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:	**3. února 2017**
Termín odevzdání bakalářské práce:	**30. května 2017**

Ve Zlíně dne 3. února 2017

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

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 23. 5. 2017

.....
podpis diplomanta

ABSTRAKT

Cílem této práce je základní seznámení s riziky, kterým je informační systém vystaven a následné navržení opatření bezpečnosti informačních systémů. 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 analýza rizik a definování pojmů, které se v oblasti analýzy používají. Praktická část definuje pojmy a obsahuje postupy a doporučení pro bezpečnost informačního systému a mobilních aplikací. Jedná se zde zejména o srovnání antivirového zabezpečení počítačového systému a mobilního zařízení. V závěrečné části je uvedena konzultace na Městském úřadě, která prakticky ukazuje danou problematiku.

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

ABSTRACT

The purpose of this bachelor thesis is to introduce the main risk of the information system use and it is subsequent security measures. It must be remembered that the risk of entry by an unauthorized person is very high these days. The theoretical part provides the reader with an insight into information security. Besides that, the definitions of the basic terms in the field of security and data protection are included. On top of that, the analysis of risk along with definitions of terms used in the field of analysis follow. The practical part defines the aforementioned basic terms and contains particular steps as well as recommendations not only for information systém security but also for mobile application security. The empirical part is focused especially on comparison of antivirus software protection computer systems to the same on protectiong mobile devices. The very last part of this work is dedicated to consultation in the town hall Veselí nad Moravou, which practically clarifies particular issues that have been chosen.

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

Na tomto místě bych rád poděkoval vedoucímu své bakalářské práce panu prof. Mgr. Romanu Jaškovi, Ph.D. za jeho věnovaný čas, odborné rady a vedení bakalářské práce.

Také bych chtěl poděkovat 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 organizace. Pomocí informací můžeme provádět statistiky dohledat spoustu jiných informací. Díky tomu 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 můžou 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 firem těžkým úkolem. Abychom zabránili hrozbám při zavádění informačního systému je dobré pro zavedení najmout specializovanou firmu. Všechny tyto technologie můžou správně fungovat, pokud jsou vytvořené 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 systému a mobilních aplikací. Tyhle 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 definicí základních pojmů z oblasti bezpečnosti informačních systémů. Dále je v téhle části popsána analýza rizik a pojmy, které se analýzy týkají. Nejdůležitější kapitolou téhle časti je ochrana dat, které je rozdělena na tři oblasti. První oblastí je fyzická bezpečnost, kde jsou definovány zejména přírodní katastrofy, které můžou informační systém ohrozit. Druhou oblastí je datová bezpečnost, kde jsou nástroje pro zvýšení bezpečnosti dat. Poslední oblastí je personální bezpečnost, která je jednou z nejdůležitějších a nejvíce podceňovanou oblastí z hlediska bezpečnosti.

Praktická část definuje jednotlivé postupy a doporučení pro bezpečnost informačního systému a informačních technologií. Většina definovaných situací se týká zabezpečení informací a dat. Je zde kladen důraz na výběr antivirového programu pro PC a také mobilních zařízení. V poslední části jsou zde uvedeny pravidla a postupy pro fyzickou bezpečnost.

Svou práci jsem konzultoval na Městském úřadě Veselí nad Moravou, kde je popsána situace ohledně bezpečnosti v praxi.

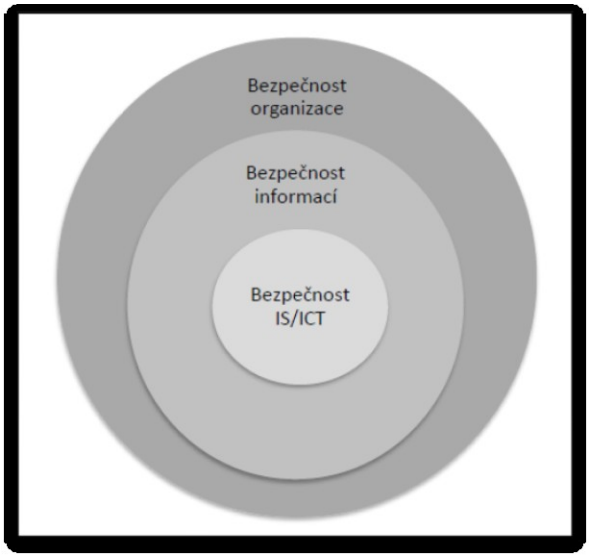
I. TEORETICKÁ ČÁST

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. Zdroj: [3]

1.1 Bezpečnostní role dle zákona o kybernetické bezpečnosti

Od 1. ledna 2015 nabyl zákon č. 181/2014 Sb., o kybernetické bezpečnosti účinnosti. Zákon upravuje práva a povinnosti osob 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. Dále také vyhláška obsahuje bezpečnostní opatření, rozsah jejich zavedení, typy 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,
- orgán nebo osoba zajišťující síť,
- správce informačního systému kritické informační infrastruktury,
- správce komunikačního systému kritické informační infrastruktury,
- správce významného informačního systému. [24]

Správci informačního, komunikačního a významného informačního systému musí zajistit odborné školení osob, které zastávají 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 informačního systému 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 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 bát nestranná a má fyzickou odpovědnost za zajištění rozvoje, 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]

1.2 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]

1.3 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. k 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]

1.4 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 technologií, 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** – sem patří 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]

1.5 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, složitost softwaru apod. [5]

Základními zranitelnými místy může 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 můžou způsobit jejich zneužití např.: odposlech,
- **lidská zranitelnost** – způsobuje největší zranitelnost např.: nezaškolení zaměstnanci.

Zranitelná místa můžou 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 můžou 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]

1.6 Hrozba a riziko

Zranitelná místa jsou vlastnostmi IS, jejichž výskyt způsobuje, že tyto místa můžou 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]

1.7 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]

1.7.1 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]

1.7.2 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. Tihle 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]

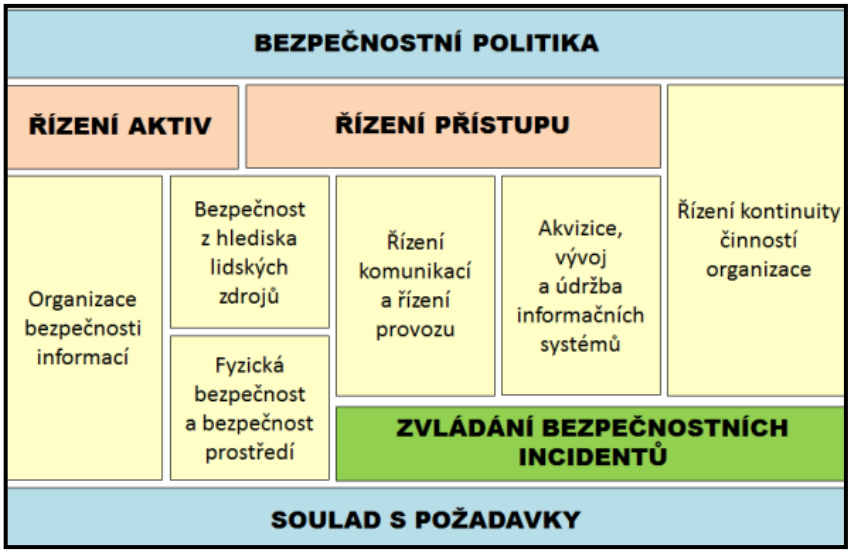
1.8 Bezpečnostní politika

Bezpečnostní politika je soubor postupů pro řízení bezpečnosti informací, která 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 rozdělena 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. Zdroj:[22]

Charakteristika 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 E-GOVERNMENT

e-Government je správa veřejných věcí, které využívají moderních elektronických nástrojů. Díky těmhle nástrojům je veřejná správa k 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 můžou 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 nahradili 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 bylo možné fungování těchto systémů, je důležité vytvořit bezpečnou infrastrukturu.

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 Datové schránky

Datové schránky jsou komunikační nástroj, který nahrazuje klasické doporučené dopisy. Slouží hlavně ke komunikaci s orgány veřejné moci. Všechny úřady musí komunikovat prostřednictvím datových schránek a s každým kdo ji má zřízenou. Datovou schránku musí mít povinně zřízenou všechny orgány veřejné moci právnické osoby zapsané v obchodním rejstříku, advokáti a daňový poradci. Ostatní si ji můžou dobrovolně zřídit. [27]

Abychom nemuseli chodit pro obálky na poštu, můžeme si zdarma zřídit datovou schránku a komunikovat tak nejen s úřady online. Díky datovým schránkám máme vždy jistotu, že se naše podání dostalo na správný úřad. Odeslanou zprávu si můžeme uložit a kdykoliv později prokázat obsah zprávy. Elektronický dokument má stejnou právní platnost jako klasický papírový. [27]

2.3 Základní registry

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

Rozdělení základních registrů:

- **registr osob** – obsahuje základní identifikační údaje o subjektech, které mají IČO, jejich provozovnách a statutárních zástupcích,
- **registr obyvatel** – obsahuje referenční údaje o fyzických osobách, které žijí na území ČR a to konkrétně jméno, příjmení, datum a místo narození, adresa místa pobytu, státní občanství, čísla identifikačních dokladů a ID datové schránky,
- **registr práv a povinností** – obsahuje údaje o vykonávaných agendách a údaje o oprávněních k přístupu k údajům v ostatních registrech,
- **registr územní identifikace, adres a nemovitostí** – slouží k evidenci územního členění státu. Obsahuje referenční údaje o stavebních objektech, pozemních, ulicích, katastrálních územích. [28]

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]

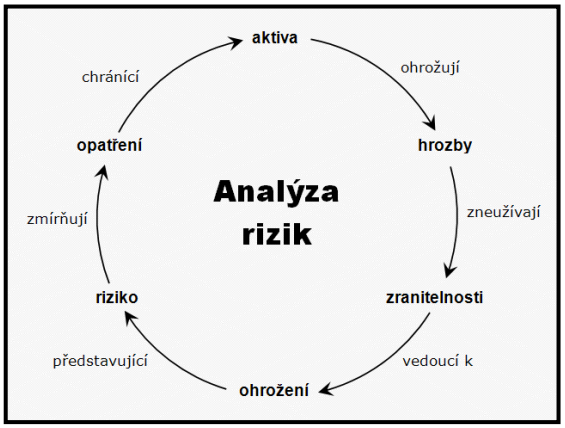
3.1 Pojmy analýzy rizik

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 hrozbou, které je můžou 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]

Musíme si uvědomit rozdíl mezi hrozbou a rizikem. Hrozby zneužívají zranitelnosti IS vedoucí k ohrožení, což je riziko, které zmírníme opatřením a chráníme tak aktiva před působením hrozeb. [7]



Obrázek 3: Analýza rizik. Zdroj:[7]

Musíme si uvědomit rozdíl mezi hrozbou a rizikem. Hrozby zneužívají zranitelnosti IS vedoucí k ohrožení, což je riziko, které zmírníme opatřením 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 systému 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 tímhle počítačem můžou provádět prakticky vše, např. mazat soubory, snadno získat 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 tyhle informace pak využít pro cílenou reklamu. Spyware se může šířit společně s několika sharewarovými programy a jejich autoři o téhle 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 uložená v podobě počítačových souborů na disku. Uložená data musíme chránit před zničením a zneužitím. Tuhle 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 tyhle 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. Takhle kontrola bývá obvykle zajištěna vrátným, který kontroluje vstup osob do objektu. Dále může být tahle 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 můžou 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. Tyhle katastrofy nemůžeme předem předvídat.

4.1.2.1 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 které patří hasicí přístroje a systémy. [4]

4.1.2.2 Zemětřesení

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

4.1.2.3 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. Tyhle 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 čemž vzniká kopie zdrojových dat. Kopie zdrojových dat bývá obvykle uložená 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 můžou být data uložená 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. Tahle 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** – tahle záloha obsahuje reflektující stav po poslední záloze a také historii přírůstkové zálohy. Také 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 můžou 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 tyhle chyby eliminovat. Máme dva druhy oprav „ hotfixy“, opravují dílčí problémy a „ patche neboli service packy“ opravují více problémů zároveň. Tyhle 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

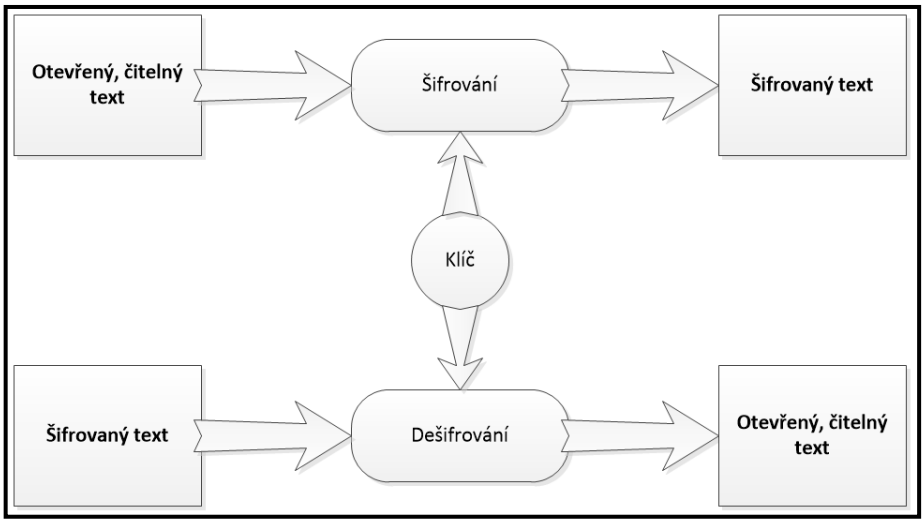
vhodné také jako ochrana před administrátory systémů, kteří nemusí mít přístup k našim datům. [2]

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.

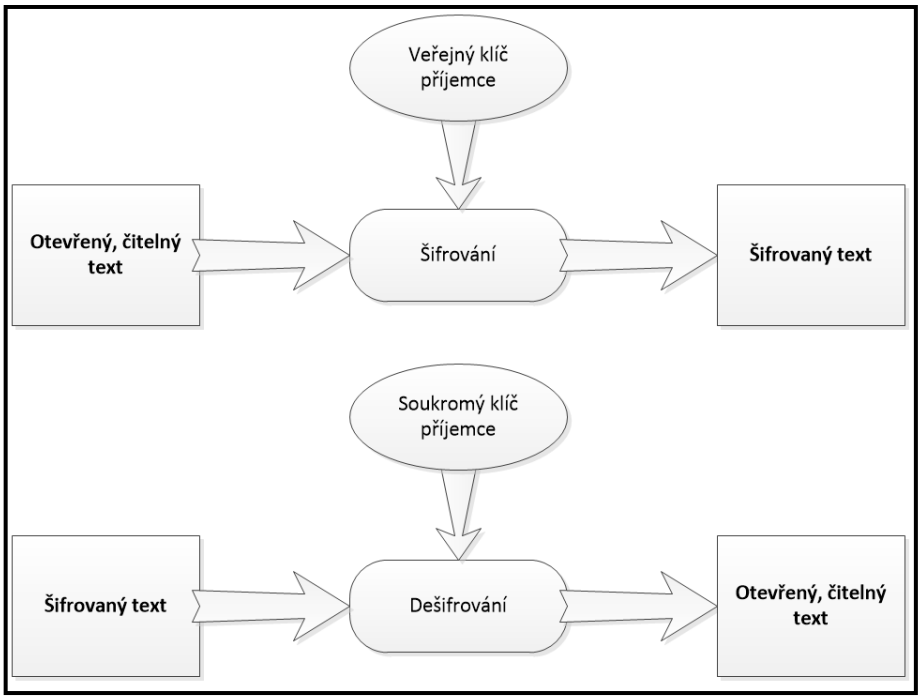
- **Symetrické šifry** – jedná se o algoritmus, který je velmi rychlý a pro šifrování a dešifrování používá stejný klíč. Rychlost vyplývá z malé výpočetní náročnosti, a proto jsou vhodné pro šifrování velkého množství dat. Dělíme je na blokové a proudové šifry. Proudové šifrují bit po bitech, ale blokové 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 4: Princip symetrické šifry. Zdroj:[2]

- **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 dostateč-

ně dlouhé klíče alespoň 128b, ale raději256b. Dále konstruovat algoritmy s využitím matematického přístupu, které umožňují útok pouze hrubou silou.[2]



Obrázek 5: Princip asymetrické šifry. Zdroj: [2]

4.2.7 Vícenásobné diskové pole

RAID je vícenásobné diskové pole nezávislých disků. Jde tedy o bezpečnost dat, pokud by selhal pevný disk. V případě selhání pevného disku jsou data ukládána na více nezávislých disků. Úroveň zabezpečení se liší podle zvoleného typu RAID pole. Mezi nejznámější typy, které se v praxi používají, patří RAID 0, RAID 1, RAID 5 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 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 tenhle 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 tyhle hesla zkouší, až získá přístupové heslo. [15]

Útok hrubou silou je velmi zdlouhavý, protože zkouší všechny možné kombinace. Avšak 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 téhle verze již můžou 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 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 můžou 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. Takhle dohoda může mít pak formu např. dodatek k pracovní smlouvě. [20]

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

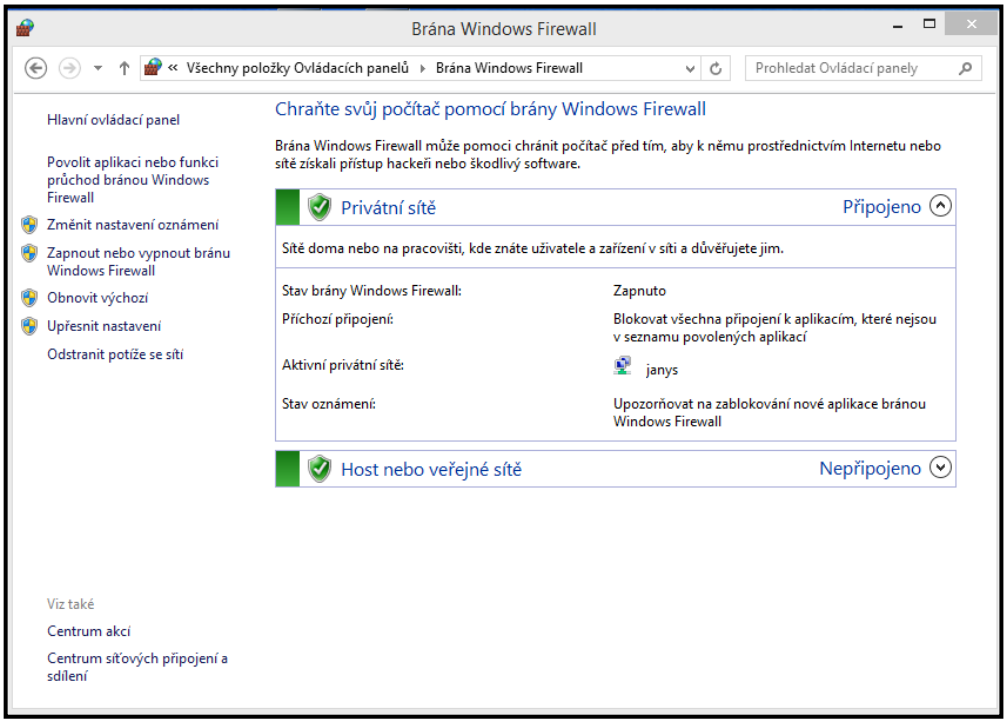
II. PRAKTICKÁ ČÁST

6 ZPŮSOB NAVRŽENÍ BEZPEČNOSTI V INFORMAČNÍCH SYSTÉMECH

V této části mé práce je popsána bezpečnost informačních systémů z hlediska opatření, která by měla obec zajistit, aby kontinuálně udržela ochranu před nežádoucími vlivy. Bezpečnostní opatření zahrnuje jak ochranu zařízení a softwaru, tak i personální bezpečnost, která je pro podnik velmi důležitá. Musíme si hlavně uvědomit, že absolutně bezpečný informační systém neexistuje a také to, že HW a SW nejsou hlavní příčinou pro nebezpečí. Hlavní příčinou je člověk, který pracuje s informačním systémem. Proto by každý uživatel informačního systému měl být řádně proškolen, aby se zmírnilo riziko nebezpečí. 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 můžou navštěvovat. Za každý informační systém je zodpovědná pověřená osoba neboli správce informačního systému. Kromě správce informačního systému musí mít každý podnik 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. Aktuálnost by se měla klást na antivirové programy, které jsou důležitou součástí každého počítače. Odpovědnost nemůže být jen stanovena, ale musí být i vyžadována,

6.1 Firewall

Systém Windows má v sobě přímo zabudovaný firewall, který nalezneme v ovládacích panelech v sekci systém a zabezpečení. Zde vidíme 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, nikdy se nedoporučuje ho vypnout. Nikdy nesmíme blokovat všechna příchozí spojení včetně aplikací, vždy musíme ponechat aktivní upozornění, abychom se mohli rozhodnout, zda novou aplikaci povolíme a bude moci komunikovat s naším PC. Některým aplikacím můžeme povolit průchod firewallem, který u nich nastavuje komunikaci buď pro veřejnou, nebo soukromou síť.



Obrázek 6: Windows firewall. Zdroj: Vlastní

6.1.1 Externí firewall

Jak již bylo zmíněno, můžeme používat také externí firewall, který bývá obvykle součástí některého z antivirových programů. Pokud bychom se rozhodli používat externí firewall musíme vždy vypnout Windows firewall. V PC může být zapnut pouze jeden.

Mezi nejznámější antivirové programy, které obsahují i firewall patří: AVG Internet Seczrity a Firewall, Avast Internet Security a Firewall a ESET Smart Security. Tyto antivirové programy jsou popsány v následující kapitole.

6.2 Antivirové zabezpečení

Antivirový program by si měl každý správce informačního systému sám vyzkoušet, zda splňuje všechny jeho požadavky. 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 tři 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.

6.2.1 ESET NOD32

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.

- **ESETNOD32** – 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 bankovnictví, ochranu před hackery a také ochranu naší sítě neboli routeru. Takhle 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 FamilySecurityPack	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 1: Porovnání programu ESET. Zdroj: Vlastní

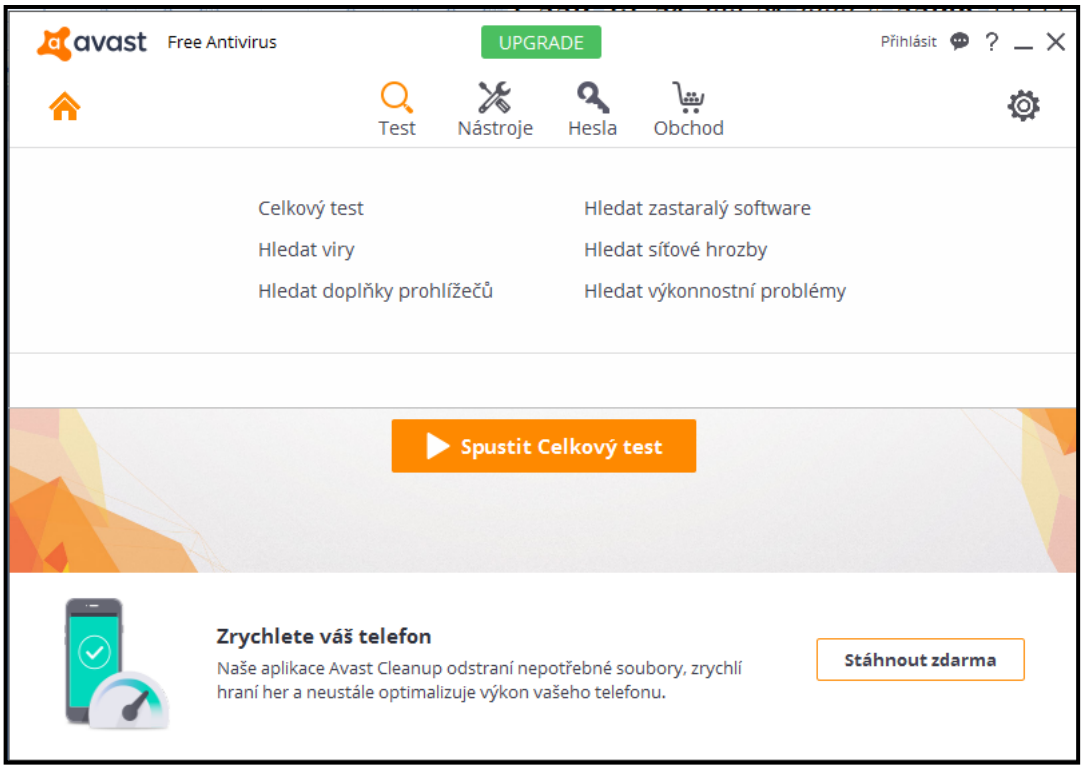
6.2.2 Avast

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 výkon-

nostní problémy. Nástroje v téhle verzi nemají firewall. K dispozici jsou: vzdálená asistence, statistika a záchranný disk.



Obrázek 7: Avast Free Antivirus. Zdroj: Vlastní

- **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. Kromě toho aplikace obsahuje 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 2: Porovnání programu Avast. Zdroj: Vlastní

6.2.3 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 prostřednic-

tvím 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 tato 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 3: Porovnání programu AVG. Zdroj: Vlastní

6.2.4 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.

6.2.5 Závěr

Jako antivirový program bych doporučil pro firmy i domácnost ESET NOD32, který sice nenabízí oproti dvěma zmíněným programům free verzi, ale nabízí nejlepší zabezpečení dat. Pro domácnost bych doporučil verzi ESET Smart Security, ale pro firmy ESET Smart Security Premium, který umožňuje také šifrování dat a správu hesel.

6.3 Antivirové zabezpečení mobilních zařízení

Na úvod je 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 tohle 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 i licencovány a podporují např. AntiTheft ochranu.

Srovnáme si zde antivirové programy od firem Avast, AVG a ESET.

6.3.1 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.

6.3.2 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.

6.3.3 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 - jak je stav baterie, viditelnost bluetooth a běžící procesy.

6.3.4 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 4: Srovnání mobilních antivirových programů. Zdroj: [19]

6.3.5 Závěr

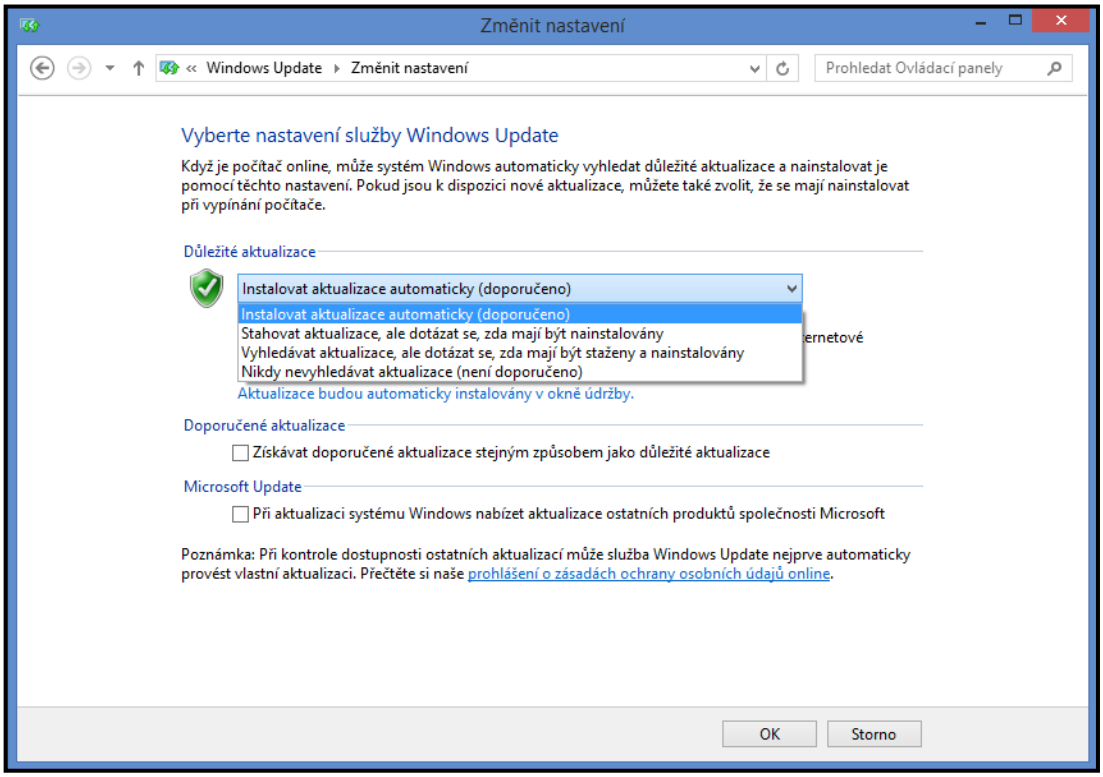
Jako antivirový program pro mobilní zařízení bych doporučil Avast Free Mobile Security, který je zcela zdarma. Díky tomu, že je zcela zdarma podporuje také rozšířené funkce, jako jsou: firewall a AntiTheft, které jsou u ostatních programů placené.

6.4 Aktualizace

Aktualizace je velmi důležitá. Pokud neprovádíme aktualizace, umožňujeme útočníkovi, aby využil bezpečnostní díry, díky kterým se může dostat do počítače. Pro spoustu uživatelů je nejjednodušší a také se to i doporučuje, aby se důležité aktualizace prováděly automaticky, ale můžeme je provádět i manuálně. Uživatelé systému Windows můžou získat nejnovější aktualizace od firmy Microsoft v Centru zabezpečení, kde si je můžou vyhledat a poté nainstalovat. Zde si také nastavují, 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 by se měly také 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.



Obrázek 8: Windows update. Zdroj: Vlastní

6.5 Používání hesel

Hesla jsou nezbytná pro zabezpečení počítačů, protože pomocí hesel se přihlašujeme k danému zařízení. Nevhodně zvolené heslo může vést ke snadnému prolomení a tím usnadnění nežádoucím osobám vstupu do systému. Proto je každý zaměstnanec zodpovědný za výběr svého hesla. Každá organizace by měla stanovit standard pro tvorbu hesel. Jednotliví zaměstnanci se musí podle daného standardu řídit a měli by používat silná hesla. Můžeme mít nejlepší zabezpečení systému, ale pokud útočník zná naše heslo k přihlášení do systému, není nám to nic platné.

Nejčastější chyby, kterých se uživatel dopouští pří používání hesla:

- používá hesla jako vlastní jméno, název firmy, jméno dítěte,
- používá hesla typu: „heslo“ nebo „1234“,
- své heslo napsal na papírek,
- heslo si několik měsíců nezměnil,
- používá stejné heslo příliš dlouho,
- svěřil své heslo další osobě.

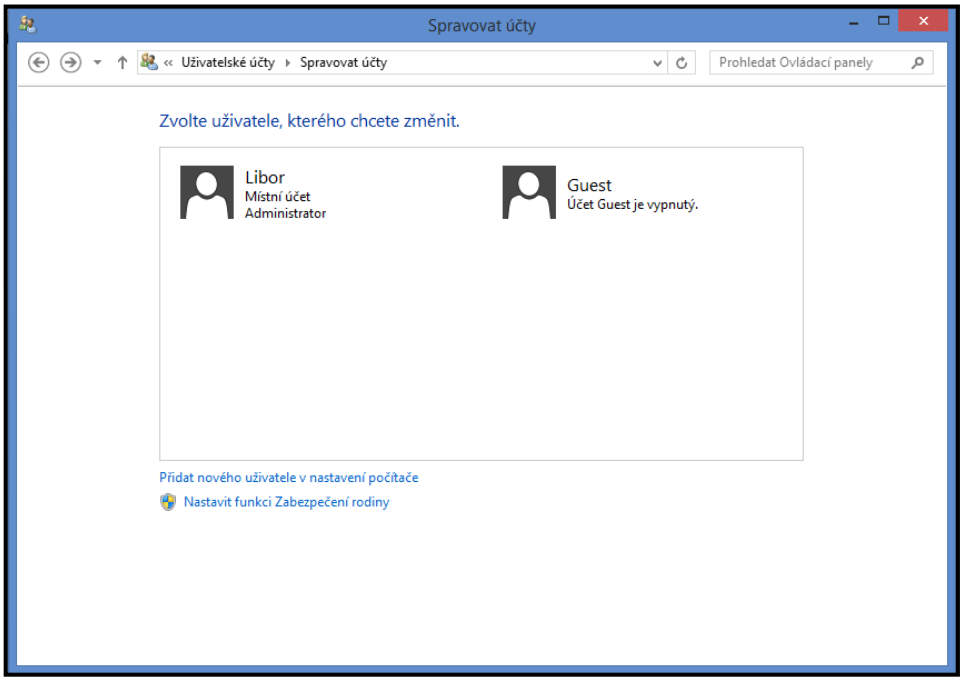
Uživatelé by měli používat hesla, které si snadno zapamatují, ale zároveň by se měli vyvarovat výše zmíněným chybám. Pro tvorbu správného a silného hesla se doporučuje vytvářet různá pravidla v organizaci, které jsou rozdílná pro správce a jednotlivé uživatele. Správci a vedoucí oddělení by především měli klást důraz na sílu 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 ve firmě. 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.

Silné heslo by mohlo být charakterizováno následujícími vlastnostmi:

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

6.6 Uživatelské účty a oprávnění

Uživatelské účty jsou jednou z nejzákladnějších bezpečností, jak můžeme zabezpečit náš počítač. Každý uživatelský účet by měl být zabezpečen pomocí hesla. Uživatelské účty můžeme rozdělit 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. Správcem PC by měla být jen jedna osoba. Ostatní uživatelé by se měli přihlašovat pomocí uživatelského účtu. Uživatelský účet je určitým způsobem omezen. Uživatel, který vlastní tenhle účet, nesmí instalovat na PC určitý SW, nesmí ani tenhle účet nijak měnit a dávat ostatním účtům oprávnění. Posledním účtem je účet host, který je ve výchozím nastavení vypnut. Tenhle účet není vhodný pro aktivní používání, slouží tedy pro občasné přihlášení osob, které nevlastní na určitém PC uživatelský účet.



Obrázek 9: Uživatelské účty. Zdroj: Vlastní

6.7 Zálohování dat

Data, o která nechceme přijít, bychom měli zálohovat minimálně na dvě úložiště. Pevný disk v PC má omezenou životnost a může tak kdykoliv přestat fungovat a tím ztratíme všechna naše data.

Máme několik možností, jak můžeme naše data zálohovat.

- **Zálohování na externí disk** – jedná se o spolehlivou ochranu dat před poškozením celého PC. Po vytvoření zálohy je nutné odpojit externí disk od PC, aby se do něj nedostal škodlivý software. Externí disk bychom neměli nechávat volně ležet u PC, vždy by měl být řádně uschován.
- **Zálohování na flash disk** – Jedná se o zálohování malého množství dat. Na flash disky bychom měli zálohovat data, se kterými chceme pracovat pravidelně nebo přenášet práci domů.
- **Zálohování na další pevný disk** – Pokud máme v PC dva fyzické pevné disky, je dobré zálohovat data na druhý disk. V případě poruchy jednoho z disku zůstanou data uložená na druhém disku.
- **Zálohování na cloud** – Jedná se o stále využívanější zálohování. Výhodou je, že data máme vždy k dispozici, pokud jsme připojeni k Internetu. Neměli bychom na

cloud ukládat citlivá data, protože data uložená na cloudu můžou být přístupná majiteli cloudu.

- **Zálohování na síťová úložiště** – Jedná se o zálohování dat ve firmách. Uživatelé ukládají svá data do sdíleného úložiště na serveru. Za tato data pak zodpovídá správce sítě, který tahle data pak dále zálohuje.

Protože počítač je pouze zařízení, které nemá doživotní životnost, musíme proto klást důraz na zálohování dat. Nikdy nevíme, kdo se nám dostane do systému nebo jaké nežádoucí vlivy můžou ohrozit PC. Data musíme zálohovat vždy, jakmile vykonáme určitou práci.

6.8 Fyzická bezpečnost

Pokud se bavíme o fyzické bezpečnosti, je důležité mít servery a dokumenty umístěny v místnostech, které jsou izolovány proti vodě a obsahují protipožární opatření. Osobní počítače, které slouží zaměstnancům, musí být umístěny v izolovaných skříních, aby nedošlo ke zničení PC. Podstatnou součástí je také fyzický přístup, kdy všechny místnosti by měly obsahovat: zámky, alarmy, evidenci návštěvníků a jednotlivá zařízení by měla být označena. Abychom zajistili evidenci zaměstnanců, je dobré jim zřídit čipovou kartu, pomocí které budou do jednotlivých místností vstupovat. Tak budeme vědět, kdo se v jednotlivých místnostech pohybuje a v jakém okamžiku.

Dodržování následujících bodů by mělo vést k zajištění fyzické bezpečnosti.

- Jednotlivé místnosti opatřit 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 servery 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 se servery a důležitými dokumenty je nutné umístit do nejvyšších pater budovy z důvodu povodní a opatřit je protipožárním opatřením. Také by tyto místnosti neměly obsahovat žádná okna,
- 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,

- Pokud si zaměstnanci berou zařízení jako tablety, notebooky domů, musí se k nim chovat jako ve své kanceláři.

6.9 Školení zaměstnanců

Školení zaměstnanců by se mělo provádět pravidelně v určitých intervalech. Měli by se školit nový zaměstnanci a poté by školení mělo probíhat minimálně jednou ročně.

Základní body, které zaměstnanci po absolvování školení musí dodržovat:

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

6.10 Požadavky na správce sítě

Manažer informačního systému na malé obci zaujímá pozici, která vyžaduje kromě řídících schopnosti i odbornost v rámci technologií. Dále musí zajistit vybudování, implementaci a neustále zlepšovat informační bezpečnost.

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]

7 MĚSTSKÝ ÚŘAD VESELÍ NAD MORAVOU

Svou práci jsem konzultoval na Městském úřadu ve Veselí nad Moravou. Úřad má celkem 100 PC, která obnovují v intervalu pěti až šesti let. Jako operační systém na všech PC je nainstalován Windows 7 a na nejnovějších PC používají i Windows 10. Jako antivirový software byl instalován program od firmy ESET ve verzi ESET Smart Security a externí firewall Sophos. Zaměstnanci mají na jednotlivých PC Power user oprávnění a můžou provádět veškeré aktualizace. Nemají téměř žádná omezení a flash disky nejsou hlídány. Avšak zaměstnanci žádné aktualizace neprovádí a nechávají vše na správci sítě, aby jim jednotlivé aktualizace provedl. Svá data pravidelně každý den zálohují na virtuální servery. Servery jsou umístěny v nejvyšším patře budovy. Jsou vybaveny požárními čidly, přístup je pomocí hesla, kdy před dveřmi je klávesnice a správce sítě zadá heslo pro přístup do místnosti. Dále je místnost izolována také proti vodě. Z hlediska bezpečnosti je celá budova napojena na Městskou policii Veselí nad Moravou, takže při neoprávněném vstupu do budovy policie ihned přijede a místo zabezpečí.

ZÁVĚR

Bez informačních technologií se žádná organizace a úřad neobejdou. Proto je nezbytnou nutností správné zajištění ochrany dat a fungování informačního systému po celou dobu jeho životního cyklu. Je důležité, aby uživatelé informačního systému věděli, jaké nebezpečí hrozí, a co se může stát, pokud nebudou dodržovat stanovené postupy.

Svou bakalářskou práci jsem zpracoval na téma: Stanovení požadavků na bezpečnost desktopových 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. Tyhle hrozby minimalizujeme pomocí ochrany dat, která byla rozdělena do tří kategorií. Jednotlivými kategoriemi byla: fyzická bezpečnost, datová bezpečnost a personální bezpečnost. V praktické části jsem se zabýval návrhem postupů řízení bezpečnosti informačních systémů na malé obci. Dále výběrem vhodného antivirového zabezpečení z pohledu ochrany dat na PC i mobilních zařízení. 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 organizace ztratit veškerá svá data. Nutností je také provádět pravidelná školení spojená s tématem informační bezpečnosti.

Za cíl v mé bakalářské práci považuji poskytnutí praktických informací, vybrání vhodného antivirového programu a podniknutí opatření, která zajišťují bezpečnost informačního systému v organizaci. I ten nejlepší informační systém nebo správce počítače nemůže zajistit ochranu dat, pokud v organizaci nedodržují základní pravidla týkající se bezpečnosti.

Na Městském úřadě ve Veselí nad Moravou, kde jsem svou práci konzultoval, byla fyzická bezpečnost správně řešena. Servery byly umístěny v nejvyšších patrech budovy a místnost byla opatřena veškerými bezpečnostními opatřeními, školení zaměstnanců bylo mnou doporučeno tak, aby probíhalo v pravidelných ročních cyklech. Co se týče jednotlivých PC tak zaměstnanci mají přístup ke všemu a můžou provádět cokoliv, nemají žádná omezení. Takováto volnost zaměstnanců zajisté 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 všechny pravidla a postupy pro snížení hrozeb.

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

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
DES	Data Encryption Standard
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HW	HardWare
IDEA	International Data Encryption Algorithm
IP	Internet Protocol
IS	Information Systém
ISMS	Information Security Management Systém
OS	Operating System
OSI	Open Systems Interconnection
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
VPN	Virtual Private Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK