zabezpečení. Vidíme zde přehled o nastavení, pro jakou privátní síť je zapnut a také, co se má provádět s nově příchozími aplikacemi. Pro každou síť, ať již veřejnou nebo privátní, můžeme definovat, zda má byt firewall zapnutý nebo vypnutý. Firewall je důležité mít vždy zapnutý, nedoporučuji ho vypínat. Správce sítě nikdy nesmí nastavit, aby se blokovali všechna příchozí spojení, včetně aplikací. Musí vždy ponechat aktivní upozornění, aby se mohl rozhodnout, zda novou aplikaci povolí a bude moci komunikovat s PC zaměstnance úřadu. Některým aplikacím může správce povolit průchod firewallem a nastavit pro ně komunikaci buď pro veřejnou, nebo soukromou síť.

Jelikož bezpečnost pro úřady je velmi důležitá a nesmíme ji nijak podceňovat, tak nám firewall může určitě napomoct ji zvýšit. Abychom zvýšili úroveň bezpečnosti, doporučoval bych rozšířit systémový firewall i externím řešením - firewallem, který bývá občas nabízen dodavateli k antivirovým programům. Pokud bychom se rozhodli používat externí firewall, musíme vždy vypnout Windows firewall. V PC může být zapnut pouze jeden.

7.4 Antivirový program

Antivirový program, je velmi důležitou součástí týkající se bezpečnosti dat. V dnešní době je na výběr velké množství antivirových programů. Některé jsou zcela zdarma a nabízejí jen základní ochranu dat a jiné komerční verze s daleko vyššími službami. Zde otestuji neznámější antivirové programy, kterými jsou ESED NOD32, Avast , AVG a Bitdefender.

Správný antivirový program musí splňovat několik požadavků:

- Musí chránit počítač v reálném čase – to znamená, že program běží na pozadí a chrání počítač v každém okamžiku.
- Musí být stále zapnutý – to klade určité nároky na technické vybavení počítače, proto si musíme vybírat antivirový program s ohledem na to, jak výkonný počítač máme.
- Musí být stále aktuální – toto je jedna z nejdůležitějších vlastností, protože neustále vznikají nové viry a pomocí aktualizací obnovujeme virovou truhlu.

7.4.1 ESET NOD 32

ESET NOD32 je antivirový program slovenské firmy ESET. Je vyvinut na operační systém Microsoft Windows, Linux, ale také na mobilní zařízení. Jedná se o velmi kvalitní program, který vyhovuje všem podmínkám tohoto typu softwaru. Jedinou nevýhodou je, že není k dispozici zdarma. Tato jediná nevýhoda je však vynahrazena technickou podporou, kterou uživatel může využít.

- **ESET NOD32** – Jedná se o základní verzi, která poskytuje základní služby jako je ochrana před viry, ochrana před anti-phishingem a také podporuje herní mód. Výhodou jsou nízké systémové nároky a technická podpora v češtině.
- **ESET Smart Security** – Jedná se o komplexní Internetovou ochranu dat pro systém Windows, která navíc od základní verze umožňuje ochranu internetového ban-

kovnictví, ochranu před hackery a také ochranu naší sítě neboli routeru. Tato verze je navíc doplněna o externí firewall.

- **ESET Family Security Pack** - Nabízí ochranu pro celé rodiny. Jedná se v podstatě o komplexní řešení jako u Smart Security, ale navíc umožňuje i ochranu mobilních zařízení a tabletu.
- **ESET Smart Security Premium** – Jedná se o prémiovou Internetovou ochranu dat pro systém Windows. Balíček je navíc doplněn oproti klasické verzi Smart Security o šifrování dat a správce hesel. Menším nedostatkem může být, že nepodporuje ochranu mobilních zařízení.

	ESET NOD32 Antivirus	**ESET Smart Security**	**ESET Family Securit Pack**	**ESET Smart Security Premium**
Ochrana před viry	X	X	X	X
Podpora v češtině	X	X	X	X
Ochrana internetového bankovnictví		X	X	X
Ochrana před hackery		X	X	X
Zabezpečená webkamera		X	X	X
Ochrana naší sítě		X	X	X
Rodičovská kontrola		X	X	X
Šifrování dat				X
Správce hesel				X
Mobilní ochrana			X	
Cena	1209 Kč	1490 Kč	1590 Kč	1890 Kč

Tabulka 3: Porovnání programu ESET. [Vlastní]

7.4.2 Shrnutí ESET NOD32

Antivirový program od firmy ESET nabízí celkem čtyři možné produkty, které se liší v nabízených funkcích a tím i v pořizovací ceně. Za velkou výhodu určitě považuji, že všechny produkty podporují češtinu. Z tabulky je jasné, že nejzákladnější a tedy nejlevnější je produkt ESET NOD32 Antivirus, který nabízí pouze ochranu před viry. Rodinná verze ESET Family Security Pack nabízí jako jediná také mobilní ochranu. Nejvyšší nabízená verze ESET Smart Security Premium nabízí oproti všem ostatním také šifrování dat a správu hesel. Antivirový software ESET považuji za jeden z nejkvalitnějších nabízených antivirových programů na trhu a doporučuji ho pro obecní úřady.

7.4.3 Avast

Avast je antivirový program, který vyvíjí společnost Avast Software s.r.o. Program je dostupný v mnoha jazycích.

Jedná se o jeden z nejpopulárnějších plnohodnotných freewarových antivirových programů pro uživatele Microsoft Windows. Avast také chrání chytré telefony a tablety.

- **Avast Free Antivirus** – Instaluje se pomocí live instalátoru, který je maličký a vše potřebné stahuje až při instalaci. Před instalací si pouze vybereme jazyk a upřesníme uložení programu. Pokud chceme ponechat po instalaci bezplatnou verzi, musíme se zaregistrovat. To provedeme tak, že vložíme svůj vlastní e-mail. Pod nabídkou test najdeme kromě klasického virového testu také další testy jako: hledat doplňky prohlížečů, hledat zastaralý software, hledat síťové hrozby a hledat výkonnostní problémy. Nástroje v téhle verzi nemají firewall. K dispozici jsou: vzdálená asistence, statistika a záchranný disk.
- **Avast Pro Antivirus** – Přináší tři zásadní novinky: ochranu DNS, Sandbox a SafeZone. Služba Sandbox nám umožňuje spouštět nebezpečné soubory, aplikace a prohlížet nebezpečné stránky. Takže pokud si nejsme jisti, jestli je soubor bezpečný, můžeme využít tuto službu. Jakmile Sandbox zavřeme, smažou se všechna data. SafeZone je služba, která je určena na prohlížení důležitých stránek, u kterých chceme mít jistotu, že nás nesleduje virus. Ochrana DNS se stará, aby u našeho routeru nešlo provést neoprávněnou změnu DNS.
- **Avast Internet Security** – Přináší komplexní ochranu od antiviru a firewallu až po ochranu bankovnictví a zabezpečení domácí sítě. I zde máme několik voleb kontroly. Kromě klasické antivirové kontroly máme zde stejné moduly jako i Free verze

(hledat doplňky prohlížečů, hledat zastaralý software, hledat sítové hrozby a hledat výkonnostní problémy.) Je zde sada nástrojů, mezi které patří: SafeZone prohlížeč, Sandbox, vzdálená asistence, statistika, firewall a záchranný disk.

- **Avast Premier** – Mezi novinkami je zrychlená verze instalace. Obsahuje aplikaci, která jedním heslem chrání všechna ostatní hesla uložená v PC. Další aplikací je SafeZone Browser, která automaticky najde a přesune všechny údaje o placení do bezpečného prostoru. Výhodou je také blokování reklam pomocí Ad Blocker.

	Avast Free Antivirus	**Avast Internet Security**	**Avast Premier**	**Avast Pro Antivirus**
Ochrana před viry	X	X	X	X
Aktualizace v reálném čase	X	X	X	X
Správce hesel	X	X	X	X
Ochrana internetového bankovnictví		X	X	X
Ochrana naší sítě		X	X	
Ochrana před spamem		X	X	
Ochrana před hackery			X	
Trvalé odstranění citlivých dat			X	
Cena	Zdarma	1190 Kč	1690 Kč	790 Kč

Tabulka 4: Porovnání programu Avast. [Vlastní]

7.4.4 Shrnutí Avast

Antivirový program od společnosti Avast nabízí celkem čtyři produkty. Kromě licenčních produktů nabízí také Free verzi, která podporuje pouze ochranu před viry a správu hesel. Nejvyšší řadou je Avast Premier, která nabízí oproti zde porovnávaným produktům také trvalé odstranění citlivých dat. Verze Avast Internet Security nabízí oproti verzi Avast Pro Antivirus také ochranu naší sítě a ochranu před spamem.

Antivirový program od společnosti Avast patří mezi známé a kvalitní antivirové softwary, ale pro obecní úřady bych volil jiný software, který nabízí lepší funkce a vyniká vyšší kvalitou ochrany.

7.4.5 AVG

AVG je antivirová společnost od české společnosti AVG Technologies. Antivirus je určen pro operační systémy Microsoft Windows, Linux, Apple OS X, iOS, ale také Android.

Na stránkách společnosti můžeme stáhnout AVG AntiVirus FREE, který je určen pro domácí použití.

- **AVG AntiVirus FREE** – Jedná se o základní bezplatnou ochranu pro PC. Tato verze je zcela zdarma a má pouze základní vlastnosti jako je ochrana před malwarem a spywarem a automatickou aktualizaci zabezpečení.
- **AVG Internet Seucirty** – Tato verze je určena pro kompletní ochranu bez omezeného počtu zařízení. Kromě předešlých vlastností, které obsahuje FREE verze je toto zabezpečení dále doplněno o: živou telefonickou podporu a podporu prostřednictvím chatu. Je také určena pro iOS a Android zařízení. Balíček obsahuje také externí firewall.
- **AVG Ultimate** – Jedná se nejlepší kompletní balíček pro neomezený počet zařízení. Kromě vlastností, které obsahují již předešlé verze, je navíc doplněna o zabezpečení více PC z jedné obrazovky, a také není omezena počtem instalací.

	AVG Antivirus FREE	**AVG Internet Security**	**AVG Ultimate**
Ochrana před viry	X	X	X
Blokování nebezpečných odkazů	X	X	X
Aktualizace v reálném čase	X	X	X
Ochrana před hackery		X	X
Šifrování		X	X
Telefonická podpora		X	X
Ochrana před finančními podvody		X	X

Pro iOS a Android aplikace		X	X
Zabezpečení více PC z jedné obrazovky			X
Neomezený počet instalací			X
Cena	Zdarma	1499 Kč	1999 Kč

Tabulka 5: Porovnání programu AVG. [Vlastní]

7.4.6 Shrnutí AVG

Antivirový program od společnosti AVG nabízí celkem tři produkty. Stejně tak jako Avast nabízí také jeden produkt, který je zdarma. Prostřední verze je AVG Internet Security, která nabízí řadu důležitých funkcí jako např. šifrování a ochranu před finančními podvody. Poslední vlajkovou verzí je AVG Ultimate, jejíž cena 1999 Kč se může zdát vyšší, ale je to způsobeno, že nabízí neomezený počet instalací a také zabezpečení více obrazovek z jednoho PC oproti nabízeným verzím od této společnost.

Stejně tak jako u Avastu nabízí společnost AVG také kvalitní antivirový software, ale pro práci na obecním úřadě bych také doporučoval jiný kvalitnější antivirový program.

7.4.7 Bitdefender Antivirus Plus 2017

Bitdefende je antivirový program, který zbytečně nezatěžuje PC, a nemusíme je složitě nastavovat. Pokud tento antivirový program porovnáme se známými programy jako AVG, Avast a další, je Bitdefender v zátěžových testech nejlepší. Jeho výkon a úroveň ochrany je jedna z nejlepších. Nevýhodou může být pro některé uživatele, že je zcela anglicky a nepodporuje češtinu. Jeho licence na jeden PC stojí 955 Kč.

Tato verze umožňuje následující funkce a vlastnosti:

- Kompletní ochrana dat,
- Ochrana online bankovnictví,
- Vzdálená správa,
- USB čistič,
- Ochrana sociálních sítí,
- Správa hesel,
- Herní, filmové a pracovní módy,
- Rychlé a bezpečné platby,

- Rychlé skenování zranitelnosti.

7.4.8 Shrnutí Bitdefender

Bitdefender jako jediný z mých porovnávaných antivirových programů nemá verzi v češtině. Toto může být pro řadu správců sítě obecního úřadu značnou nevýhodou. Jedná se o kvalitní antivirový software, který dosahuje velmi výborných výsledků v zátěžových testech. Pro práci na úřadě bych určitě volil antivirový program, který podporuje češtinu.

7.4.9 Výběr zvolených antivirových programů

Jelikož obecní úřad, kde jsem prováděl analýzu současného stavu, používá antivirový program ESET Smart Security, doporučil jsem z důvodu práce s velmi důležitými, citlivými daty a informacemi používání nejvyšší nabízené verze od firmy ESET, tedy ESET Smart Security Premium, která umožňuje šifrování dat a správu hesel. Také menší výhodou v porovnání s AVG Ultimate je, že je levnější, takže můžeme ušetřit i pořizovací náklady, zejména při větším počtu počítačů. Tento antivirus také doporučuji z důvodu velmi vysokého procentuálního nalezení viru, oproti zde uvedeným antivirovým programům.

7.5 Antivirové zabezpečení mobilních zařízení

Pokud by zaměstnanci obecního úřadu chtěli pro práci používat mobilní zařízení, musí jej chránit antivirovým softwarem stejně, jako chráníme počítače. Je však dobré zmínit, že majitelé operačního systému iOS a Windows Phone se o antivirový program zajímat nemusí. Do těchto OS se vir těžko dostane, a pokud by to nastalo, odstraní se aktualizací softwaru. Jsou zde k dispozici produkty, které poskytují rodičovskou kontrolu a AntiTheft ochranu.

Zde porovnám ochranu mobilních telefonů s operačním systémem Android. Většinu bezpečnostních produktů můžeme stáhnout v obchodě Google Play a následně nainstalovat. Některé programy jsou zcela zdarma, nabízí základní ochranu dat a některé jsou licencovány a podporují např. AntiTheft ochranu.

Srovnám zde antivirové programy od firem Avast, AVG a ESET.

7.5.1 Avast Free Mobile Security

Avast Free Mobile Security je multifunkční aplikace což znamená, že chrání proti virům, skenuje a chrání osobní údaje. Tato aplikace obsahuje také firewall a AntiTheft ochranu v

případě ztráty. Podle Google Play se jedná se o nejlépe hodnocenou aplikaci pro bezpečnost na Android.

Instalace je velice jednoduchá máme na výběr ze dvou variant:

- Jednoduchý režim – máme zde přístup k základním funkcím, doporučuje se nezkušeným uživatelům,
- Pokročilý režim – máme k dispozici více možností, můžeme si volit, jak se bude např. AntiTheft nazývat.

7.5.2 AVG Antivirus

Tato aplikace podporuje ochranu před viry, poskytuje testování aplikací a souborů a také kontroluje webové stránky v reálném čase, než se otevřou. Poskytuje ochranu proti krádeži, kdy podporuje vyhledávání polohy telefonu a v případě ztráty ho můžeme zablokovat. Umožňuje pokročilou ochranu osobních údajů, kdy můžeme zamknout některé aplikace a omezit přístup uživatelům. Díky tomu chráníme naše data. V poslední řadě umožňuje sledování využití baterie a mobilních dat. Můžeme zde vypínat aplikace, které zpomalují naše zařízení, a také zde můžeme zálohovat aplikace na SD kartu.

7.5.3 ESET Mobile Security

Tato aplikace chrání naše data neustále. Jedná se o kompletní ochranu před virem a poskytuje kvalitní detekci hrozeb s Antispamem. Kromě výše uvedeného obsahuje také Anti-Theft pro vypátrání zařízení. Chrání všechny aplikace i na SD kartě, které jsou v daném zařízení nainstalovány. Umožňuje filtrování nežádoucích SMS a MMS zpráv pomocí povolených či zakázaných čísel. Můžeme také zakázat neznámá čísla. Na vyžádání může prověřit i funkce zařízení – jaký je stav baterie, viditelnost bluetooth a běžící procesy.

7.5.4 Srovnání zvolených antivirových programů pro mobilní zařízení

	Avast Free Mobile Security	AVG AntiVirus	ESET Mobile Security
Antivir	X	X	X
SMS Antispam	X	X	X
Ochrana prohlížeče	X	X	X
Bezpečnostní audit	X		
Vzdálené zablokování	X	X	X
Vzdálené vymazání	X	X	X
Vyhledávání telefonu	X	X	X
Kontrola SIM karty	X		X
Firewall			X
Zálohování aplikací a kontaktů		X	
Rodičovská kontrola			
Ochrana soukromí	X	X	X
Automatické aktualizace	X	X	X
Cena	Zdarma	30 dní zdarma poté 346 Kč	30 dní zdarma poté 289 Kč

Tabulka 5: Srovnání zvolených antivirových programů. [19]

7.5.5 Závěr

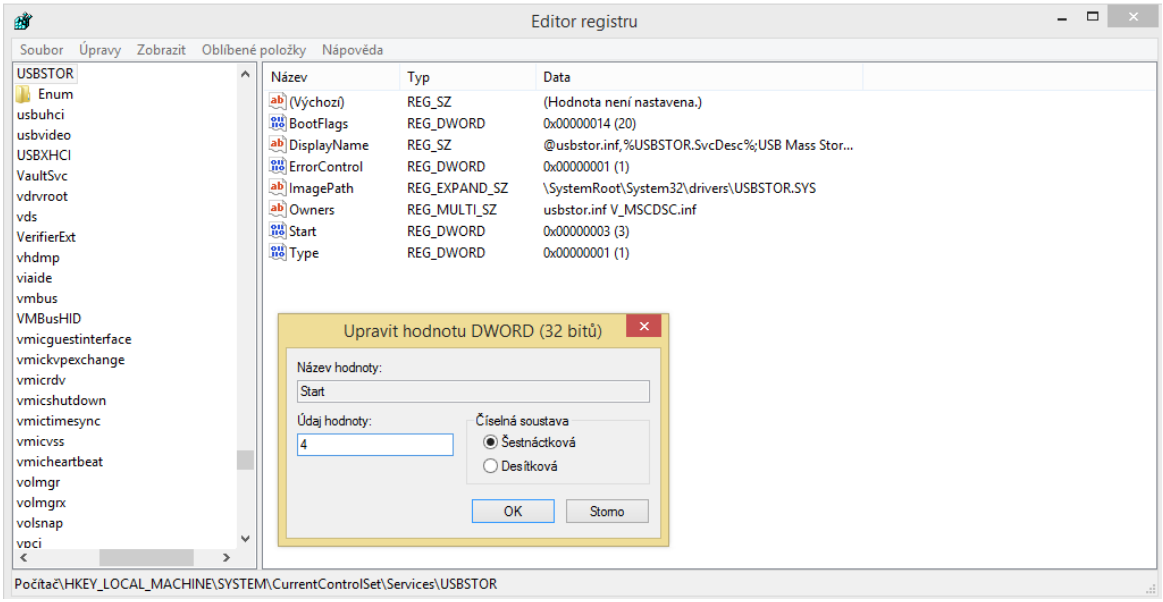
Uživatelům, kteří chtějí používat mobilní zařízení pro práci na obci, doporučuji, aby měli na smarthphonech nainstalován rovněž jako na PC antivirový program pro ochranu dat. V rámci obce a ochrany mobilních zařízení doporučují antivir ESET Mobile Security, který sice není zdarma, ale jelikož pracujeme na obecním úřadě, musíme používat velmi kvalitní antivirový software na svých smartphonech.

7.6 Uživatelské oprávnění

Uživatelské účty jsou jednou z nejzákladnějších bezpečností, jak můžeme zabezpečit náš počítač. Zaměstnanci na obecním úřadě musí zabezpečovat svůj uživatelský účet pomocí silného hesla. Uživatelské účty můžeme rozdělit celkem do tří skupin: správce počítače, uživatel a host. Účet správce počítače neboli admin má veškerá práva k počítači a může s ním prakticky cokoliv provádět. Může tedy udělovat ostatním účtům, co smí provádět, instalovat a měnit uživatelské účty. Také může instalovat a nastavovat aplikace potřebné pro danou práci.

Jelikož se o PC na obecním úřadě v Těmicích stará externí firma Syscom Bzenec doporučoval jsem, aby starosta neboli správce sítě dohlížel, jaké oprávnění firma nastavila ostatním zaměstnancům úřadu. Starosta stejně jako ostatní zaměstnanci mají nastavené power user oprávnění. Toto nastavení nepovažuji za příliš vhodné, protože všichni mohou provádět na PC cokoliv. Pro zvýšení bezpečnosti jsem doporučoval, aby toto nastavení používal pouze pan starosta a ostatní uživatelé se přihlašovali pomocí uživatelského účtu. Uživatelský účet je určitým způsobem omezen. Uživatel, který vlastní tento účet, nesmí instalovat na PC určitý SW, nesmí ani tento účet nijak měnit a dávat ostatním účtům oprávnění.

V poslední řadě, co jsem vytkl, je povolení flash disků všech zaměstnanců. Stejně tak, jako u nastavení uživatelských účtů, může mít toto povolení také negativní vliv na bezpečnost důležitých dat. Význam povolení flash disků bych povolil pouze panu starostovi obce a správci sítě. Ostatním zaměstnancům bych flash disky zakázal, protože pomocí flash disků můžeme přenášet z jednoho počítače do druhého viry nebo kopírovat na flash disky informace, se kterými na úřadě pracují. Zakázáním flash disků můžeme určitě také zvýšit bezpečnost dat.



Obrázek 12: Zákaz flash disků. [vlastní]

Na obrázku č. 12 vidíme jak provést zákaz flash disků. Nejprve klikneme na „Start“ a poté vybere „Spustit“. Jakmile se otevře okno, zadáme příkaz „regedit“ a potvrdíme. Následně vyhledáme a vybereme v rozšířeném stromě: "HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ UsbStor". Otevřeme „Start“, kdy do hodnoty údajů zadáme hodnotu „4“. Musíme se ujistit, že máme zvolenou šestnáctkovou číselnou soustavu. Jakmile to provedeme, nebudeme moci komunikovat pomocí flash disků, ale všechny připojené periferie budou dostávat napájení.

7.7 Používání hesel

Každý zaměstnanec obecního úřadu musí používat hesla pro přihlášení na PC a ke všem aplikacím, které vyžadují přihlašování pomocí hesla. Hesla stejně jako uživatelské účty slouží k základnímu bezpečnostnímu opatření před vstupem nežádoucích osob do systému. Tvorbu hesla nesmí zaměstnanci nijak podceňovat, protože nevhodně zvolené heslo může vést ke snadnému prolomení. Každý zaměstnance je zodpovědný za výběr svého hesla a každý obecní úřad by měl stanovit standard pro tvorbu hesla. Jednotliví zaměstnanci se musí podle daného standardu řídit a měli by používat silná hesla. Můžeme mít nejlepší zabezpečení systému, ale pokud útočník zná přístupové údaje k přihlášení do systému, úroveň bezpečnosti významně klesá.

Každý zaměstnanec obecního úřadu musí své heslo pravidelně aktualizovat, aby se zabránilo snadnému prolomení hesla. Všechny zaměstnance musíme upozornit, aby se vyvarovali následujícím chybám:

- nesmí používat hesla jako vlastní jméno, název obce, jméno dítěte,
- nesmí používat hesla typu: „heslo“ nebo „1234“,
- nesmí své heslo napsat na papírek a nechat ho ležet např. v šuplíku nebo vedle počítače,
- nesmí používat stejné heslo příliš dlouho,
- nesmí svěřit své heslo další osobě.

Zaměstnanci by měli používat hesla, které si snadno zapamatují, ale zároveň by se měli vyvarovat výše zmíněným chybám. Pro tvorbu správného a silného hesla jsem doporučil, aby obec vytvořila pravidla pro tvorbu hesla, která budou rozdílná pro správce, neboli v našem případě pana starostu obce, a ostatní zaměstnance. Správce musí klást důraz na sílu svého zvoleného hesla. Ostatní zaměstnanci nemusí klást až tak velký důraz na hesla, ale měli by také používat dostatečně silná hesla. Zaměstnanci nesmí své hesla svěřovat ostatním osobám a to ani v případě, pokud to po nich požaduje správce či vedoucí oddělení. V žádném případě nesmí heslo říkat kolegyním nebo kolegům. V případě, že s počítačem delší dobu nepracujeme, je vhodné nastavit spořič obrazovky tak, aby se zadalo heslo pro zahájení práce. Díky tomu zabráníme manipulování s počítačem, pokud nejsme u něj právě přítomni.

Doporučené pravidla pro tvorbu silného hesla:

- musí obsahovat minimálně osm znaků,
- musí se kombinovat malá i velká písmena a číslice,
- může obsahovat speciální symboly,
- musí se pravidelně aktualizovat alespoň v půl ročních intervalech a musí se výhradně lišit od předcházejícího hesla,
- za silné heslo můžeme považovat např. 08io1fRZ.

7.8 Aktualizace

Jak bylo zmíněno v předešlé kapitole, obecní úřad nechává obstarávat svá PC externí firmou Syscom Bzenec. Firma provádí pravidelné aktualizace, protože aktualizace jsou velmi důležité. V případě, že by firma neprováděla pravidelné aktualizace, můžeme umožnit

útočníkovi, aby snadněji využil bezpečnostních děr a dostal se do počítače. Pro spoustu správců sítě je nejjednodušší, a také bych to i doporučoval, aby se důležité aktualizace prováděly automaticky. Můžeme je ale provádět i manuálně. Nejnovější důležité aktualizace od firmy Microsoft můžeme získat v Centru zabezpečení, kde je vyhledáme a poté nainstalujeme. Zde také nastavíme, aby se aktualizace od firmy Microsoft instalovaly automaticky. Díky tomu docílíme, že budeme mít aktuální software a nemůže se nám stát, že na určitou aktualizaci zapomeneme.

Aktualizovat musíme také i jiné programy od jiných výrobců. Jednotlivé aktualizace najdeme vždy na stránce daného výrobce k určitému produktu.

Důležité je mít aktuální internetový prohlížeč a hlavně antivirový program, který si pomocí aktualizací doplňuje virovou databázi, díky které odhaluje viry a tím snižuje riziko infikace systému.

7.9 Školení zaměstnanců

Obecní úřad žádné školení svých zaměstnanců neprovádí. Může to mít však negativní dopad na celkovou bezpečnost. Pro zvýšení ochrany bezpečnosti a odborné kvalifikace zaměstnanců jsem doporučoval, aby obecní úřad prováděl pravidelná školení v určitých intervalech. Školení by se mělo provádět alespoň jednou ročně. Proškolit by se měli jak noví zaměstnanci, tak i stávající.

Zde uvedu několik základních bodů, které jsem doporučil, aby obecní úřad provedl v rámci školení. Školení určitě také pomůže k nápravě bezpečnosti.

- vysvětlit zaměstnancům, že musí zabezpečovat dokumenty, se kterými právě nepracují,
- pokud tisknout důležité dokumenty, musí si je ihned vzít a nenechat je nikde ležet bez dohledu,
- zaměstnanci musí na PC používat jen programy určené k jejich práci a navštěvovat webové stránky, které s danou prací souvisí,
- v případě odchodu zaměstnance ze své kanceláře se musí ihned odhlásit z PC,
- po skončení práce musí veškerá svá data uložit a zálohovat
- zaměstnanci musí evidovat své příchody a odchody.

7.10 Požadavky na správce sítě

Manažer informačního systému na malé obci zaujímá pozici, která vyžaduje kromě řídících schopností i odbornost v rámci technologií. Dále musí zajistit vybudování, implementaci a neustálé zlepšování informační bezpečnosti.

Manažer informačního systému musí plnit řadu funkcí a úkolů:

- musí prosazovat bezpečnost informací,
- musí se neustále učit novým věcem z důvodu realizace nezbytných bezpečnostních opatření,
- musí provádět stanovené plány ohledně zvládání rizik a musí dohlížet na splnění všech plánovaných úkolů,
- musí monitorovat výkonnost systému řízení bezpečnosti informací a bezpečnostních opatření,
- musí připravovat podklady pro přezkoumání systému.

Z důvodu vysokých nároků na manažery informační bezpečnosti, je dobré absolvovat kurz a získat mezinárodně uznávaný certifikát „Information Security Manager podle ISO/IEC 27001“.

Tento kurz je tvořen třemi částmi:

- ISMS standardy ISO 27001 a ISO 27002 – po ukončení tohoto kurzu účastníci znají procesy a požadavky k implementaci norem ISO 27001 a ISO 27002. Mají také základy pro neustále zlepšování systému,
- psychologické základy pro manažera IS – účastníci jsou schopni prosazovat podnikové cíle na úrovni pracovních vztahů, také se zde naučí jak vytvářet a vést projektové týmy,
- právní základy pro manažera IS – zde se účastnící seznámí se zákony ohledně informační bezpečnosti. [29]

8 SROVNÁNÍ OBECNÍHO ÚŘADU S MĚSTSKÝM ÚŘADEM

V této části své práce srovnám zabezpečení informačního systému z pohledu malé obce Těmice, která má 904 obyvatel s větším městem Veselí nad Moravou, které má 12476 obyvatel.

	Obecní úřad Těmice	**Městský úřad Veselí nad Moravou**
Počet počítačů	3	100
Operační systém	Windows 10	Windows 7, Windows 10
Firewall	Windows firewall	Sophos
Antivirový program	ESET Smart Security	ESET Smart Security
Zálohování dat	starosta sám, zaměstnan-cům externí firma	Zaměstnanci
Omezení oprávnění	NE	NE
Flash disky	Povoleny	Povoleny
Aktualizace	Externí firma Syscom	Správce sítě
Školení zaměstnanců	NE	NE
Fyzická bezpečnost	Špatně	Správně

Tabulka 7: Srovnání obecního a městského úřadu. [vlastní]

V následující tabulce jsem provedl srovnání obecního a městského úřadu. Obecní úřad v Těmicích používá pro svou práci jen tři PC, zatímco městský úřad ve Veselí nad Moravou používá celkem 100. Ty obnovují v intervalu pěti až šesti let. Oba úřady používají Windows 10, ale městský úřad používá na nejstarších i Windows 7 Professional. Jelikož se jedná o úřad, doporučoval jsem, aby městský úřad používal na všech PC nejnovější operační systém. Jako antivirový program oba úřady používají antivir od firmy ESET verzi ESET Smart Security. Jak už jsem zmiňoval v předešlé kapitole, úřady pracují s velmi důležitými a citlivými daty a proto jsem doporučil úřadům používání nejvyšší nabízené verze ESET Smart Security Premium. Co se týče firewallu, tak obecní úřad používá zabudovaný Windows firewall, zatímco městský úřad používá externí firewall Sophos. V tomto případě určitě poskytne lepší bezpečnost externí firewall oproti zabudovanému přímo v systému

Windows. Na základě tohoto poznatku jsem doporučil, aby obecní úřad začal také používat některý z nabízených externích firewallu na trhu. Oba úřady poskytují zaměstnancům veškerou volnost a všichni mají na svých PC nastavené power user oprávnění. Stejně tak flash disky mají oba úřady povoleny na všech PC. Oběma úřadům jsem doporučil zakázání flash disků svým zaměstnancům a povolit je pouze správcům sítě a starostovi obce. Postup, jak zakázat flash disky, jsem zmiňoval v předešlé kapitole. Co se týče aktualizací, městský úřad je nechává na svých zaměstnancích, takže se může stát, že nemají delší dobu aktuální programy, které denně využívají. I zde jsem doporučil, aby na aktualizace dohlížel a prováděl je sám správce sítě. Bude mít tak přehled o celkovém stavu daných PC. Jelikož obecní úřad nechal svá PC obstarávat externí firmou Syscom Bzenec, může nastat stejný problém jako na městském úřadě. Proto i zde má pan starosta obce dohlížet nad aktuálností programů a celkovým stavem daných PC. Zálohování městský úřad provádí pravidelně každý den, kdy zálohování nechává na svých zaměstnancích. I tento postup nepovažuji za nejlepší, co se týče bezpečnosti dat. Ke značnému zlepšení by mohlo pomoci, kdyby zálohování dat prováděl sám správce sítě, protože má určitě lepší znalosti a nemůže se stát, že zálohování provede špatně. Obecní úřad v Těmicích si nechává zálohovat data již zmíněnou externí firmou, ale i pan starosta si svá data zálohuje zcela sám na externí pevné disky. To považuji za správné řešení. Fyzickou bezpečnost mají oba úřady řešenou zcela odlišně. Městský úřad, co se týče umístění serverů, ji řeší správně. Servery má umístěny v nejvyšších patrech budovy. Místnost je vybavena protipožárními čidly a izolací proti vodě. Před místností se nachází klávesnice, kdy správce sítě zadá pro přístup heslo a poté může vstoupit do místnosti. Oproti tomu obecní úřad fyzickou bezpečnost nijak neřeší. Jak jsem zmiňoval, data zálohuje na externí pevné disky, ale neukládá je do žádné speciální místnosti, jakou má městský úřad. Tento postup považuji za velmi závažné pochybení, protože nikdy nemůžeme vědět, co se může stát. K částečné nápravě by stačilo umístit externí disky alespoň do protipožárního sejfu. Fyzický přístup oba úřady do jednotlivých místností neevidují, stejně tak, jako neevidují příchody a odchody svých zaměstnanců. V obou úřadech jsem doporučil zřízení čipových karet svým zaměstnancům. Budeme mít jednoznačný přehled o vstupu do jednotlivých místností a také budeme evidovat příchody a odchody zaměstnanců. Z hlediska bezpečnosti městský úřad má celou budovu napojenu na Městskou policii ve Veselí nad Moravou, takže při neoprávněném vstupu do budovy, případném požáru, policie ihned přijede a místo zabezpečí. Obecní úřad na malé obci nemá

ani to základní zabezpečení (mříže na oknech, zabezpečovací systém, protipožární sejf na uložení dat, atd.…).

Pan starosta mi ochotně objasnil současnou situaci v obci, za což mu patří moje velké poděkování a byl jsem velmi rád, že naslouchal mému doporučení ohledně ochrany a zabezpečení PC, ukládaných dat a celkového zabezpečení obecního úřadu.

ZÁVĚR

Bez informačních technologií se neobejde žádný obecní úřad. To platí stejnou měrou jak pro firmy, tak pro organizace veřejné správy. Je nezbytné, aby zajištění ochrany dat a fungování informačního systému bylo vyžadováno po celou dobu jeho životního cyklu. Je důležité, aby uživatelé informačního systému věděli, jaká nebezpečí hrozí, a co se může stát, pokud nebudou dodržovat stanovené postupy.

Svou bakalářskou práci jsem zpracoval na téma „Stanovení požadavků na bezpečnost destopových systémů a mobilních zařízení malé obce“. V teoretické části této práce byly definovány základní pojmy týkající se bezpečnosti informačního systému. Dále zde byly představeny možné hrozby, které nejčastěji ohrožují informační systém. Dané hrozby minimalizujeme pomocí ochrany dat, která byla rozdělena do tří kategorií. Jednotlivými kategoriemi byla: fyzická, datová a personální bezpečnost. V praktické části jsem se zabýval návrhem postupů řízení bezpečnosti informačních systémů v malé obci. Dále výběrem vhodného antivirového zabezpečení z pohledu ochrany dat na PC i mobilních zařízení pro specifické prostředí malé obce. Kromě antivirového zabezpečení, byly stanoveny postupy zajišťující fyzickou bezpečnost, která je velmi důležitá pro uchování zálohovaných dat na serverech. V případě podcenění fyzické bezpečnosti může obec ztratit veškerá svá data. Nutností je také provádět pravidelná školení uživatelů o informační bezpečnosti.

Cílem mé bakalářské práce je poskytnutí praktických informací a doporučení pro výběr antivirového programu, návrh vhodných opatření, které by mohla zvýšit bezpečnost informačního systému v malé obci. I ten nejlepší informační systém nebo správce počítače nemůže zajistit ochranu dat, pokud uživatelé nedodržují základní pravidla týkající se bezpečnosti.

Na Městském úřadu ve Veselí nad Moravou a Obecním úřadu v Těmicích, kde jsem svou práci konzultoval, byla fyzická bezpečnost řešena odlišně. Ve Veselí byly servery umístěny v nejvyšších patrech budovy a místnost byla opatřena veškerými bezpečnostními opatřeními, v Těmicích nebyla vůbec řešena. Školení zaměstnanců na obou pracovištích bylo mnou doporučeno tak, aby probíhalo v pravidelných ročních cyklech. Co se týče jednotlivých PC, tak zaměstnanci mají přístup ke všem nastavením a můžou provádět cokoliv, nemají žádná omezení. Takováto volnost zaměstnanců má negativní dopad na bezpečnost dat. Zaměstnanci by v pracovní době měli mít přístup pouze k aplikacím, které používají ke své práci a neměli by s PC provádět žádné jiné činnosti.

Na závěr je dobré připomenout, že bezpečný informační systém nelze nikdy stoprocentně navrhnout, proto musíme dodržovat všechna pravidla a postupy pro snížení hrozeb, a to včetně pravidelných uživatelských školení zaměstnanců.

SEZNAM POUŽITÉ LITERATURY

[1] HANÁČEK, Petr a Jan STAUDEK. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000. ISBN 80-238-5400-3.

[2] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů*. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978 - 80 - 7454 - 312 - 8.

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

[4] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: ComputerPress, 2004. ISBN 80-251-0106-1.

[5] *Bezpečnostní politika firmy* Pardubice, 2007. Bakalářská práce. Univerzita Pardubice, Fakulta Ekonomicko-správní.

[6] *Řízení vybraných bezpečnostních rizik v podnikových informačních systémech*. Zlín, 2006. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky.

[7] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009. Knihovnicka.cz. ISBN 978-80-7399-731-1.

[8] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: GradaPublishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

[9] *Získávání dat z cizího počítače a možnosti aktivní obrany* [online]. Zlín, 2010 [cit. 2017-02-08]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/14307/hejtman_2010_dp.pdf?sequence=1. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky.

[10] Autentizace a autorizace [online]. trisul [cit. 2017-02-9]. Dostupné z: http://www.trisul.cz/bezpecnost-autentizace-autorizace/

[11] Antivirový program. *Antivirové centrum* [online]. [cit. 2017-02-10]. Dostupné z: http://www.antivirovecentrum.cz/antiviry.aspx

[12] RAID. *svethardware*[online]. [cit. 2017-02-11]. Dostupné z: http://www.svethardware.cz/nas-prace-s-daty-a-sdileni-pro-pokrocile/37490-2

[13] RAID10. *dell*[online]. [cit. 2017-02-12]. Dostupné z: http://www.dell.com/support/Article/cz/cs/czbsdt1/SLN129581/CS

[14] VPN.*technet.microsoft*[online]. [cit. 2017-02-13]. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd469653(v=ws.11).aspx

[15] Heslo.*antimalware*[online]. [cit. 2017-02-14]. Dostupné z: https://www.antimalware.cz/blog/jak-vytvorit-bezpecne-heslo

[16] Moderní správa IT ve firmě. In: Http://www.businessit.cz/ [online]. Praha: Bispiral, 2011 [cit. 2016-12-20]. Dostupné z: http://www.businessit.cz/ebooks/moderni_sprava_IT_ve_firme.pdf

[17] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Brno: ComputerPress, 2004. ISBN 80-251-0178-9.

[18] Zálohování. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): WikimediaFoundation, 2017 [cit. 2017-03-27]. Dostupné z: https://cs.wikipedia.org/wiki/Z%C3%A1lohov%C3%A1n%C3%AD_dat

[19] *Mobilní Antivirové programy* [online]. antivirovecentrum, 2012 [cit. 2017-04-18]. Dostupné z: https://www.antivirovecentrum.cz/clanky/srovnani-antiviru-pro-mobilni-zarizeni.aspx

[20] *BYOD* [online]. Lupa.cz, 2014 [cit. 2017-04-18]. Dostupné z: http://www.lupa.cz/clanky/na-co-si-dat-pozor-pri-pouzivani-byod-zarizeni-ve-firmach/?utm_expid=.1rnVC9uKTLGPIiC_juvx9A.0&utm_referrer=https%3A%2F%2Fwww.google.cz%2F

[21] *BYOD* [online]. managementmania.com, 2016 [cit. 2017-04-18]. Dostupné z: https://managementmania.com/cs/byod-bring-your-own-device

[22] DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[23] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cybersecurityglossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 9788072514366.

[24] *Bezpečnostní role dle zákona o kybernetické bezpečnosti* [online]. govcert.cz [cit. 2017-04-18]. Dostupné z: https://www.govcert.cz/cs/faq/vyhlaska-o-kyberneticke-bezpecnosti/

[25] *Egovernment* [online]. Praha: mvcr.cz, 2017 [cit. 2017-04-18]. Dostupné z: http://www.mvcr.cz/clanek/co-je-egovernment.aspx

[26] *Czech POINT* [online]. Praha: mvcr.cz, 2017 [cit. 2017-04-18]. Dostupné z: http://www.mvcr.cz/clanek/czech-point-czech-point.aspx

[27] *Datové schránky* [online]. Praha: mvcr.cz, 2017 [cit. 2017-04-18]. Dostupné z: http://www.mvcr.cz/clanek/datove-schranky-datove-schranky.aspx

[28] *Základní registry* [online]. Praha: mvcr.cz, 2017 [cit. 2017-04-18]. Dostupné z: http://www.mvcr.cz/clanek/zakladni-registry-zakladni-registry.aspx

[29] *Manažer informační bezpečnosti* [online]. Praha, http://cz.cis-cert.com/, 2017 [cit. 2017-04-18]. Dostupné z: http://cz.cis-cert.com/Trainings/Information-Security/IS-Manager/Information-Security-Manager-ISO-27001.aspx

[30] *Informační systém veřejné správy* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/informacni-systemy-verejne-spravy.aspx

[31] *Zákon č. 365/2000 Sb.,* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx

[32] *Vyhláška č. 64/2008 Sb.,* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/vyhlaska-c-64-2008-sb-o-forme-uverejnovani-informaci-souvisejicich-s-vykonem-verejne-spravy-prostrednictvim-webovych-stranek-pro-osoby-se-zdravotnim-postizenim-vyhlaska-o-pristupnosti-10.aspx

[33] *Vyhláška č. 53/2007 Sb.,* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/vyhlaska-c-53-2007-sb-o-referencnim-rozhrani.aspx

[34] *Vyhláška č. 52/2007 Sb.,* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/vyhlaska-c-52-2007-sb-o-postupech-atestacnich-stredisek-pri-posuzovani-zpusobilosti-k-realizaci-vazeb-isvs-prostrednictvim-referencniho-rozhrani.aspx

[35] *Vyhláška č. 530/2006 Sb.,* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/vyhlaska-c-530-2006-sb-o-postupech-atestacnich-stredisek-pri-posuzovani-dlouhodobeho-rizeni-isvs.aspx

[36] *Vyhláška č. 529/2006 Sb.,* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/vyhlaska-c-529-2006-sb-o-dlouhodobem-rizeni-informacnich-systemu-verejne-spravy.aspx

[37] *Vyhláška č. 528/2006 Sb.,* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/vyhlaska-c-528-2006-sb-o-informacnim-systemu-o-informacnich-systemech-verejne-spravy.aspx

[38] *Vyhláška č. 469/2006 Sb.,* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/vyhlaska-c-469-2006-sb-o-informacnim-systemu-o-datovych-prvcich.aspx

[39] *Atestace* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/udelene-atesty-574971.aspx

[40] *Atestace* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/udelene-atesty-574971.aspx

[41] *Atestační střediska* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/atestacni-strediska-s-poverenim-k-provadeni-atestaci-udelenym-podle-novely-zakona-c-365-2000-sb.aspx

[42] *Akreditace* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.mvcr.cz/clanek/atestace-a-akreditace-akreditace.aspx

[43] *Český institut pro akreditaci, o. p. s.* [online]. Praha: mvcr.cz, 2017 [cit. 2017-07-09]. Dostupné z: http://www.cia.cz/o-nas.aspx

[44] *IS DP.* [online]. Praha: www.sluzby-isvs.cz, 2017 [cit. 2017-07-09]. Dostupné z: https://www.sluzby-isvs.cz/ISDP/DefaultSSL.aspx

[45] *IS o ISVS.* [online]. Praha: www.sluzby-isvs.cz, 2017 [cit. 2017-07-09]. Dostupné z: https://www.sluzby-isvs.cz/ISoISVS/Views/Public/Login.aspx?action=get

[46] *Kybernetická bezpečnost* [online]. Praha: http://www.kybernetickyzakon.cz/, 2014 [cit. 2017-07-09]. Dostupné z: http://www.kybernetickyzakon.cz/

[47] *Těmice* [online]. Těmice: Temice.cz, 2014 [cit. 2017-07-09]. Dostupné z: http://www.temice.cz/historie.html

[48] *Vztah úrovně bezpečnosti v organizaci [online*]. Praha: 2012 [cit. 2017-07-09]. Dostupné z: https://is.bivs.cz/th/19112/bivs_b/BP_Vesely.pdf

[49] *Zámek HW [online*]. [cit. 2017-07-09]. Dostupné z: http://www.fujitsu.com/cz/Images/W-CM20381_tcm58-13523.png

[50] *Zámek PC skříně [online*]. [cit. 2017-07-09]. Dostupné z: http://www.noblelocks.com/desk/NG76.html

[51] *RAID 6 [online*]. [cit. 2017-07-09]. Dostupné z: https://www.zive.cz/clanky/prehled-vsech-rezimu-raid---rychlejsi-a-bezpecnejsi-

ukladani-dat/raid-6-7-adg-30-50-53-/-zhodnoceni/sc-3-a-111138-ch-27728/default.aspx

[52] *Lokalizace obecního úřadu Těmice [online*]. [cit. 2017-07-09]. Dostupné z: https://mapy.cz/zakladni?x=17.2661351&y=49.0018901&z=17&base=ophoto&source=firm&id=354310&q=T%C4%9Bmice

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
BYOD	Bring Your Own Device
CD	Compact Disc
ČIA	Český institut pro akreditaci
DES	Data Encryption Standard
DVD	Digital Video Disc
FTP	File Trasfer Protocol
HW	Hardware
HTTP	HyperText Trasfer Protocol
ICT	Information and Comunication Technology
IČO	Identifikační číslo organizace
ID	Identification
IDEA	International Data Encryption Algorithm
IP	Internet Protocol
IS	Information System
IS/ICT	Information System/ Information and Comunication Technology
ISO	International Organization for Standardization
IEC	International Electrotechnical Commision
ISDP	Informační systém o datových prvcích
ISMS	Information Security Management System
ISVS	Informační systém veřejné správy
OS	Operating System
OS DOS	Operating System Disc Operating System
OSI	Open Systems Interconnection

PC	Personal Computer
PDF	Portable Document Format
QC	Qualification certificate
RAID	Redundant Array of Independent Disks
SW	Software
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
TELNET	Telecommunication Network
VPN	Virtual Private Network
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK