VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O. P. S., ČESKÉ BUDĚJOVICE

Bakalářská práce

Bezpečnost informací v informačních technologiích

Autor práce: Petr Molnár
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Prezenční
Vedoucí studia: doc. JUDr. PhDr Jiří Bílý, CSc.
Katedra: Katedra právních oborů a bezpečnostních studií

2014

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

……

Děkuji vedoucímu bakalářské práce doc. JUDr. PhDr Jiřímu Bílému, CSc., Za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

MOLNÁR, P. *Bezpečnost informací v informačních technologiích : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2014. 59 s. Vedoucí bakalářské práce : doc. JUDr. PhDr Jiří Bílý, CSc.

Klíčová slova: bezpečnost informací, zabezpečení, informační systém, bezpečnostní normy

Tato práce v teoretické části zkoumá způsoby zabezpečení a ochrany dat uložené v počítačích, jak proti útočníkovi, tak i proti živelné pohromě (požár, výpadek elektrické energie). Jednotlivé zabezpečení jsou uváděny na úrovní bezpečnosti běžných uživatelů informačních technologiích, tak i v organizacích. Dále práce analyzuje normy, které se používají při vytváření bezpečnostních systémů. Normy vytvářejí požadavky, podle kterých má daný systém být vytvořen. Také práce se věnuje právním předpisům ČR, jako je zákon č. 101/2000 Sb. O ochraně osobních údajů. V praktické části je použita dotazníková metoda pro sběr dat. Výstupem tohoto dotazníku jsou vydána doporučení k zajištění bezpečnosti dat a informací.

ABSTRACT

MOLNÁR, P. *Information security in iformation technology : bachelor thesis.* České Budějovice : The College of European and Regional Studies, 2014. 59 p. Supervisor : doc. JUDr. PhDr Jiří Bílý, CSc.

Keywords: information security, security, information systems, security standards

This work examines the theoretical methods of security and protection of data stored on computers as against an attacker, as well as against natural disaster (fire, power failure). Individual contributions are placed on the level of security of ordinary users of information technology, as well as in organizations. The thesis also analyzes the standards that are used when creating security systems. Standards form the requirements, according to which the system is to be created. Also, work is devoted to the legislation of the Czech Republic, as Law No. 101/2000 Coll. About Privacy Policy. In the practical part of the questionnaire method used to collect data. The outcome of this questionnaire is issued recommendations to ensure the security of data and information.

Obsah

1. Úvod

V dnešní době, kdy rozvoj informačních technologií strmě stoupá a vyvíjí se nové technologie a prostředky pro komunikaci, které se uplatňují téměř v každé lidské činnosti a s tím vznikl nový virtuální prostor, také označován jako kyberprostor, ve kterém se realizují různé operace např.: řízení státu, samosprávy, zdravotnictví nebo i prostá komunikace mezi lidmi, což může mít za následek vyšší ohrožení společnosti jak úmyslným, např. útok hackera nebo neúmyslným zneužitím těchto technologií. Nepřítelem nemusí být soused, ale může to být osoba, která je na druhé straně zeměkoule. Může se jednat o skupinu nebo dokonce jednotlivce, který provádí daný útok. Informatika je základním nástrojem organizované společnosti ale může být také nástrojem jak tuto společnost snadno destabilizovat.

Pro zajištění správné funkčnosti informačních technologií a eliminaci rizik působící na tyto systémy se musí vytvářet adekvátní ochranné prostředky nebo protiopatření a dále tyto opatření neustále zdokonalovat, jelikož se objevují nové hrozby, které se mění a proto se i daná ochrana musí těmto hrozbám přizpůsobit. Takovou ochranu nazýváme informační bezpečnost, která je členěna na tří základní podskupiny a každá s těchto atribut ovlivňuje ochranu informací jinak.

Úvodem jsou v práci vymezeny základní pojmy a atributy, jako jsou: dostupnost, integrita, důvěrnost, jež spadají jako celek do informační bezpečnosti. Práce bude zaměřena na prostředí běžných uživatelů informačních technologii, budou též uvedeny příklady zabezpečení informací v organizacích.

Dále bude pozornost věnována zabezpečovacím normám, případně budou uvedeny zákonné předpisy, které se týkají daného problému. Normy budou posuzovány podle efektivity, pro jakou oblast jsou nejvýhodnější (zda je vhodné aplikovat tyto normy i v „domácím prostředí“). Kdo a jak může vydávat tyto normy, popis základní normy využívající se pro vytváření určité úrovně bezpečnostní pro počítačové systémy. V této části se také prozkoumá analýza rizik.

Další část práce je věnována samotnému zabezpečení počítačového systému. Tato kapitola je rozdělena do dvou podskupin: fyzická a softwarová bezpečnost. V jednotlivých kapitolách jsou uvedeny případné hrozby a způsoby jak ochránit data a informace v počítačích. Zde jsou uvedeny některé způsoby ochrany dat v organizacích tak i v pro běžné uživatele.

2. Cíle a metodika

Hlavním cílem této práce je zjistit možnosti, jak zabezpečit a ochránit informace uložené v počítačích, jak proti případnému útočníkovi, tak i proti živelním pohromám. Možnosti, jak zabezpečit informace se můžou provádět na fyzické, tak i softwarové úrovni. Fyzické zabezpečení má zamezit přístup nepovolaným osobám k datovému úložišti nebo zajištění bezpečnosti pomocí technických zařízení např. čtečky biometrických údajů, magnetické karty a jiné. Softwarová bezpečnost se zajišťuje pomocí aplikací v daném systému, jako jsou antivirové programy, firewall a další. Tyto možnosti mají působit proti hrozbám, které mohou nastat jak úmyslně např. hacker nebo i v organizaci při ztrátě zaměstnanecké loajality, či neúmyslně, jako je nedbalost zaměstnanců nebo i výpadek elektrického proudu, přepětí atd.

Dílčím cílem je zjistit efektivitu norem na vytváření bezpečnostních opatření chránící informace. Normy jsou obecná kritéria, podle kterých se hodnotí daný systém, který musí mít jasně daná specifika, což představuje finanční zátěž, a proto je nutné zvážit, zda aplikování norem na daný systém nebude dražší než při případné ztrátě dat. Proto je prováděna analýza rizik, při které se zváží veškerá fakta (cena zabezpečení proti ceně chráněných dat) a výsledkem je přijmutí daných opatření. Normy mohou vytvářet jen autorizovaní výrobci (společnosti, organizace) a jsou neustále upravována.

Práce je rozdělena do dvou hlavních částí na teoretickou a praktickou část. V první části, se s pomocí analýzy odborné literatury uvedou možnosti zabezpečení a ochrany informací uložené v počítači. Bezpečnost je nutné rozlišovat na „domácí prostředí“ tj. běžní uživatele informačních technologií a dále na organizační prostředí (firmy, organizace). Úroveň zabezpečení se v těchto dvou rovinách liší a to z několika důvodů: finanční (každé zabezpečení je určitá peněžní zátěž), technické (použití speciálních technologií) a personální (organizace mají najaté odborníky) prostředky.

Ke zjištění, jaká rizika mohou působit na daný systém, je třeba uskutečnit detailní analýzu rizik. Výsledkem takové analýzy jsou negativní elementy, které mohu působit na informace a proti kterým se vytváří bezpečnostní opatření. V prostředí běžných uživatelů se může jednat např. pravidelná aktualizace systému, antivirový program, firewall či zálohování dat. V organizačním prostředí může být zavedeno např. selekce zaměstnanců (určení přístupu k informacím), protipožární ochrana, omezený přistup k serveru nebo stavba Faradayovy klec (proti elektromagnetickému rušení).

V teoretické části jsou dále uvedeny normy, které se mohou podílet na vytváření bezpečnostních systémů. Jedny z prvních norem byly vytvořeny v USA, některé z nich jsou převzaty do ČR. V současné době je platná celá škála norem, jako CC (common criteria) jsou obecná kritéria pro hodnocení bezpečnostních systému. V této práci je podrobněji popsána norma ISO/IEC 27001:2005 – jakožto mezinárodní standart definující požadavky na systém managementu bezpečnosti informací.

Tohoto problému se týkají také zákonné předpisy, jako: zákon č. 101/2000 Sb. – zákon o ochraně osobních údajů; zákon č. 106/1999 Sb. – zákon o svobodném přístupu k informacím, zákon č. 365/2000 Sb. – zákon o informačních systémech veřejné správy.

V druhé části práce – praktická část, se budou sbírat data formou dotazníku. Dotazník se bude skládat pouze z uzavřených otázek, týkající se vše okolo bezpečného používání počítače, což bude vést ke zjištění postoje osob, které často využívají výpočetní techniku. Získaná data budou zpracována do podoby grafů, ze kterých se vytvoří doporučení jak správně používat počítač a chránit v něm uložené informace.

Stanovení hypotézy

Hypotéza 1: Počet respondentů využívající jakýkoliv bezpečnostní program je vyšší než 70%.

Hypotéza 2: Více jak 70% respondentů nesdílí svůj počítač s jinými uživateli.

Hypotéza 3: Své heslo nemění více jak 50% respondentů.

3. Informační bezpečnost

Bezpečnost je brána, jako ochrana čehokoliv před nepříznivými jevy (ztráta, poškození, zničení) působící na daný předmět. Informační bezpečnost lze chápat, jako praktickou disciplínu informatiky zajišťující ochranu důvěrnosti, integrity a dostupnosti dat a informací po celý životní cyklus, což znamená od vzniku dané informace, zpracování, ukládání, přenos až po její likvidaci. Tato disciplína se rychle rozvíjí, jelikož se vytvářejí nové programy, jak pro podporu ochrany dat a informací, ale i programy vytvořené útočníky (hackeři, teroristé). Nejedná se jenom o ochranu před úmyslným poškozením dat způsobenou lidskou činností, ale řadí se sem i živelné pohromy (požár, výpadek proudu).[1]

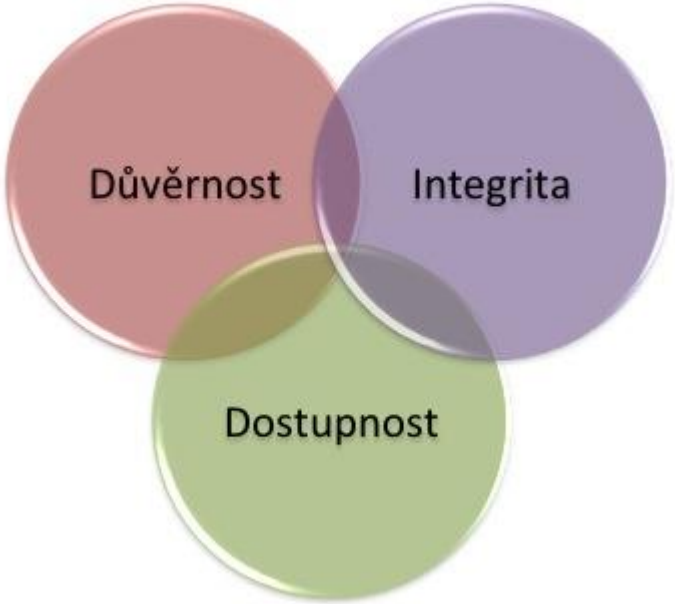
V této oblasti informační bezpečnosti již vnikla řada firem zabývající se různými aspekty zabezpečení aktiv (určitá informace, která se chrání), jak na softwarové úrovni (vývoj antivirových programů) tak i technické zabezpečení počítačových systémů. Pojem počítačový systém, si lze představit, jako soubor částí ovlivňující data a informace. Do tohoto „balíku“ patří určité datové médium (pevný disk, optický disk, flash disk), na kterém jsou uloženy data. K jejich přečtení či práci s nimi je zapotřebí užít hardwaru (osobní počítač, server). Funkčnost hardwaru zajišťuje mimo jiné jeho softwarové zařízení (operační systém, jiné programové aplikace). Data mohou být uložena na serveru, za účelem sdílení pro více uživatelů, tak je důležité zajistit síťové připojení (LAN, WAN) k tomuto úložišti. Veškeré zařízení je vždy umístěno v určité budově, ve které je tento systém spravován a užíván.[2]

Informační bezpečnost si klade za cíl ochranu informací po její celý životní cyklus. K vytvoření patřičné ochrany, se strategie celého systému opírá o tři základní pilíře: Důvěrnost, dostupnost a integrita dat. Tyto tři základní atributy, jsou na sobě závislé a měly by být v rovnováze, co se týče jejich aplikace pro vytváření bezpečnosti informací. Každý jednotlivý pilíř je zaměřen na jinou oblast. Důvěrnost je ochrana dat před neoprávněným přístupem osob, kterým nejsou určeny. Dostupnost si klade za cíl zachování přístupových komunikačních cest mezi uživatelem a datovým úložištěm

[1] HOWLETT, T. *Open source security tools.* New Jersey : Pearson Education, 2005. S. 26.
[2] *Clever and Smart* [Online]. 2008-2014 [cit. 2014-1-2]. Dostupný z WWW: <http://www.cleverandsmart.cz/informacni-bezpecnost/>.

uschovávající data a informace. Integrita se zabývá ochranou dat z hlediska její správnosti i nepoškozenosti.[3]

Obrázek 1 – znázorňuje propojenost všech tří zabezpečovacích atribut[4]



3.1. Důvěrnost

Nejčastěji se dá definovat, jako zajištění přístupnosti informace pouze těm, kteří jsou k tomu oprávněni, a jejím cílem je ochrana těchto informací před neoprávněním čtením. Nežádoucí zpřístupnění (anglicky disclosure) se v informační bezpečnosti označuje, jako narušení důvěrnosti. K zajištění tohoto atributu, je potřeba vytvořit klasifikační schéma určující, kdo má přístup k jakému druhu informací. Toto schéma je především vytvářeno ve velkých společností operující s velkým množstvím informací nacházející se jak ve státním, tak i v soukromém sektoru. Schémata se mohou lišit podle bezpečnostní politiky daných subjektu, ale jsou vytvořena nejběžnější schémata.[5]

Klasifikace pro státní sektor:[6]

Přísně tajné (top secret) – nejvyšší stupeň, zde už může mít nežádoucí zpřístupnění zničující dopad.

[3] *Ikaros* [Online]. 1997-2013 [cit. 2014-1-2]. Dostupný z WWW: <http://www.ikaros.cz/bezpecnost-dat-v-informacnich-systemech>.
[4] *Informace a bezpečnost* [Online]. 2011 [cit. 2014-1-4]. Dostupný z WWW: <http://www.vlastnicesta.cz/clanky/informace-a-bezpecnost/>.
[5] *Ikaros* [Online]. 1997-2013 [cit. 2014-1-2]. Dostupný z WWW: <http://www.ikaros.cz/bezpecnost-dat-v-informacnich-systemech>.
[6] *Clever and Smart* [Online]. 2008-2014 [cit. 2014-1-2]. Dostupný z WWW: <http://www.cleverandsmart.cz/informacni-bezpecnost/>.

Tajné (secret) – nežádoucí zpřístupnění může mít značný dopad.

Důvěrné (confidental) – nežádoucí zpřístupnění může mít významný dopad na národní bezpečnost.

Citlivé, ale neklasifikované (sensitive but unclassfied) – nežádoucí zpřístupnění by nemělo mít významný dopad na národní bezpečnost.

Neklasifikované (unclassfied) – nejnižší stupeň, nežádoucí zpřístupnění by nemělo mít žádný dopad na národní bezpečnost.

Vytvořený schémat, by neměl mít málo klasifikačních stupňů, jelikož by to mohlo vést k podcenění hodnoty informací a vytvoření velkého množství stupňů vede k chaotickému zařazování informací (vybrat správnou kvalifikaci je obtížné).

Pro soukromé subjekty je nejčastěji používán:[7]

Důvěrné (confidential) – nejvyšší stupeň, nežádoucí zpřístupnění se zdrcujícím dopadem (vývojové plány, strategie subjektu).

Soukromé (private) – nežádoucí zpřístupnění má negativní dopad (osobní údaje zahrnující jak zaměstnance, tak i zákazníky organizace).

Citlivé (sensitive) – nežádoucí zpřístupnění má již negativní dopad (jedná se o finanční politiku organizace, informace o produktu).

Veřejné (public) – nejnižší stupeň, ve kterém by nežádoucí zpřístupnění nemělo mít dopad na organizaci.

K zajištění důvěrnosti, je nutné vytvořit určitá bezpečnostní opatření v několika úrovních (logická, fyzická a organizační úroveň). Každá z těchto úrovní ovlivňuje bezpečnost jinak a přijímá jiná opatření proti hrozbám působící na důvěrnost. Může se jednat např. o fyzické zabezpečení datového úložiště (uzamčení pevného disku do

[7] *Clever and Smart* [Online]. 2008-2014 [cit. 2014-1-2]. Dostupný z WWW: <http://www.cleverandsmart.cz/informacni-bezpecnost/>.

trezoru, uzamčená místnost se serverem), ke kterému mají přístup jen oprávněné osoby. Nejedná se jenom hardware počítače, ale i dokumenty v listinné podobě. Dále se může jednat o šifrování informací vzhledem k jejich hodnotě. Hodnota informace se může za určitý čas změnit a snížit tím nutnost ochrany před nežádoucím zpřístupněním, může se jednat např. o provedení plánované akce, kdy po jejím dokončení není třeba dále chránit informace.[8]

3.2. Dostupnost

Je charakterizována, jako zajištění přístupu k informaci v tu dobu, kdy je s ní potřeba pracovat. Cílem této atributy je udržení dostupnosti pro osoby mají oprávnění s nimi nakládat, jelikož dobře chráněné informace jsou k ničemu, když nebudou přístupné v době nutnosti. S přibývajícími útoky na servery způsobující vyřazení komunikačních cest, se začaly cíle v informační bezpečnosti soustřeďovat nejen na ochranu informací před nežádoucími přístupy, ale také zajišťovat přístup uživatelům, kteří jsou oprávněni s nimi pracovat.[9]

Narušení dostupnosti, se může objevit v několika směrech. Jedním z nich je selhání hardwaru, což má za následek narušení přístupu či dokonce zničení informací. Do tohoto nežádoucího jevu, se zařazuje veškerá technika, která je v jakémkoliv kontaktu s informacemi. Může se jednat o poškození pevného disku či jiného datového úložiště nebo přerušení samotného datového kabelu znemožňující navázat spojení. Dále se sem počítá i odpojení či jen výpadek elektrického napájení, což může vést ke ztrátě dat a informací, se kterými se pracovalo a nebyly uloženy či jinak zálohovány před začátkem tohoto nepříznivého jevu.[10]

K ochraně a zajištění dostupnosti, se využívají různá opatření, kterými může být např. vytváření duplikátů, ať se jedná o pevný disk či napájení (vytvoření náhradního zdroje), tak se může vytvořit záložní systém celého počítače a dokonce celé sítě. Avšak vytváření těchto duplikátu nese několik nevýhod a nutné je všechny zvážit. Jednou nevýhodou je, že při vytváření opatření je určitá finanční zátěž rostoucí s počet vytvořených záložních prostředků. Dále s tím roste náročnost na údržbu a správu takto

[8] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 60-61.
[9] HOWLETT, T. *Open source security tools.* New Jersey : Pearson Education, 2005. s. 27.
[10] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 61.

vytvořených systémů a také vzroste počet míst, ve kterých se může objevit závada (může se jednat o kterýkoliv prvek a kabelové spojení mezi nimi).[11]

Mezi jednotlivými prvky musí být zajištěna synchronizace, protože pokud jeden z nich selže, tak druhý záložní komponent musí převzít úlohu a plně pracovat se stejnými daty jako na původním prvku. Zajistit synchronizaci se dá pomocí aplikace či síťovou vrstvou, ale stále se jedná o těžký úkol. Pokud by se tyto stavy neošetřily, mohlo by nastat rozdělení činnosti jak hlavního prvku, tak i sekundárního, což by vedlo k tomu, že každá část by pracovala zvlášť a pak by obsahovala jiné informace. Dostupnost by byla zajištěna na úkor integrity informací.[12]

3.3. Integrita

Nejčastěji se dá definovat, jako atribut zajišťující správnost a úplnost informace. Cílem je tedy zajistit celistvost informace proti nežádoucí změně, která může být provedena úmyslně, nedopatřením nebo selháním hardwaru. Pokud dojde k tomuto jevu, může se stát, že změna nebude ihned detekována a než bude odhalena, tak může uplynout určitý čas. V takovém případě se již těžko dohledávají ztracená původní data, jelikož nelze dohledat, kdy byla informace změněna. Pokud byla nežádoucí změna provedena dlouho před samotným zjištěním, tak ani opatření ve způsobu archivace či zálohování příliš nepomohou, jelikož se zde bude pravděpodobně nacházet modifikace dané informace.[13]

Základním opatřením proti nežádoucí změně je zavedení záznamů veškerých prováděných modifikací v systému, aby bylo možné zjistit, kdy a kde byla změna provedena a pak se dá opravit na původní hodnotu. Jedná se nejjednodušší opatření, ke kterému by se dále měla provádět pravidelná archivace, pro dosažení co nejrychlejší a nejpřesnější obnovy změněné informace na původní hodnotu. Dále se může jednat o použití aplikace pro šifrování, která by kódovala informace před samotným uložením na datová média. Takto zašifrovaný text je dále chráněn kontrolním součet, který zjistí, zda nebyla provedena změna.[14]

---

[11] *Clever and Smart* [Online]. 2008-2014 [cit. 2014-1-2]. Dostupný z WWW: <http://www.cleverandsmart.cz/informacni-bezpecnost/>.
[12] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 63.
[13] *Clever and Smart* [Online]. 2008-2014 [cit. 2014-1-2]. Dostupný z WWW: <http://www.cleverandsmart.cz/informacni-bezpecnost/>.
[14] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 60.

4. Osvětlení vybraných pojmů

V této části jsou uvedeny určité pojmy týkající se tohoto tématu, které jsou stručně a výstižně popsány ke snadnému pochopení jejich významu.

Data – je název pro údaj, který je získám pozorováním nebo měřením určitého jevu či objektu v daném okamžiku. Jedná se především o číselné údaje pro lepší zpracování a je základním kamenem pro informaci.[15]

Informace – je široký pojem využívaný pro různé významy. Obecně lze chápat jako údaj, který je tvořen souhrnem dat a určitým způsobem je prezentuje navenek.[16]

Autentizace – je určitý proces ověření identity osoby a jejího oprávnění k přístupu.[17]

Autorizace – je ověření, zda má subjekt příslušná práva k provádění daných operací (pracovat s daty, provádět změny v systému).[18]

Firewall – jedná se software monitorující síťovou komunikaci mezi počítačem a internetem. Dá se charakterizovat, jako ochrana hranic sítě a může zablokovat případnou snahu o nežádoucí průnik z vnější sítě.[19]

Honeypot – je uměle vytvořený systém či celá síť, která je vytvořena za účelem nalákání a sledování hackerů. Může také sloužit i jako obranná síť, jelikož může odvést pozornost.[20]

Sandbox – je vyhrazená část v systému sloužící určitému programu, zatím co zbylá část systému nemá k programu přístup. Jedná se bezpečnostní mechanizmus k otestování nedůvěryhodných programů.[21]

---

[15] *Wordpress* [Online]. 2010 [cit. 2014-2-14]. Dostupný z WWW:<http://stipek.wordpress.com/slovnik/>.
[16] *Wordpress* [Online]. 2010 [cit. 2014-2-14]. Dostupný z WWW:<http://stipek.wordpress.com/slovnik/>.
[17] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, 2004. s. 65.
[18] *Wordpress* [Online]. 2010 [cit. 2014-2-14]. Dostupný z WWW:<http://stipek.wordpress.com/slovnik/>.
[19] *Viry.cz* [Online]. 2014 [cit. 2014-2-14]. Dostupný z WWW:<http://www.viry.cz/firewall-vs-bezny-uzivatel/>.
[20] *Wordpress* [Online]. 2010 [cit. 2014-2-14]. Dostupný z WWW:<http://stipek.wordpress.com/slovnik/>.
[21] *Wordpress* [Online]. 2010 [cit. 2014-2-14]. Dostupný z WWW:<http://stipek.wordpress.com/slovnik/>.

Hacker – je označován subjekt využívající své znalosti v oblasti výpočetní techniky k vyhledávání a objevování bezpečnostních nedostatků. Může se jednat o osobu orientující se v detailech programových kódů a jejich zlepšování. Osoba programující s posedlostí se dá také označit za hackera.[22]

Malware – je obecný výraz pro veškeré škodlivé programy a kódy, jež mají za úkol způsobit újmu či získat určitá data.[23]

Spyware – jedná se program, který je umístěn v počítači bez vědomí uživatele. Nikterak nepoškozuje počítač či uložená data, ale shromažďuje a monitoruje data, která pak odesílá tvůrci škodlivého programu.[24]

Botnet – je skupina počítačů ovládaná bez vědomí jejich uživatelů. Takto podmaněné stroje jsou využívány k šíření nevyžádané pošty.[25]

Adware – je program nutící uživateli různé reklamy během prohlížení internetu. Nemusí se jednat o škodlivý software, jelikož může být doprovázen tzv. EULA licenční ujednání, s kterými musí uživatel souhlasit v případě užívání určitých programů.[26]

Keylogger – je škodlivý program snímající vše co uživatel napíše na klávesnici. Takto získává jména a hesla k účtům.[27]

Trojan – je označován jako trojský kůň. Program je uzpůsoben tak, že na venek se chová jako legitimní software, ale hlavním cílem je určitým způsobem škodit, či stahovat jiný nežádoucí software do počítače.[28]

---

[22] *Počítačová bezpečnost a ochrana dat* [Online]. [cit. 2014-2-14]. Dostupný z WWW: <http://marlib.cmsps.cz/bezpecnost/bezpecnost.html/>.

[23] *PC security* [Online]. [cit. 2014-2-14]. Dostupný z WWW: <http://pc-security.cz/slovnik-pojmu/malware//>.

[24] *Počítačová bezpečnost a ochrana dat* [Online]. [cit. 2014-2-14]. Dostupný z WWW: <http://marlib.cmsps.cz/bezpecnost/bezpecnost.html/>.

[25] *Root.cz* [Online]. 1998 - 2004 [cit. 2014-2-14]. Dostupný z WWW: <http://www.root.cz/slovnicek/>.

[26] HOMÉR. *Zálohování a ochrana dat* [Online]. 2009[cit. 2014-2-20]. Dostupný z WWW: <http://uloz.to/xm9XdZo/zalohovani-a-ochrana-dat-doc/>.

[27] *Wordpress* [Online]. 2010 [cit. 2014-2-14]. Dostupný z WWW: <http://stipek.wordpress.com/slovnik/>.

[28] KURTZ, G., MCLURE, S., SCAMBRAY, J. *Hacking bez tajemství.* Praha : Computer Press, 2002. s. 508.

Virus (worm) – jedná se o program šířící se samovolně pomocí e-mailu či přenosných datových mediích.[29]

Hoax – je označována zpráva, která je nepravdivá a může vyvolat paniku. [30]

Phising – je označováno jako podvodné jednání útočníka, který se snaží přimět svoji oběť k tomu, aby navštívila stránky, které jsou napodobeniny originálních internetových stránek a zde v nich zadala své přihlašovací údaje.[31]

Backdoor – dá se také označit jako „zadní vrátka“ a jedná se o úmyslně vytvořenou funkci v programu umožňující vstup nepovolaným osobám do systému a případně umožní ovládnutí systému. Jejich kompletní odstranění je velmi náročné.[32]

DoS (Denial of Service) – označováno jako odmítnutí služby a jedná se o útok proti internetovým službám, při kterém dochází k přehlcení požadavků, které vedou k nedostupnosti pro ostatní uživatele.[33]

[29] *Wordpress* [Online]. 2010 [cit. 2014-2-14]. Dostupný z WWW:<http://stipek.wordpress.com/slovnik/>.
[30] *Hoax.cz* [Online]. 2000 - 2014 [cit. 2014-2-14]. Dostupný z WWW: <http://www.hoax.cz/cze/>.
[31] *Počítačová bezpečnost a ochrana dat* [Online]. [cit. 2014-2-14]. Dostupný z WWW: <http://marlib.cmsps.cz/bezpecnost/bezpecnost.html/>.
[32] KURTZ, G., MCLURE, S., SCAMBRAY, J. *Hacking bez tajemství.* Praha : Computer Press, 2002. s. 489.
[33] *Lupa.cz* [Online]. 1998 - 2014 [cit. 2014-2-14]. Dostupný z WWW: <http://www.lupa.cz/clanky/denial-of-service-dos-utoky-zaplavove-typy/>.

5. Způsoby zabezpečení a ochrany dat a informací

V této oblasti jsou uvedeny jednotlivé způsoby ochrany dat a informací uložené v počítačích a jsou popsány základní principy fungování těchto opatření proti nežádoucím jevům. Celá část je rozdělena do dvou sekcí. První je orientována na fyzickou (hardwarovou) ochranu a druhá se zaměřuje na softwarovou (aplikační) vrstvu.

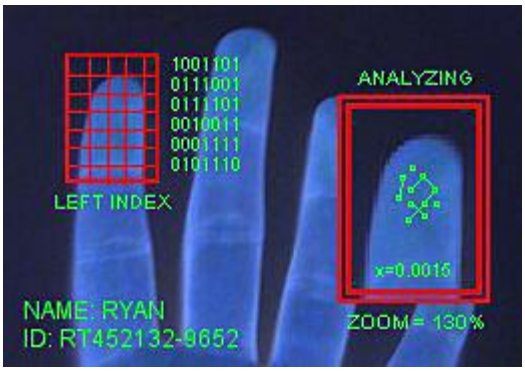
5.1. Technické zabezpečení dat a informací

Tato část se zaměřuje na způsoby ochrany dat a informací na technické úrovni, respektive ochranná opatření opírající se o fyzickou existenci příslušných zařízení, ať se jedná o přídavné čtečky či úprava stavebního stavu budovy.

Biometrická autentizace

Jedno ze základních technických opatření, se vztahuje k biometrické identifikaci, což znamená využití unikátních, nemněných vlastností těla, jako přístupového klíče k datům a informacím. Především se jedná o otisky prstů, které jsou jedinečné a neopakovatelné. Základem pro prácí s takovýmto typem zabezpečení je čtečka, která disponuje vysokým rozlišením, jelikož je nutné dokonale rozpoznat, o jakého uživatele se jedná. Čtečka vytvoří obraz papilárních linií prstu a určí zásadní body důležité pro identifikaci a pak jim určí identifikační číslo. Poté se tato informace, jako celek uloží do databáze, na kterou je čtečka připojena. Dochází-li k autentizaci, čtečka porovnává obraz vyskytující se na snímací jednotce a vnitřní databáze, shodnou-li se, je příslušné osobě povolen přístup k datům a informacím. [34]

Obrázek 2 - zobrazuje analýzu základních bodů na prstu[35]



[34] *Biometrický identifikační systém* [Online]. 2006 - 2008 [cit. 2014-1-4]. Dostupný z WWW: <http://www.vlastnicesta.cz/clanky/informace-a-bezpecnost/>.
[35] *Biometrický identifikační systém* [Online]. 2006 - 2008 [cit. 2014-1-4]. Dostupný z WWW: <http://www.vlastnicesta.cz/clanky/informace-a-bezpecnost/>.

Tento systém se dá využít v mnoha směrech, ať se jedná o kontrolu přístupu do budov či místností, sledování docházky či ochrany dat a informací uložené v počítačích. Biometrické čtečky mohou být součástí velkého systému pro mnoho osob či rozsáhlost a počet snímacích zařízení, ale celá síť je náročná na údržbu, což se projevuje i ve finanční zátěži. Takovéto bezpečnostní opatření se nejčastěji vyskytují ve velkých organizacích. Zato malá jednoduchá zařízení je možno připojit k počítači přes USB a pomocí softwaru se dají snadno ovládat. Podobnými snímacími jednotkami jsou již vybaveny některé typy notebooků zvyšující bezpečnost uložených dat.[36]

Biometrická autentizace se netýká jen papilárních linií. Stejně efektivně se dá využít i oční duhovky. K realizaci takovéhoto opatření se používá zařízení podobné kameře, které pořídí několik snímků za vteřinu a vytvoří tak soubor snímků oka. Takto vytvořené snímky se digitalizují a jsou poslány do procesoru, který je vyhodnotí. Systém se zaměřuje na určité charakterizující znaky oka a porovnává je s vnitřní databází. Takto vytvořené vzorky jsou unikátnější než otisky prstů či DNA, dokonce ani jednovaječná dvojčata nemají stejnou duhovku. K identifikaci se dá rovněž použít i tvar obličeje, který je založen na základních bodech vyskytující se na tváři (vzdálenost očí, tvar nosu, tvar úst). Všechny tyto prvky jsou snímány kamerou a získaná data jsou porovnávána s databází.[37]

Do biometrické autentizace se také řadí ověřování hlasového vzorku, jež využívá unikátních vlastností lidského hlasu vedoucí ke snadné identifikaci. Nejprve se do vnitřní databáze nahraje určité heslo či jednoduchá fráze, která bude použita pro identifikaci uživatele. Pokud daný uživatel bude chtít získat přístup do systému, musí říci stanovené heslo nebo frázi, jež jsou uloženy v databázi. Zároveň musí být zohledněny další faktory, jako je: výška hlasu, rychlost a jeho intenzita. Tato technika není až tak přesná jako u ostatních identifikačních biometrických metod (otisky prstu, obraz duhovky), ale nejvíce je použita při ověřování přes telefonní linky. Někdy se tato metoda ověření hlasu zaměňuje s rozlišování hlasu. Každá s těchto metod se zaměřuje na jiné aspekty. Ověření hlasu určuje konkrétního uživatele, tedy rozeznává osoby, zatímco u rozlišování hlasu se neurčuje vlastník, ale rozeznávají se pouze řečená slova.[38]

---

[36] *Biometrický identifikační systém* [Online]. 2006 - 2008 [cit. 2014-1-4]. Dostupný z WWW: <http://www.vlastnicesta.cz/clanky/informace-a-bezpecnost/>.
[37] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 68.
[38] MINISTR, J. *Informační bezpečnost.* Karviná : SOŠ ochrany osob a majetku s.r.o., 2011. s. 81

Ochrana dat proti živelním pohromám

Jedná se veškeré škodlivé elementy, které mohou působit na počítačový systém a veškeré hrozby jsou přírodního charakteru. Jedním z prvních nebezpečí je napěťové přepětí způsobené úderem blesku. Veškeré součásti počítačového systému jsou stavěny na určité napájení a jsou velmi náchylné k jakémukoliv mírnému vzestupu napětí, při kterém jsou nenávratně poškozeny. K eliminaci tohoto škodlivého jevu se používá proti-přepěťová ochrana, také označována jako bleskojistka. K zajištění plné bezpečnosti je nutné vytvořit několik stupňů ochrany. První stupeň se nejčastěji nachází u hlavního rozvaděče, jako hlavní vstupní brány napětí pro počítačový systém. Druhý stupeň se má nacházet ve vedlejším rozvaděči či ve skříncе s jističi pro danou část objektu. Třetí stupeň by se měl vyskytovat přímo u dané zásuvky, ke které je počítač připojen. Všechny tyto prvky pak dohromady tvoří ochranu proti přepětí, a pokud nastane, tak se sice může dostat přes určitý stupeň, ale jsou vždy v záloze další. Na rozdíl od jednostupňové ochrany, která se nejčastěji vyskytuje až u koncové zásuvky, nemusí vydržet dané přepětí a propustí jej dále a tím dojde k poškození počítačového systému. [39]

Další nežádoucí situací spojenou s napětím je výpadek elektrické sítě ať již z důvodů přírodní katastrofy či jen při výskytu poruchy. Takovýto výpadek je nebezpečný zejména ve chvíli, kdy je pracováno s daty a nebylo provedeno uložení před výskytem této nežádoucí situace, tak veškerá práce je nenávratně ztracena. Nemusí to být zrovna úplný výpadek, ale stačí jen zakolísání energetické sítě, což může vést k vypnutí počítače. Nejjednodušším opatřením proti tomuto nežádoucímu jevu je časté ukládání provedených změn, aby se zabránila či zmírnila jejich ztráta. Také je možné využít náhradní napájecí zdroje, jež mají za úkol v případě výpadku elektrické sítě udržet v chodu ještě několik minut počítačový systém. Daný náhradní systém musí být ale dostatečně rychlý, protože nesmí dojít k vypnutí počítače mezi dobou výpadku elektrické sítě a zapnutí náhradního zdroje. Několik minut bohatě postačuje k uložení potřebných souborů a tím se zabrání k jejich ztrátě.[40]

K dalším nebezpečím přírodního charakteru, se dá zařadit elektromagnetické záření. Takovéto záření se může vyskytovat okolo každého vodiče, kterým prochází

[39] MOJMÍR, K. *Bezpečnost domácího počítače.* Praha : Grada, 2006. s. 35.
[40] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 55.

proud nebo i Slunce může vyslat vysoký elektromagnetický impuls poškozující veškerou elektroniku. K ochraně počítače se dá použít speciální uzavřené Faradayovy klece, které ochraňuje veškeré komponenty uložené uvnitř. Velikost klece se může podle účelů lišit, některé velké organizace zabývající se výpočetní technikou, jej staví po celé velikosti svého sídla a tím chrání veškeré vybavení vyskytující se uvnitř budovy. Jindy se jedná pouze o velikost daného datového úložiště. K ochraně proti elektromagnetickému záření se dá umístit počítač či datové úložiště dál od rozvodové kabelové sítě, jelikož mohou být zdrojem nežádoucího magnetického záření.[41]

Mezi živelné pohromy se také řadí požár, jenž může vniknout úmyslně či technickou závadou. Ať vznikne jakýmkoliv způsobem, jedná se o devastující škodlivý jev pro veškerou elektroniku. K zamezení či úplné eliminaci tohoto elementu je třeba přijmout nezbytná opatření, jako např.: zákaz kouření či zacházení s otevřeným ohněm v blízkosti výpočetní techniky, neumisťovat snadno hořlavé předměty poblíž větracích otvorů chladící vnitřní vybavení počítače či zavedení protipožární ochrany v podobě automatického hasícího systému. Často by mělo také docházet ke kontrolám přívodných kabelů k napájení, jelikož můžou být porušeny, což vede k vysokému riziku vzniku požáru.[42]

Také voda je jedním z největších hrozeb pro jakoukoliv nechráněnou elektroniku, jednak při kontaktu s vodou může dojít k poškození komponentu či jednotlivých součástek, které jsou ohroženy vznikem zkratu, jelikož voda funguje jako vodič a může způsobit nežádoucí kontakt mezi komponenty a tím je zničit. Dále se může jednat o nečistoty přicházející společně s vodou, které ulpí na součástkách nebo proniknou do vnitřních mechanismů různých komponentů. S nežádoucí nečistotou samozřejmě přichází i oxidace vodivých cest jednotlivých součástí, což může vést k jejich poškození. K eliminaci tohoto nežádoucího jevu se dají použít speciální úložné „boxi“, či již upravená úložná média, která jsou odolná vůči působení vody. Také je možné umístit počítač či úložné média mimo předpokládaný dosah působení vody např. nepít při práci s počítačem nebo nepokládat sklenici s vodou do blízkosti elektrických zařízení.[43]

[41] *Elektrodynamika* [Online]. 2010 [cit. 2014-1-16]. Dostupný z WWW: <http://kdf.mff.cuni.cz/vyuka/elektrodynamika/doku.php?id=experimenty:faradayova_klec>.
[42] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 54.
[43] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 54.

Omezení přístupu

Jedná se o bezpečnostní ochranu ve způsobu výběru uživatelů k jakým datům a informacím mají přístup. Jedná se o selektivní přístup na úrovni fyzické a softwarové bezpečnosti. Fyzická úroveň je vytvoření hmatatelné ochrany dat mající za úkol jejich ochranu před nežádoucím zpřístupněním. Můžou být vytvořeny zvláštní místnosti, ve kterých se nachází server či datová úložiště a do této části mají přístup pouze pověřené osoby, aby se předešlo nechtěné ztrátě dat a informací, zpravidla se jedná o správce sítě udržující chod celého systému, či úschovné trezory, do kterých se ukládají datové média, ke kterým má přístup jen ten uživatel pracující s danými daty. Softwarová úroveň spočívá ve vytvoření osobních účtů společně s jejich nastavení přístupu k určitým informacím. Všichni uživatelé mají přístup do společné sítě, ale mají odlišné přístupové pravomoci. Tedy každý uživatel má přístup do jiné úrovně zabezpečení a k jinému druhu informací.[44]

Tokeny, čipy, magnetické karty

K zlepšení zabezpečení dat a informací mohou být použity různé předměty, jako jsou: magnetické karty, čipy či tokeny, které jsou požity při autentizaci do systému příslušným uživatelem. Tyto předměty můžou být náhražkou za přihlašovací údaje, tedy není nutné zadávat heslo a stačí jen přiložit předmět k čtecímu zařízení k získání přístupu. Výhodou takovéhoto systému je, že si dotyčný uživatel nemusí pamatovat přihlašovací údaje, což může předejít situacím při jejich zapomenutí a zároveň se jedná o vcelku rychlý proces autentizace. Takovýto jednoduchý systém, může ale nést velké riziko při ztrátě takovéhoto bezpečnostního předmětu, jelikož se dá snadno zneužít nežádoucí osobou, při využití tohoto druhu identifikace. K zvýšení bezpečnosti při případném odcizení předmětu je zavedení kombinací zabezpečovacích úrovní, např. při čtení magnetické karty je nutné zadat přístupové heslo ověřující skutečného uživatele nebo využití dvou přihlašovacích zařízení provádějící autentizaci naráz. Tyto zařízení jsou v určité vzdálenosti od sebe a můžou být obsluhovány dvěma osobami, čímž se zvyšuje bezpečnost celého systému, protože pouze oprávněné osoby mají přístup do systému.[45]

[44] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 53.
[45] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 57-58.

5.2.Softwarové zabezpečení dat a informací

V této části se zabezpečení dat zaměřuje na aplikační vrstvu, tedy na konkrétní programy nebo jiné prostředky, které jsou umístěny v počítači mající za úkol snížit či úplně eliminovat nežádoucí hrozby působící na chráněná data a informace. Jedná se o specializovaný software určený pro konkrétní situace, pro které je určen.

Antivirové programy

Tento software se dá označit za základní zabezpečení po každý počítač vyhledávající škodlivé a nežádoucí programy jako jsou např.: trojské koně, viry. Na trhu jsou k mání různé verze těchto aplikací, může se jednat o freeware (program, který je volně dostupný a za jeho používání se nic neplatí), či různé trial verze (program je zdarma, ale po určité době je nutné si jej zakoupit) a neposlední řadě placené programy s plnohodnotnou podporou vývojářů. Veškeré tyto zabezpečovací programy poskytují více méně stejnou úroveň zabezpečení, i když placený software může plnit lepší funkci, jelikož je uživateli poskytována vyšší „péče“.[46]

Tento program funguje na vcelku jednoduchém principu. Porovnává svou vnitřní databázi s daným programem. Proto je nutné, aby databáze byla vždy aktuální, protože jsou neustále vyvíjeny novější a zákeřnější programy. K vyhledávání jsou používány testy počítače provádějící se na základě manuálního příkazu uživatele nebo automaticky v předem nastavenou dobu. Pokud se zkoumaný soubor shoduje, tak se jedná s největší pravděpodobností o malware a dle typu antiviru lze provést určité akce, jak je: odstranění škodlivého programu či přesunout do virového tresoru nebo opravit daný soubor. Především záleží na druhu antivirového programu, jelikož můžou mít různou dobu provádění testů či jejich důkladnost a spolehlivost (zda je nalezený program skutečně škodliví).[47]

Antispyware

Jedná se o software pracující na podobném principu jako antivirový program, akorát je zaměřen na vyhledávání spywaru, což je škodlivý maleware, který se vydává

[46] *Muj soubor* [Online]. 2012 [cit. 2014-2-14]. Dostupný z WWW: <http://mujsoubor.cz/magazin/nejlepsi-antivirove-programy>.
[47] *Muj soubor* [Online]. 2012 [cit. 2014-2-14]. Dostupný z WWW: <http://mujsoubor.cz/magazin/nejlepsi-antivirove-programy>.

za jiný program, který jsme si v dobrém mínění uložily do počítače a pak může otevřít „zadní vrátka do operačního systému dalším škodlivým programům či jen sbírá různá data o uživateli a odesílá je zpět tvůrci programu. Proto může být jeho odhalení náročné, jelikož je dobře skrytý. Antispyware má za úkol takovéto hrozby vyhledávat a odstraňovat či blokovat jejich komunikaci s vnějším prostředím.[48]

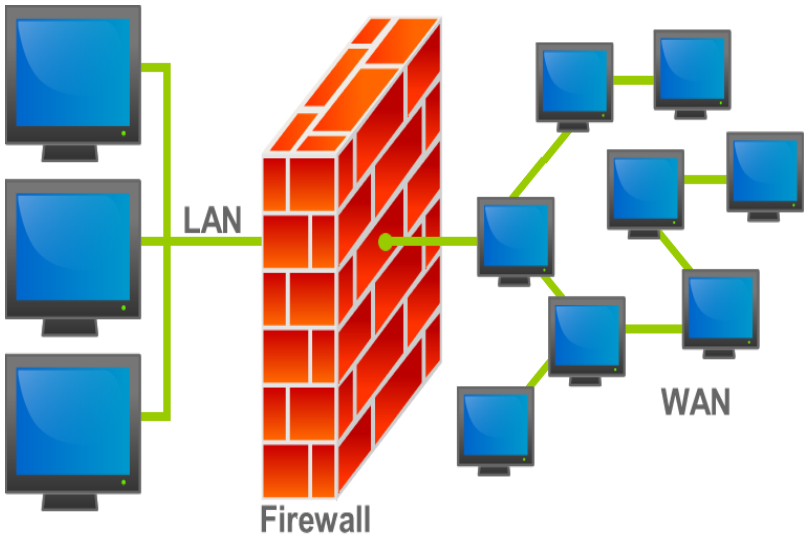
Firewall

Je software oddělující prostředí počítače či vnitřní sítě a vnějšího prostředí internetu. Jednak zajišťuje ochranu před nežádoucím průnikem do počítače z internetu (může se jednat o různé útoky osob snažící se získat kontrolu nad počítačem či jen získat přístup k uloženým datům). Také třídí příchozí pakety a propustí pouze ty, které jsou vyžadovány uživatelem. Dnešní verze firewallu obsahují mnoho nastavení, např. možnost zvolit jaký program může komunikovat s vnějším prostředím internetu, či kontrolovat jaká jsou aktivní spojení a možnost jejich přerušení.[49]

Firewally se dají rozdělit do dvou velkých skupin: aplikační proxy servery a paketové filtry. Aplikační proxy servery se dají považovat za bezpečnější, ale díky své limitovanému výkonu se nejvíce hodí pro kontrolu dat a informací vycházející směrem ven z místního prostředí než ke kontrole toku dat přecházejícího z vnějšího prostředí, výhodou tohoto druhu programu je jeho vysoká rychlost zpracování. Druhým typem je firewall s paketovým filtrem, ten se zejména používá tam, kde je potřeba vysoká kapacita přenášených dat oběma směry a také je kladen důraz na kvalitu spojení s internetem, nevýhodou je mít dostatečně výkonný hardware, jelikož je na něj kladena vysoká náročnost.[50]

[48] *Antivirove centrum* [Online]. 1998 - 2014 [cit. 2014-2-13]. Dostupný z WWW: <http://www.antivirovecentrum.cz/antispyware.aspx>.
[49] *Viry.cz* [Online]. 2014 [cit. 2014-2-14]. Dostupný z WWW: <http://www.viry.cz/firewall-vs-bezny-uzivatel/>.
[50] KURTZ, G., MCLURE, S., SCAMBRAY, J. *Hacking bez tajemství.* Praha : Computer Press, 2002. s. 422.

Obrázek 3 – grafické znázornění firewallu[51]



Aktualizace softwaru

Tento úkon by měl být prováděn co nejčastěji, protože žádný program není dokonale naprogramován a vyskytují se v něm jisté chyby, které jsou využívány útočníky ke svým činnostem, může se např. jednat o snahu převzít kontrolu nad počítačem, či „propašovat“ škodlivý program. Mezi nejdůležitější software bezpochyby patří operační systém provádějící službu prostředníka mezi hardwarem a ostatním programovým vybavení počítače. Tedy bez správné funkčnosti tohoto softwaru nelze plně využívat funkcí počítače. Proto je nutné udržovat operační systém aktuální k zajištění jak jeho funkčnosti, ale i bezpečnosti, jelikož se jedná také pouze o program mající i své chyby, které nemusí být identifikovány a mohou být hrozbou pro uživatelská data a informace uložená na těchto zařízeních. Jednotlivý výrobci vytvářejí bezpečnostní týmy mající za úkol nalezení těchto chyb a zároveň k jejich eliminaci za pomoci vydaných „záplat“ v aktualizacích. [52]

Zálohování

Jedná se o další ochranu dat a informací proti různým nežádoucím jevům, jako je např. ochrana proti ztrátě úložného média, selhání hardwarového zařízení, selhání softwaru nebo ochrana proti chybám vytvořených uživatelem. Zálohování je prováděno

[51] *ZCU* [Online]. [cit. 2014-3-5], Dostupný z WWW: <http://home.zcu.cz/~gabra6/>.
[52] *Viry.cz* [Online]. 2014 [cit. 2014-2-14]. Dostupný z WWW: <http://www.viry.cz/firewall-vs-bezny-uzivatel/>.

u všech dat mající svou cenu, ať vyjádřenou penězi či osobní hodnotou a vytvořené kopie jsou umístěny v bezpečném místě. Provádění takovéhoto úkonu by měl být prováděno pravidelně, či v momentech, kdy bylo s daty pracováno, pokud se ovšem bude záloha často měnit, tak je dobré zvolit „přírůstkovou metodu“ vytvářející několik souborů, které jsou v určitých intervalech aktualizovány. Takováto metoda může předejít nežádoucí změně, která se může vyskytnout v datech a jejímu rychlému odstranění (může se vyskytnout chyba, která již byla zálohována, ale jsou k dispozici další kopie, které jsou použity k obnově žádoucího stavu v datech).[53]

Důležitým faktorem při vytváření záloh je vybrat médium, na které se data budou ukládat. Druhů, na které lze ukládat kopie je mnoho a záleží na uživateli, jaký typ zvolí. Mezi nejčastěji používaná média se dají zařadit magnetové pásky používající se k zálohování serverů. Tyto pásky se dají označit za nejspolehlivější, jelikož se používají z dob zrození výpočetní techniky a jsou tudíž ověřeny. Dále jsou často používány duplikáty pevných disků označovány jako RAID 0,1,10,5. Jedná se tedy o propojený systém úložných médií taktéž využívány k záloze serverů, ačkoliv při havárii záložního disky, se mohou data poškodit či nenávratně ztratit. Pro domácí využití se nečastěji používají přenosná média typu FLASH, či rozšířená optická média (CD, DVD, Blue-ray), která jsou finančně dostupná, a v celku se s nimi snadno pracuje, i když se na takovouto zálohu nelze dlouhodobě spolehnout, jelikož se životnost CD, DVD udává okolo 5-10let, protože dochází ke stárnutí výrobního materiálu. Také se k tomu může podepsat skladovací podmínky takovýchto médii, jelikož může dojít k poškrábání povrchu a tím znemožnit čtení disku.[54]

Kryptologie

Prvopočátky kryptografie se nacházejí již v Cézarově monoalfabetické substituční šifře. Jedná se vědeckou disciplínu zabývající se, jak ochranou dat a informací před neoprávněným čtením, tak i jejich celistvosti. Tato věda se dá rozdělit do dvou skupin, první část se zaměřuje na kódování a šifrování textu, kterou nazýváme

[53] HOMÉR. *Zálohování a ochrana dat* [Online]. 2009[cit. 2014-2-20]. Dostupný z WWW: <http://uloz.to/xm9XdZo/zalohovani-a-ochrana-dat-doc/>.
[54] MINISTR, J. *Informační bezpečnost.* Karviná : SOŠ ochrany osob a majetku s.r.o., 2011. s. 94 – 95.

kryptografie, zatímco druhá část je soustředěna na analýzu algoritmů a zašifrovaných dat, označovanou jako kryptoanalýza.[55]

Data a informace nacházející se v běžné číslicové podobě se označují jako otevřený text, jelikož se dá snadno přečíst a je dostupný všem osobám mající přístup k tomuto textu a právě i nežádoucí uživatelé, kterým nejsou tato data a informace určeny. Za použití různých algoritmů, se z otevřeného textu provede převod na šifrovaný nečitelný text, takovýto proces je nazýván šifrování. Pro vytváření zašifrovaných textů, je možno využít dvou základních typů šifer. Jedná se o symetrickou a asymetrickou kryptografii, jež se liší v technice šifrování.[56]

Symetrická kryptografie je založena na principu jednoho šifrovacího klíče. Tedy pomocí klíče je vytvořen z otevřeného textu zašifrovaný a využití stejného klíče je umožněn opačný proces, ze kterého je znovu získán otevřený text, čitelný pro uživatele vlastnící požadovaný klič. Výhodou tohoto typu šifrování je nízká výpočetní náročnost, což umožňuje rychlejší šifrování či dešifrování. Jsou zde i nevýhody v podobě distribuce klíče každému uživateli, kterým je šifrovaný text určen, což s sebou může nést určité riziko v podobě odhalení klíče.[57]

Asymetrická kryptografie je odlišná od předchozího typu šifrování jedním klíčem. V tomto typu šifrování jsou využity dva klíče, které jsou založeny na náročnosti jejich matematického výpočtu, jak při šifrování, tak i dešifrování, což se projevuje v delší časové náročnosti pro dekódování zprávy, proto se tento typ šifrování nehodí pro komunikaci vyžadující rychlou reakci. Jeden z klíčů je označován jako soukromý klíč, k němuž má přístup pouze jeho vlastník a druhý je nazýván veřejným klíčem, jelikož se zpravidla nachází na veřejně přístupné databázi, do které mohou uživatelé nahlížet. Oba klíče jsou jiné matematické hodnoty zajišťující vzájemnou ochranu, jelikož není možné pomocí veřejného klíče vytvořit odpovídající soukromý klíč. Tento systém je využit při vytváření elektronického podpisu. Jednoznačnou výhodou této šifry je její relativní bezpečnost využívající vysokých číslicových výpočtů.[58]

Elektronický podpis je založen na principu asymetrické šifry, jenž je využíván při zjišťování identity autorů dokumentů nahrazující podobu vlastnoručního podpisu. Skládá se z velmi vysokého čísla, jež využívá jako svou ochranu proti prolomení. Použití podpisu je jednak využíváno k identifikaci toho, kdo jej vytvořil, ale také se

[55]KURTZ, G., MCLURE, S., SCAMBRAY, J. *Hacking bez tajemství.* Praha : Computer Press, 2002. s. 510.
[56] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 4-5.
[57] JAŠEK, R. *Informační a datová bezpečnost*. Zlín : Univerzita Tomáše Bati ve Zlíně, 2006, s. 93.
[58] PETERKA, J. *Báječný svět elektronického podpisu*. Praha : CZ.NIC, 2011, úroveň 1-8 – 1-9.

využívá při komunikaci s veřejnou správou, jež pro veškeré dokumenty přijaté v elektronické podobě přikládá stejnou váhu, jako pro informace poskytnuté v listinné podobě.[59]

[59] PETERKA, J. *Báječný svět elektronického podpisu*. Praha : CZ.NIC, 2011, úroveň 1-2 – 1-3.

6. Normy a certifikace

Jedná se o stanovená pravidla pro různé výrobce informačních technologií, aby se zajistila jejich vzájemná kontabilita a mohla mezi nimi probíhat komunikace. Nejedná se zde jen o normy technické, ale jsou zde i normy zabývající se počítačovou bezpečností, které jsou zaměřeny na ochranu dat a informací.

Vytvářet takovéto normy mohou pouze standardizované organizace, jež mohou být národního, mezinárodního či odborového charakteru. Česká republika je v této oblasti zastoupena Českým normalizačním institutem vydávající české normy pro různé oblasti technických, bezpečnostních odvětví. Tato norma je označována jednotným názvem ČSN. Mezi nejvýznamnější mezinárodní normalizační organizaci se řadí International Standardization Organization, označována zkratkou ISO vyskytující se u všech norem vydaných touto společností. Pro standarty vydaných Evropskou unií je použito označení EN. Veškeré vytvořené normy je možno přebírat i jinými státy, jakožto i Český normalizační institut přejímá zahraniční standarty, jež nesou kombinované označení jako např.: ČSN ISO nebo ČSN EN. Musí však nést stejné číselné označení, jako u vytvořeného originálu.[60]

6.1. Hodnocení informačního systému

Pro získání přehledu bezpečnosti informačního systému jsou použity normy, jež mají za úkol poskytnout možnost výběru uživateli, jaký druh bezpečnostního systému si zvolí a do kterého investuje finanční prostředky. Vývojář daného zabezpečovacího systému může dodržovat pravidla stanovené normou, což dává výslednému produktu určitou míru bezpečnosti. Na konec systém zhodnotí odborný posuzovatel z hlediska jeho bezpečnosti a za použití příslušných norem určí, jak je tento systém bezpečný. K hodnocení bezpečnosti je možno užit několik norem a záleží jen na osobě, jaký typ zvolí. První hodnotící normou jsou americká kritéria TCSEC, která vznikla pro potřeby americké armády a k nim odpovídající požadavky kladeny na systém. Tato kritéria definují několik bezpečnostních tříd označeny velkými písmeny – D, C, H, A. Každá z těchto tříd má svou úroveň bezpečnosti. Dále se do hodnotících norem řadí evropská kritéria ITSEC, která byla vytvořena zejména pro obchodní zaměření, jelikož je zde vícero bezpečnostních úrovní pro detailnější selekci dat a informací. Přednostně se zde

[60] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 17-18.

vyskytují třídy funkčnosti určující funkce bezpečnosti obsažené v informačních systémech. Jednotlivé stupně ochrany, jsou vytvořeny tak, aby byly synchronní s americkými kritérii. Mají i podobná dělení: F C, F C2, F B1, F B2, F B3. Dále se zde vyskytují třídy zaručující určitou míru bezpečnosti obsahující prostředky, kterými se má ověřit správné nasazení bezpečnostních funkcí. Mezi další normy se sem řadí kanadská kritéria CTCPPEC, ve které je bezpečnost vnímána poněkud jiným směrem. Bezpečnostní funkce jsou rozděleny do několika skupin mající několik funkcí. Podle druhu bezpečnostní funkce v každé skupině, se stanoví úroveň zajištění bezpečnosti. V neposlední řadě se zde nacházejí i společná common criteria, která vnikla spojením všech předchozích norem. Jedná se o „běžná kritéria“ sjednocující vydané normy, zejména pro výrobce výpočetní techniky k zajištění kontability mezi jednotlivým hardwarem různých výrobců a zemí. [61]

Tabulka 1 - hodnocení kritérií pro důvěryhodné systémy[62]

Třída	Název	Základní údaje
A1	Ověřená konstrukce	Formální specifikace ověřenou na nejvyšší úrovni, kanál pro formální skrytou analýzu, ukázka neformální kódové korespondence
B3	Bezpečnostní domény	Referenční kontrola (zabezpečení jádra), "vysoce odolný vůči průniku"
B2	Strukturovaná ochrana	Formální model, omezení skrytých kanálů, zabezpečení orientované architektury, "relativně odolný vůči průniku"
B1	popsané ochrany bezpečnosti	Povinně přístupné ovládací prvky, označení bezpečnosti, odstraňování chyb související s bezpečností
C2	Kontrolovaný přístup	Individuální odpovědnost, rozsáhlí audit, add-on balíčky
C1	Diskrétní	Sektorová kontrola přístupu, ochrana proti nehodám mezi spolupracujícími uživateli
D	Minimální ochrana	Nehodnoceno

[61] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. s. 17-18.
[62] GASSER, M. *Building a Secure Computer Systém.* Ney York : Van Nostrand Reinhold, 1988. s. 5.

6.1.1. Analýza rizik

Každá činnost v oblasti informačních technologií je více méně spojeno s určitým rizikem, které je možno definovat jako nebezpečí, které může nastat kdykoliv během určité události nebo akce a negativně ovlivnit data a informace či jiné strategie a cíle. Míra rizika se dá zjistit z několika faktorů, jednak je to velikost negativního dopadu a pravděpodobnost, kdy se dané riziko vyskytne. Hlavním cílem analýzy rizik je tedy určit, jaká rizika hrozí a také jejich dopady s možností zjištění přijatelnosti pro daný systém. Velikost rizika se dá stanovit podle pravděpodobnosti jeho výskytu a dopadu pro informační systém. Takto uskutečněná analýza je použitelná pro každou oblast, i pro IS organizace a společnosti.[63]

Výsledkem analýzy rizik neboli bezpečnostní analýzy, jsou informace potřebné k učení kontrolních mechanizmu, které jsou nutné pro daný systém a naopak přebytečné. Provedením analýzy rizik je nutné myslet na nezbytný faktor a tím je čas. Takto získané informace jsou získány v určitém časovém okamžiku a vzhledem k neustálému vývoji, jak v informačním prostředí, tak i prostředí ve kterém se pracuje, je nutné analýzu rizik aktualizovat v určitém časovém horizontu.[64]

V současné době je možno využít 4 přístupů k při provádění analýzy rizik:[65]

1, Základní analýza rizik – veškerá opatření jsou postavena na základě podobnosti jiných systémů a z všeobecných bezpečnostních standardů.

2, Neformální analýza rizik – analýza je provedena odborníky bez užití bezpečnostních standardů.

3, detailní analýza rizik – analýza je provedena strukturovanou metodou ve všech bodech bezpečnostní analýzy. Jedná se o nejpřesnější metodu, avšak je s tím spjata finanční a časová náročnost.

4, kombinovaná analýza rizik – jedná se o analýzu, v niž může být použita základní, neformální a detailní metoda v jakékoliv oblasti, dle výběru. Tato analýza je nečastěji používanou metodou.

Výstupem takovéto analýzy rizik, je popis rizik, které mohou nastat pro informační systém a zároveň i popsání bezpečnostních požadavků snižující působení

[63] MINISTR, J. *Informační bezpečnost.* Karviná : SOŠ ochrany osob a majetku s.r.o., 2011. s. 46.
[64] JAŠEK, R. *Informační a datová bezpečnost*. Zlín : Univerzita Tomáše Bati ve Zlíně, 2006, s. 50.
[65] POŽÁR, J. *Informační bezpečnost*. Plzaň : Aleš Čeněk, 2005. s. 86.

rizika na přijatelnou úroveň. Jsou zde i uvedeny detaily stávajících bezpečnostních opatření, proto je nutné tento dokument chránit před přístupem nepovolaných osob. Kvůli obsahu podrobných informací o kritických místech v organizaci, je tento dokument určen úzkému okruhu lidí v managementu a v rámci organizace má nejvyšší stupeň utajení.[66]

6.2. Charakteristika normy ISO/IEC 27001

Norma ISO/IEC se dá charakterizovat, jako určitý postup řešení v oblasti informační bezpečnosti. Veškeré zkušenosti a znalosti získané v oblasti informační bezpečnosti, jsou shrnuty do tohoto dokumentu mezinárodního charakteru. Celý dokument je rozdělen do několika sekcí a zároveň stanovuje příslušné bezpečnostní požadavky pro každou úroveň, což zajišťuje určitou úroveň ochrany pro data a informace. Obsahem dokumentu je: bezpečnostní politika, organizace bezpečnosti informací, klasifikace a řízení aktiv, bezpečnost lidských zdrojů, fyzická bezpečnost a bezpečnost prostředí, řízení komunikací a řízení provozu, řízení přístupu, vývoj a údržba informačního systému, zvládání bezpečnostních incidentů, řízení kontinuity činností organizace, soulad s požadavky. Veškeré bezpečnostní požadavky lze charakterizovat, jako seznam úkolů, jenž musí být splněny k dosažení optimálního zabezpečení, zároveň musí být popsány obecně pro použitelnost v různých typech oborů (bankovnictví, doprava, vzdělání).[67]

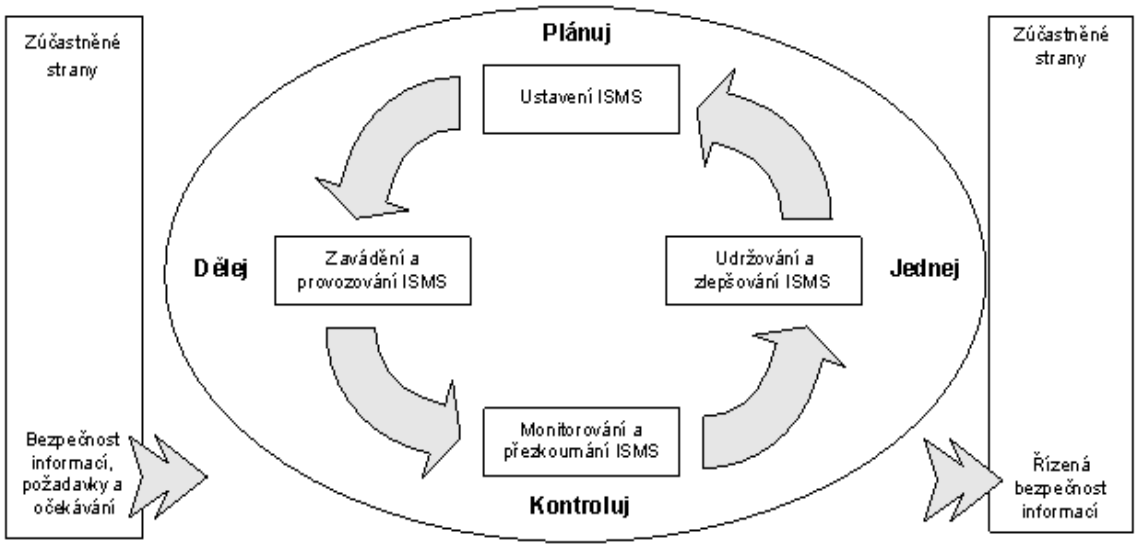
Obsahem této normy je prosazování tzv. procesního přístupu, jež je určitou aplikací systému procesů v organizaci a jejich identifikaci a vzájemným působením a řízením. Pro správnou a efektivní funkčnost organizace, musí být identifikovány a řízeny činnosti, které jsou navzájem propojeny. Činnost využívající zdroje a řízení za určitým účelem přeměny vstupu na výstup, se dá označit jako proces. Výstup daného procesu, může být použít jako vstup do jiného procesu. Při využití procesního přístupu v oblasti bezpečnostního managementu, je kladen důraz na: pochopení požadavků na bezpečnost informací organizace a potřebu stanovení politiky a cílů bezpečnosti informací, zavedení a provozování opatření pro management bezpečnosti informací

[66] MINISTR, J. *Informační bezpečnost.* Karviná : SOŠ ochrany osob a majetku s.r.o., 2011. s. 47.
[67] MINISTR, J. *Informační bezpečnost.* Karviná : SOŠ ochrany osob a majetku s.r.o., 2011. s. 59 – 60.

v kontextu s řízením celkových rizik činností organizace, monitorování a přezkoumání výkonnosti a účinnosti ISMS, neustálé zlepšování založené na objektivním měření.[68]

Tato norma povoluje model známí jako PDCA (plan-do-check-act), neboli plánuj-dělej-kontroluj-jednej, jež může být aplikován na všechny procesy ISMS (information security management system). Celý model rozdělen do čtyř základních kroků, jež na sebe navazují.

Obrázek 4 – modelový příklad PDCA[69]



Prvním krokem je plán, neboli zhodnotit současnou výkonnost či případné problémy v systému. Shromáždit data o zásadních problémech s cílem eliminovat jejich příčiny. Nakonec navrhnout a naplánovat řešení, jak dosáhnout požadovaného cíle. Druhým krokem je provedení plánu, jež zavádí v účinnosti naplánované řešení. Třetím krokem je kontrola zhodnocující výsledky, získané testováním systému a je nutné posoudit úroveň dosažení naplánovaných cílů. Posledním krokem je samotné jednání [70]

6.3.Zákonné předpisy

Tato část kapitoly se věnuje právním předpisům týkající se oblasti informační bezpečnosti. Pozornost není věnována jen zákonné stránce, ale na úvod kapitoly jsou

[68] ČSN ISO/IEC 27001. *Systém managementu bezpečnosti informací.* Praha : Český normalizační úřad, 2006. s. 6.
[69] *Csnonline* [Online]. [cit. 2014-3-14]. Dostupný z WWW: <http://csnonlinefirmy.unmz.cz/html_nahledy/36/76533/76533_nahled.htm>.
[70] *Patlalca site* [Online]. 2010 [cit. 2014-3-14]. Dostupný z WWW: <http://patlalca.wz.cz/2010/03/RIZENI-JAKOSTI-VE-STREDNIM-PODNIKU.html>.

uvedena pojmosloví související s právem, jako je např. duševní vlastnictví či právo autorské.

Právo duševního vlastnictví

Tento pojem se dá charakterizovat jako souhrn právních norem vznikající při lidské tvůrčí činnosti. Tedy základním předmětem pro duševní vlastnictví je nehmotná podstata, na rozdíl od ostatních věcí movitého a nemovitého charakteru. Tento pojem byl vymezen v roce 1967 světovou organizací duševního vlastnictví, jež dává autorská práva duševnímu vlastnictví v souvisejících oblastech, jako jsou: vynálezy, průmyslové vzory, ochranné známky, obchodní firmy a obchodní jména, vědecké objevy, práva na ochranu proti nekalé soutěži a všechna další práva vztahující se k nehmotné činnosti v různých oblastech např. průmyslu, vědní obory, literatura a umělectví, obchodní tajemství, zlepšovací návrhy, know-how, topografie polovodičů, odrůdám rostlin, obsah databáze a typografické znaky.[71]

Za duševní vlastnictví se dá však považovat pouze to, co je dostatečně originální a nedá se opakovat. Pro určení hodnoty duševního vlastnictví je nutno vzít v potaz několik faktorů, jednak záleží na míře využitelnosti a jaký je přínos pro společnost i jedince, dále záleží na schopnosti podnětu k vytváření další tvorby (hmotné či nehmotné).[72]

Autorské právo a software

Autorské právo se dá charakterizovat, jako soubor právních norem upravující vztahy z tvorby literární, vědecké či umělecké nebo se na toto právo dá nahlížet, jako na souhrn oprávnění mezi autorem a jeho dílem. K právu autorskému je příbuzné oprávnění dalších osob, může se jednat např. o: pořizovatel databáze či výkonného umělce. Také se zde projevuje účast jiných subjektů, které zprostředkovávají užití děl v konkrétních případech, jedná se o: divadelní agentury, umělecká galerie. Software (počítačový program) je v České republice chráněn autorským právem, jež je součástí duševního vlastnictví. Avšak autorské právo chrání pouze konkrétní vytvořená díla, které lze vnímat v určité podobě, ale nechrání samotné myšlenky či ideje.[73]

[71] ŠTĚDROŇ, B. *Ochrana a licencování počítačového programu.* Praha : Wolters Kluwer, 2010. s. 2 - 3.
[72] *Czeplinn* [Online]. 2010 [cit. 2014-3-15]. Dostupný z WWW: <http://www.czeplinn.eu/cs/articles/mental-property/110-duevni-vlastnictvi>.
[73] *Autorské právo* [Online]. 2011 [cit. 2014-3-15]. Dostupný z WWW: <http://www.autorske-pravo.info/pojem-autorskeho-prava>.

Softwarový patent

Patent je určen k právní ochraně určitého vynálezu, jež zaručuje majiteli výlučné právo pro využívání vynálezu. Platnost tohoto patentu se uděluje na 20 let. Jedná se o jakýsi monopol, který je časově omezen a je udělen vynálezci nebo objeviteli určité technologie, ale za podmínky, že musí být zveřejněna. Patentovat lze jak konkrétní věc, produkt, tak i určitý proces. Softwarový patent je určen k ochraně virtuálního majetku, konkrétně určitý programový proces (způsob programování).[74]

Zákony související s informační bezpečností

Zákonné formy pro informační bezpečnost se vyskytují různých oblastí, jako je: trestní zákon, obchodní či občanský zákoník. Každé jednání se posuzuje a řadí pod konkrétní paragraf v dané oblasti nebo určují odpovědnost subjektů pracující s daty a informacemi.

Zákon č. 499/2004 Sb. O archivnictví a spisové službě a o změně některých zákonů. Tento zákon upravuje výběr a evidenci archiválií, ochranu archiválií, práva a povinnosti vlastníků archiválií, práva a povinnosti držitelů a správců archiválií (dále jen "držitel archiválie"), využívání archiválií, zpracování osobních údajů pro účely archivnictví, soustavu archivů, práva a povinnosti zřizovatelů archivů, spisovou službu, působnost Ministerstva vnitra (dále jen "ministerstvo") a dalších správních úřadů na úseku archivnictví a výkonu spisové služby, správní delikty.[75]

Zákon č. 106/1999 Sb. o svobodném přístupu k informacím. Podle §2 je povinnost poskytovat informace následující: [76]

1. Povinnými subjekty, které mají podle tohoto zákona povinnost poskytovat informace vztahující se k jejich působnosti, jsou státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce.
2. Povinnými subjekty jsou dále ty subjekty, kterým zákon svěřil rozhodování o právech, právem chráněných zájmech nebo povinnostech fyzických nebo

[74] ŠTĚDROŇ, B. *Ochrana a licencování počítačového programu*. Praha : Wolters Kluwer, 2010. s. 7.
[75] ČESKO. Zákon č. 499 ze dne 30. Června 2004 o archivnictví a spisové službě a o změně některých zákonů. In *Sbírka zákonů České republiky*. 2004, částka 173, s. 1. Dostupné také z WWW:<http://www.zakonyprolidi.cz/cs/2004-499>.
[76] ČESKO. Zákon č. 106 ze dne 8. Června 1999 o svobodném přístupu k informacím. In *Sbírka zákonů České republiky*. 1999, částka 39, s. 1-2. Dostupné také z WWW:<http://eagri.cz/public/web/mze/legislativa/pravni-predpisy-mze/tematicky-prehled/Legislativa-ostatni_uplna-zneni_zakon-1999-106-pristup-k-informacim.html>.

právnických osob v oblasti veřejné správy, a to pouze v rozsahu této jejich rozhodovací činnosti.

3. Zákon se nevztahuje na poskytování informací, které jsou předmětem průmyslového vlastnictví, a dalších informací, pokud zvláštní zákon upravuje jejich poskytování, zejména vyřízení žádosti včetně náležitostí a způsobu podání žádosti, lhůt, opravných prostředků a způsobu poskytnutí informací.
4. Povinnost poskytovat informace se netýká dotazů na názory, budoucí rozhodnutí a vytváření nových informací.

Zákon č. 412/2005 Sb. O ochraně utajovaných informací a o bezpečnosti způsobilosti. Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.[77]

Zákon č. 101/2000 Sb. O ochraně osobních údajů a o změně některých zákonů. Tento zákon v souladu s právem Evropských společenství, mezinárodními smlouvami, kterými je Česká republika vázána, a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.[78]

Zákon č. 365/2000 Sb. Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů. Tento zákon stanoví práva a povinnosti, které souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy.[79]

[77] ČESKO. Zákon č. 412 ze dne 21. Září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In *Sbírka zákonů České republiky*. 2005, částka 143, s. 1. Dostupné také z WWW:<http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/uplne-zneni-zakona-c-4122005/>.
[78] ČESKO. Zákon č. 101 ze dne 4. Dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In *Sbírka zákonů České republiky*. 2000, částka 32, s. 1. Dostupné také z WWW:<http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00101&cd=76&typ=r>.
[79] ČESKO. Zákon č. 365 ze dne 14. Září 2000 o informačních systémech veřejné správy. In *Sbírka zákonů České republiky*. 2000, částka 99, s. 1. Dostupné také z WWW:<http://www.zakonyprolidi.cz/cs/2000-365>.

7. Vyhodnocení dotazníku

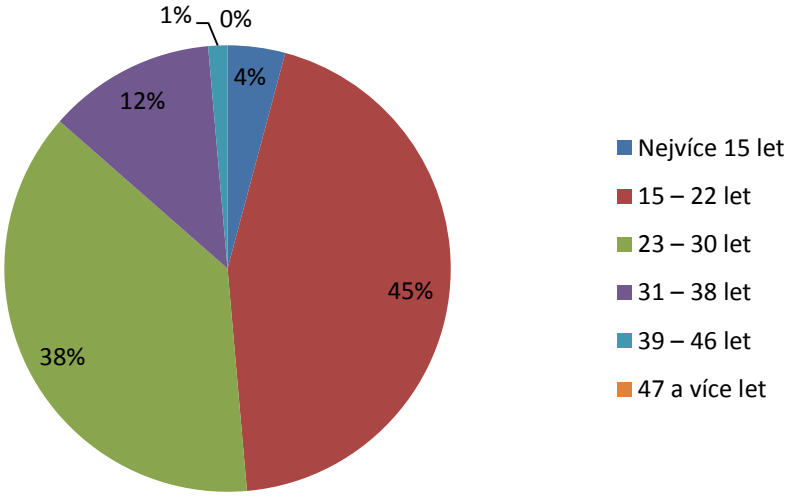
V této části je obsaženo vyhodnocení jednotlivých otázek dotazníku. Celý dotazník je vytvořen 15 uzavřenými otázkami a jednou možností výběru. Respondenti byli získáváni na sociálních sítích, jelikož se dá předpokládat, že zde budou uživatele, často využívající počítač. Závěrem hodnocení jsou vydána doporučení, jak správně chránit svá data a informace. Dotazník byl prezentován v elektronické formě a celkem jej vyplnilo 288 respondentů.

Věková skupina

Tato otázka v dotazníku měla spíše orientačně zařadit respondenta do určité věkové skupiny.

Z grafu je patrné, že nejpočetnější věková skupina respondentů je v rozmezí mezi 15 a 22 roky tvořící 45% (tedy 128 lidí) z celkového počtu. Následovány jsou 38% (109 lidí) pro věkovou skupinu 23 – 30 let. Dále již malou skupinu tvořili respondenti od věku 31 let a výše tvořící celkově 17% (39 lidí). Lze tedy říci, že nejpočetnější skupina uživatelů, kteří odpovídali na tento dotazník, se nachází ve věkovém rozhraní 15 – 30 let tvořící dohromady 83% (237 lidí).

Graf 1 – věková skupina respondentů[80]



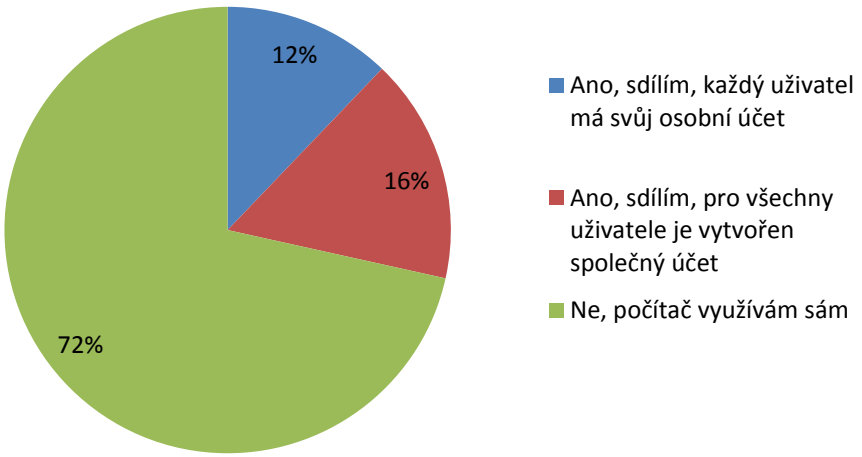
[80] Vlastní zdroj

Sdílíte počítač s ostatními uživateli?

Tato otázka si klade za cíl, zjistit zda je počítač sdílen i jinými uživateli. Počet uživatelů pracující na jednom přístroji je důležitý z pohledu bezpečnosti, jelikož každý uživatel se jinak chová při prohlížení internetových stránek a případně stahování různých souborů. Tím může ohrozit bezpečnost jiných uživatelů.

Největší počet respondentů 72% (206 lidí) využívají počítač sami, tedy si mohou kontrolovat bezpečnost dat a informací. V případě sdílení počítače s jinými uživateli jsou dvě možnosti. První z nich je použití stejného účtu, jež vybralo 16% (47 lidí). Druhou možností je sdílení počítače, ale při použití správce účtů, která tvoří nejmenší skupinu s 12% (35 lidí). Tato možnost se dá považovat za bezpečnou, protože každý uživatel má svůj osobní účet a zároveň jsou chráněny data jiných osobních účtů nacházející se v daném počítači.

Graf 2 – sdílení počítače[81]



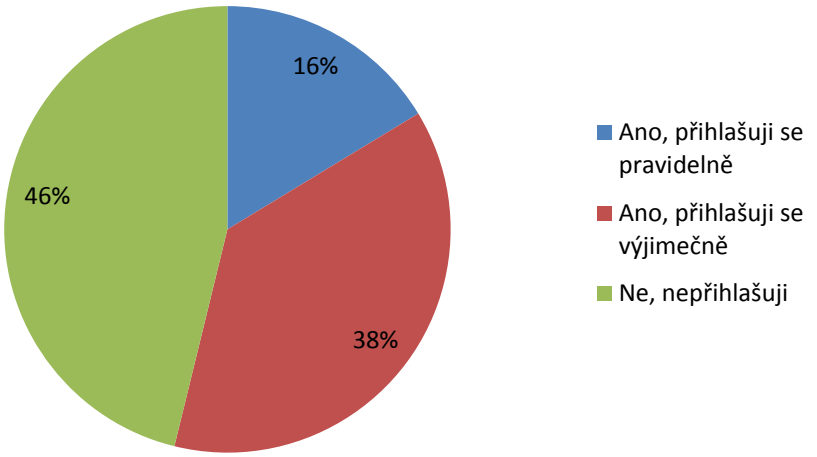
[81] Vlastní zdroj

Přihlašujete se na internetové účty na veřejných počítačích (kavárny, školy)?

Používání veřejně přístupných počítačů nese s sebou bezpečnostní riziko, jelikož má k tomuto hardwaru kdokoliv přístup a proto mohou být infikovány škodlivým softwarem za účelem získání přihlašovacích údajů veškerých uživatelů používající tento počítač.

V dotazníkovém šetření bylo zjištěno, že největší počet respondentů 46% (133 lidí), nevyužívá veřejných počítačů. V otázce přihlašování se na tyto počítače jsou vytvořeny dvě otázky. První se zaměřila na výjimečné využití volící 38% (108 lidí). Druhá otázka zjišťovala pravidelné používání veřejné přístupných počítačů, kterou vybralo 16% (47 lidí).

Graf 3 – přihlašování na veřejných počítačích[82]



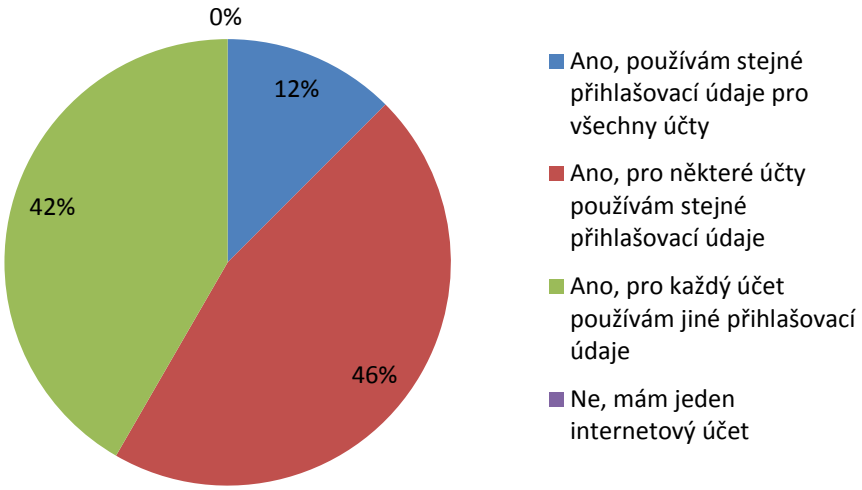
[82] Vlastní zdroj

Využíváte více internetových účtů (e-mail, on-line hry, sociální profily)?

Tato otázka se zaměřila na užívání více internetových účtů a také na přihlašovací údaje k nim.

Z grafu je patrné, že každý respondent má více jak jeden internetový účet. Rozlišení otázek bylo v možnostech přihlašovacích údajů. První variantou je, zda uživatel používá stejné heslo a jméno k přihlášení do všech svých účtů, tuto možnost zvolilo 12% (36 lidí) respondentů tvořící nejmenší část. Druhá otázka se naopak zaměřila na používání jiných přihlašovacích údajů pro každý účet, jež byla vybrána v 42% (120 lidí). Poslední variantou bylo, zda jsou stejné přihlašovací údaje použitu jen u některých účtů tvořící největší část respondentů s 46% (132 lidí).

Graf 4 – používání více internetových účtů[83]



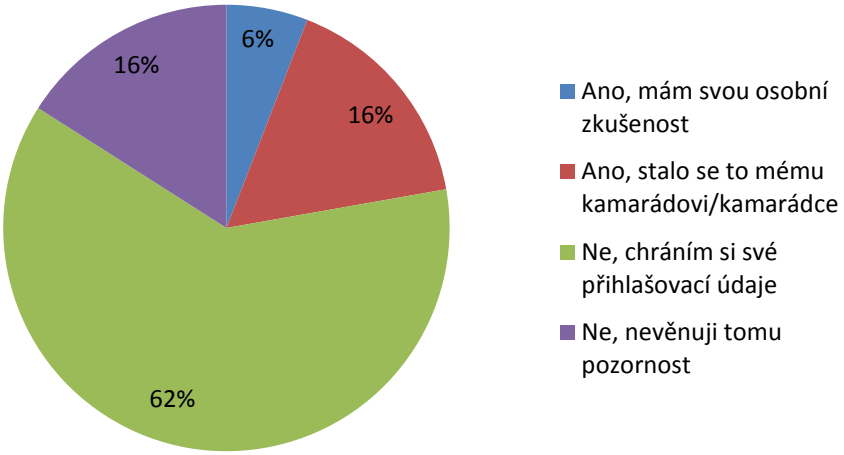
[83] Vlastní zdroj

Setkali jste se s případem odcizení internetového účtu?

Tato otázka zjišťuje, zda se respondent setkal s odcizením internetového účtu, jednak ze své osobní zkušenosti či z okolí jeho přátel.

Z grafu je patrné, že největší počet respondentů si chrání své přihlašovací údaje nebo se snaží zabránit zneužití svého účtu v 62% (178 lidí) a zároveň se nesetkali s případem odcizení. Druhou nejpočetnější odpovědí je setkání se odcizením v okruhu přátel, tato varianta byla vybrána 16% (47 lidí). Další odpovědí, ve které se respondenti nesetkali s tímto případem a berou ho na lehkou váhu nevěnujíce mu pozornost, zvolilo 16% (46 lidí). Ostatní 6% (17 lidí) mají svou osobní zkušenost.

Graf 5 – setkání s případem odcizení[84]



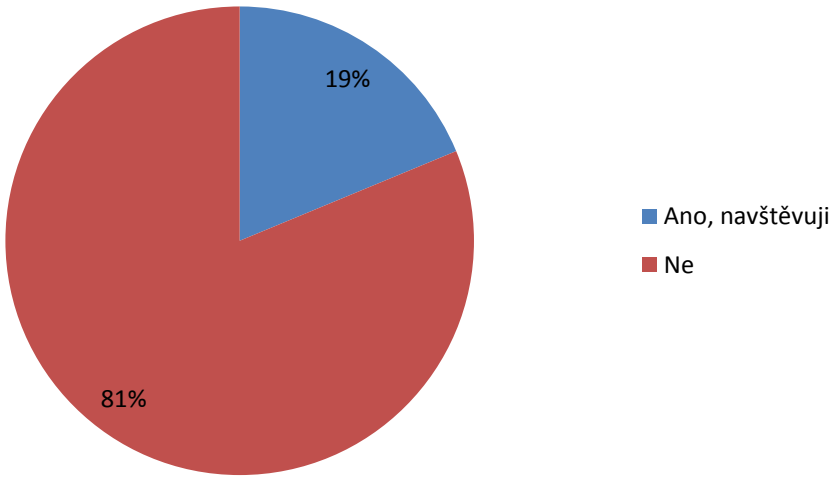
[84] Vlastní zdroj

Navštěvujete internetové stránky, které jsou označeny jako nedůvěryhodné?

V této otázce se zjišťuje, zda respondenti navštěvují stránky, které jsou označeny jako nedůvěryhodné. Může se jednat o stránky, na kterých se ukrývá škodlivý software a během prohlížení těchto stránek, se může infiltrovat do počítače nebo to mohou být internetové stránky s neúplnou certifikací.

Z odpovědí vyplývá, že 81% (234 lidí) se těmto stránkám vyhýbá a nenavštěvuje je. Zatím co 19% (54 lidí) se nebojí tyto nedůvěryhodné internetové stránky navštěvovat.

Graf 6 – navštěvování nedůvěryhodných stránek[85]



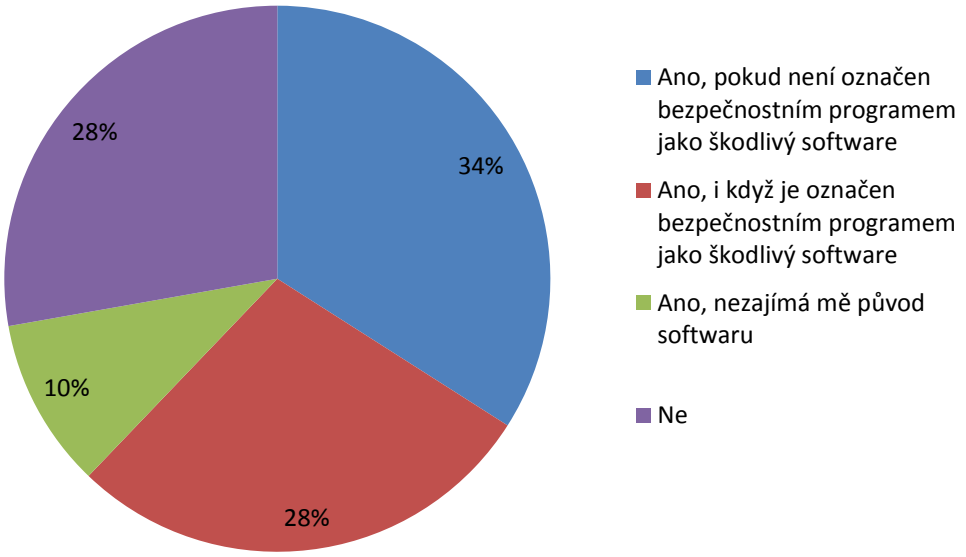
[85] Vlastní zdroj

Stahujete či jinak pracujete se softwarem, u kterého si nejste jistí jeho důvěryhodností?

Tato otázka si klade za cíl zjistit, zda respondent pracuje s programem, u kterého si není jistý je důvěrnosti či původem a také za jakých okolností je ochoten s tímto softwarem manipulovat. Takto neznámý program může nést s sebou určité riziko, jelikož se může jednat škodlivý software s určitým cílem poškodit uživatele.

Největší část respondentů 34% (98 lidí) je ochotna pracovat s tímto typem programu za předpokladu, že nebude označen jako škodlivý software bezpečnostním programem nacházející se v daném počítači. Další část 28% (81 lidí) pracuje s tím softwarem, i když je určen jako škodlivý software. S takto nedůvěryhodným programem odmítá pracovat 28% (80 lidí) respondentů. V posledním případě respondenti pracuji s tímto softwarem a přitom je nezajímá jeho původ a to v 10% (29 lidí).

Graf 7 – Pracování s nedůvěryhodným programem[86]



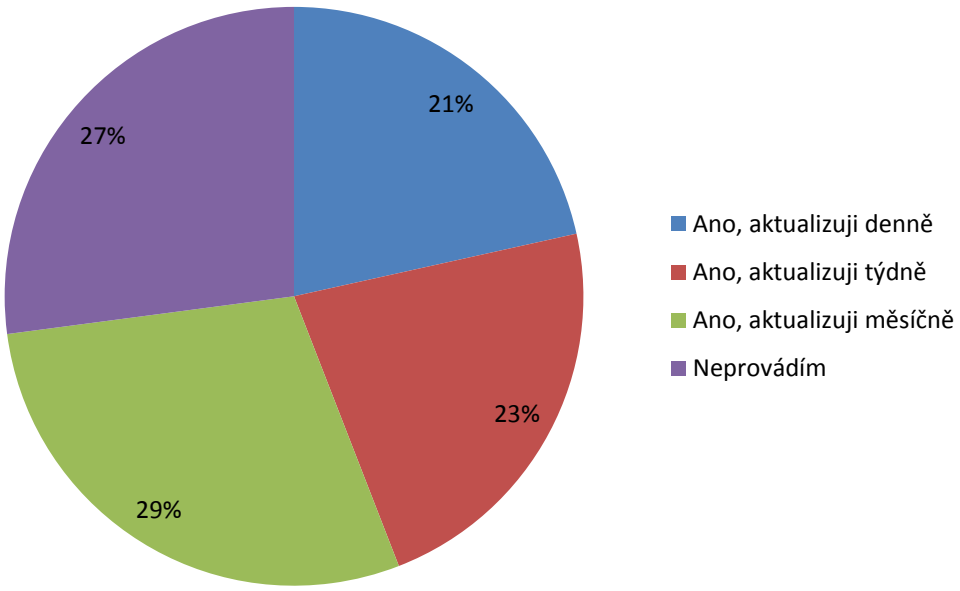
[86] Vlastní zdroj

Provádíte pravidelné aktualizace softwaru (operační systém, antivirové programy)?

Provádění pravidelných aktualizace je zásadní k udržení určité úrovně bezpečnosti v počítači, jelikož je nutné přizpůsobovat software novým vznikajícím hrozbám.

Největší podíl respondentů tvoří 29% (83 lidí) uvádějící, že provádějí aktualizaci softwaru v měsíčním cyklu. Druhou nejčastější odpovědí je neprovádění programové aktualizace v 27% (78 lidí). Třetím nejčastějším výběrem respondentů, je provádění aktualizací týdně, což zvolilo 23% (65 lidí). Poslední možnost zvolilo 21% (62 lidí) uvádějící denní aktualizace softwaru.

Graf 8 – pravidelné aktualizace softwaru[87]



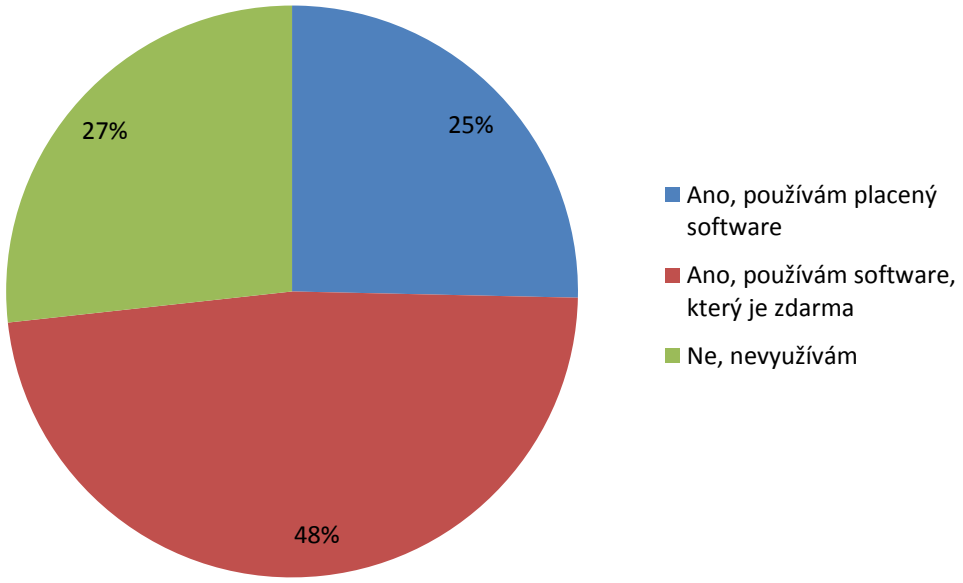
[87] Vlastní zdroj

Využíváte nějaké programy k ochraně dat a informací na svém počítači?

Bezpečnostní software by měl být nedílnou součástí počítače, jelikož může odhalit škodlivý program ještě před tím, než provede určitou nežádoucí činnost. Případně může zjistit, zda se již v počítači nenachází jiný nežádoucí software.

Dle grafu používá téměř polovina respondentů 48% (138 lidí) bezpečnostní program, který je nabízen zdarma. Tento typ programu je přijatelný, ale na rozdíl od placeného softwaru vybraný 25% (73 lidí) respondentů, nemusí nabízet určité ovládací prvky či plnou podporu. V 27% (77 lidí) respondenti uvedli, že neužívají bezpečnostní software ve svém počítači.

Graf 9 – typ používaného softwaru[88]



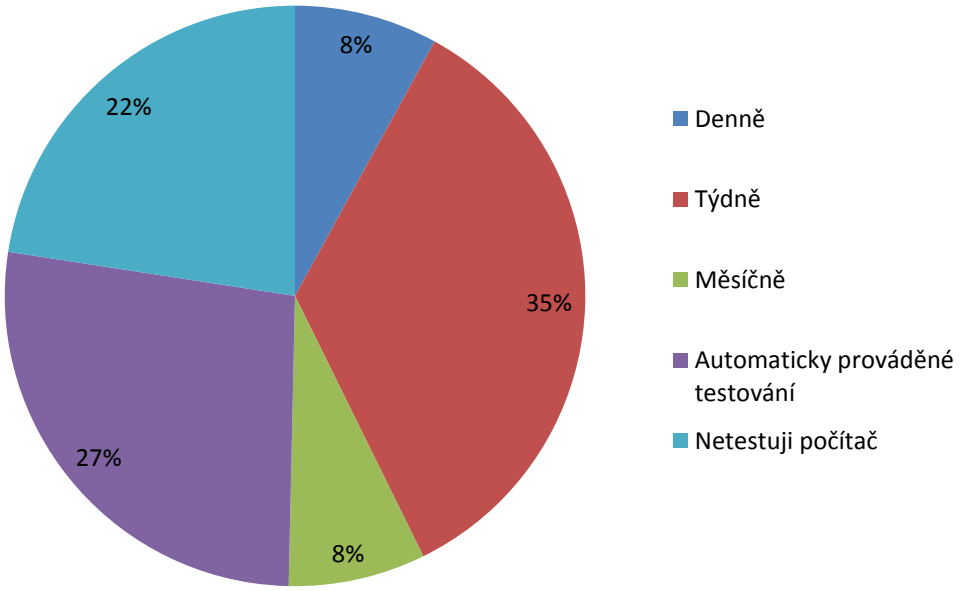
[88] Vlastní zdroj

Jak často provádíte testování počítače na škodlivý software?

Časté prováděné testování počítače může vést k odhalení skrytého škodlivého programu a tak předejít případnému nežádoucímu stavu.

Nejčastějším časovým cyklem pro kontrolu počítače je dle grafu týdně prováděné. Tuto možnost zvolilo 35% (100 lidí) respondentů, což je největším počtem. Druhá nejčastější zvolenou odpovědí je automaticky prováděné testování, na které se spoléhá 27% (78 lidí). Třetím největším počtem 22% (65 lidí) jsou respondenti, kteří neprovádí kontrolu počítače. Poslední dvě odpovědi, jsou co do počtu zvolených otázek, na shodné úrovni. První odpověď zvolilo 8% (23 lidí), kteří provádějí aktualizace každý den a druhá byla zaměřena na aktualizaci softwaru v měsíčním cyklu, kterou zvolilo 8% (22 lidí).

Graf 10 – četnost provedených testů na škodlivý software[89]



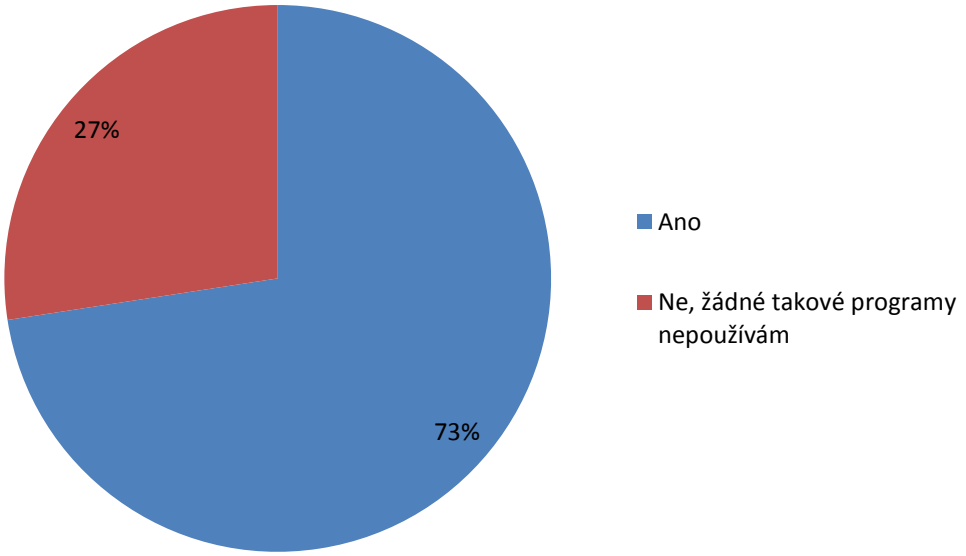
[89] Vlastní zdroj

Používáte programy pro správu softwaru (defragmentace, čištění registru)?

Používání těchto programů nepřímo ovlivňuje bezpečnost informací. Spíše slouží k údržbě softwarového vybavení počítače, ale může zabránit určitým nežádoucím jevům, jako je zpomalení výkonnosti počítače či jeho úplnému zkolabování z důvodu výskytu chyb v registrech.

Dle grafu je jednoznačné, že většina 73% (209 lidí) využívá určitou formu programů pro správu softwaru, ať v placené formě či zdarma. Zbylý počet respondentů 27% (79 lidí) nevyužívá žádného druhu takovéhoto programu.

Graf 11 – Používání programů pro správu softwaru[90]



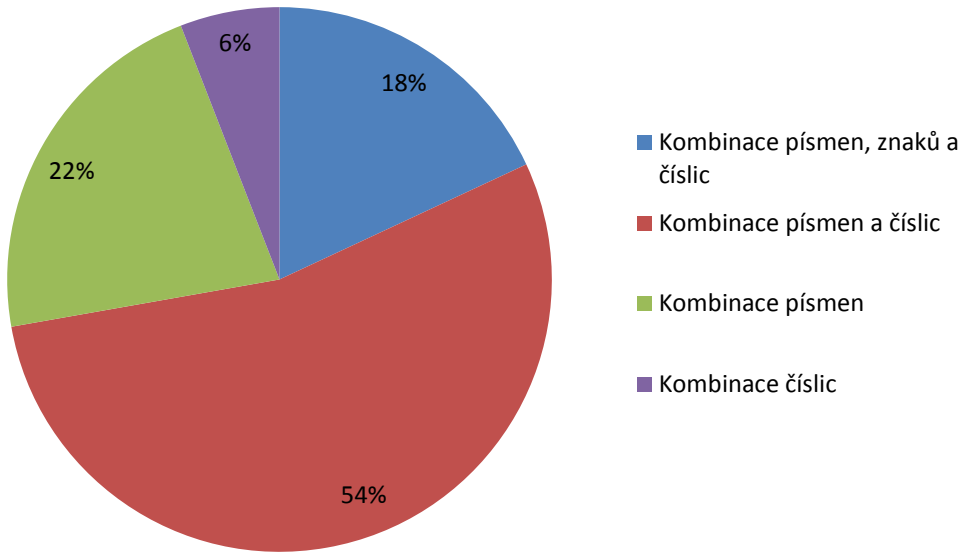
[90] Vlastní zdroj

Jako druh hesla používáte pro vaše účty?

Druh hesla je důležitý pro jeho bezpečnost, jelikož při využití kombinace znaků, písmen a číslic roste doba nutná pro jeho prolomení případným útočníkem.

Nejčastěji volenou odpovědí respondentů 54% (156 lidí), kteří používají ve svém hesle kombinací písmen a číslic. Druhou nejčastější odpovědí je využití hesla složenou jen z písmen, tuto variantu zvolilo 22% (63 lidí). S 18% (52 lidí) respondentů je tato odpověď na třetím místě. Tuto možnost volili uživatelé hesla tvořenou kombinací písmen, znaků a číslic. Poslední variantu hesla skládající se pouze z číslic zvolilo 6% (17 lidí).

Graf 12 – druh hesla[91]



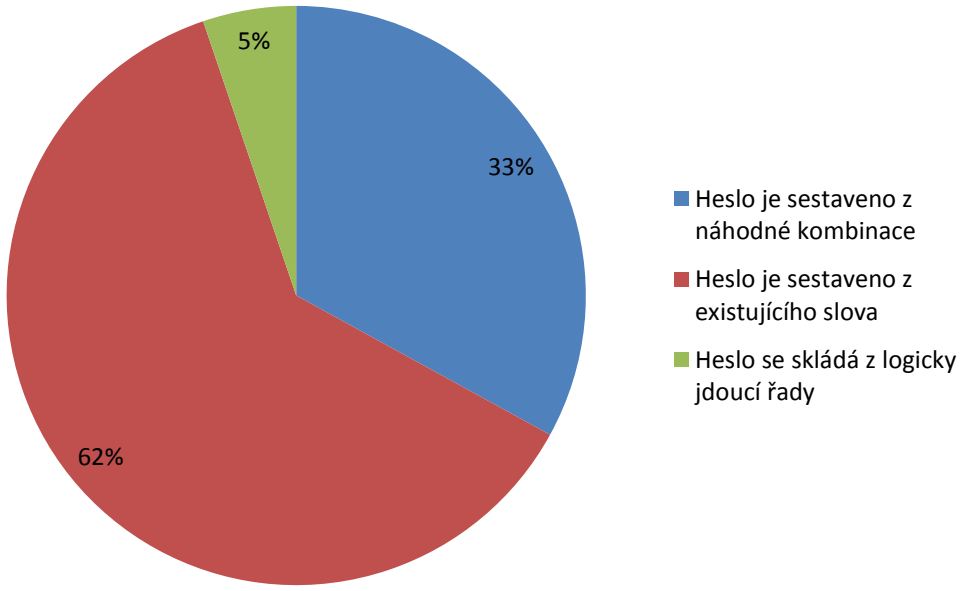
[91] Vlastní zdroj

Jaká je skladba vašeho hesla?

Skladba hesla je jaký si postup jak bylo heslo vytvořeno. Může se jednat o náhoně poskládané heslo či je to určité existující slovo, ať přeložené do jiného jazyka nebo je to jednoduchá matematická posloupnost.

Z grafu lze vyčíst, že největší podíl 62% (178 lidí) respondentů, používá heslo, které bylo vytvořeno z již existujícího slova. Druhou možnost zvolilo 33% (95 lidí), jejíž heslo je sestaveno pomocí náhodné kombinace. V poslední odpovědí se heslo skládá z určité logické posloupnosti, ať matematické či jazykové. Tuto variantu zvolilo 5% (15 lidí).

Graf 13 – skladba hesla[92]



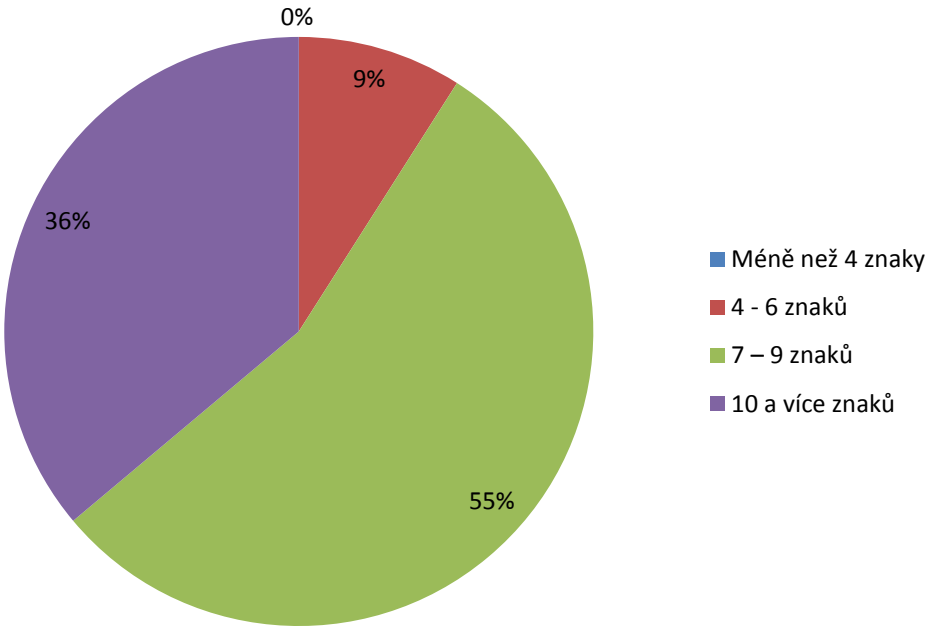
[92] Vlastní zdroj

Jaká je délka vašeho hesla?

Každé heslo by mělo mít správnou délku, jelikož dobře složené heslo může být snadno prolomeno, pokud obsahuje málo znaků, ovšem s rostoucí délkou roste i jeho doba potřebná k překonání.

Na první pohled je patrné, že heslo s méně jak 4 znaky nevyužívá žádný z respondentů, může to být dáno tím, že při registraci nových účtů, je vyžadováno heslo s minimálním počtem 6 či více znaků. Délku hesla 4 – 6 znaků zvolilo 9% (26 lidí). Nejdelší heslo s 10 a více znaky využívané respondenty, zvolilo 36% (104 lidí). Nejvíce volenou odpovědí je délka hesla používající 7 – 9 znaků, kterou vybralo 55% (158 lidí).

Graf 14 – délka hesla[93]



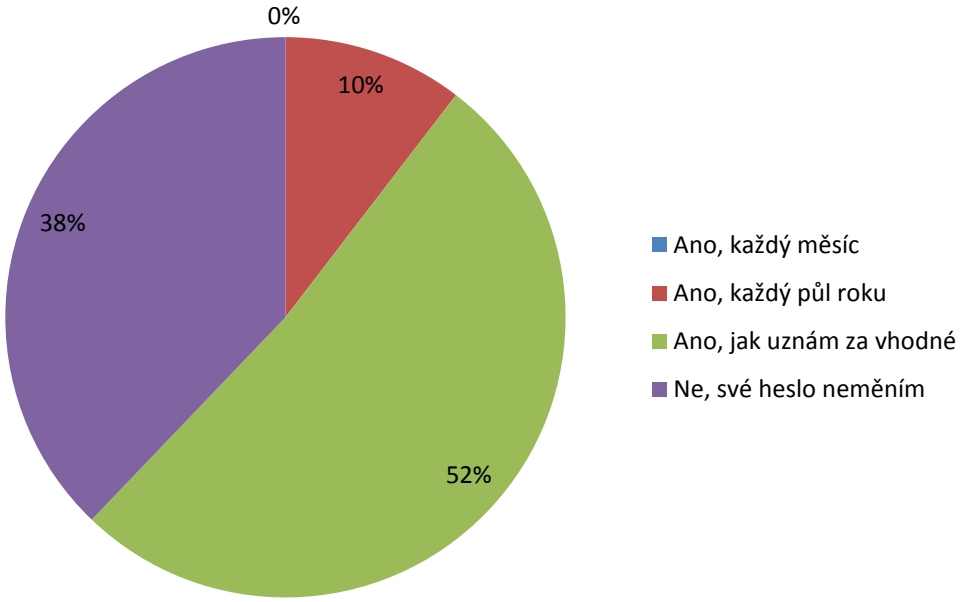
[93] Vlastní zdroj

Měníte své heslo pravidelně?

Každé heslo je potřeba změnit z bezpečnostních důvodů, ať již v určitém časovém cyklu nebo kdykoliv je potřeba. Pokud chrání velmi důležitá data a informace, měla by se provádět změna hesla častěji, aby jej nebylo možné zjistit určitou metodou používanou útočníky.

Nejvíce zvolenou možností respondenty je změna hesla dle jejich uvážení. Tuto možnost vybralo 52% (149 lidí) nejspíše proto, že nemají stanovený určitý časový cyklický termín a jednají na základě svých pocitů. Druhou nejčastější odpovědí respondentů je, že své heslo nemění, což zvolilo 38% (109). Třetí varianta s 10% (30 lidí) stanovila termín obměny hesla na každých půl roku. Poslední možnost aktualizace hesla každý měsíc, žádný z respondentů nezvolil, možná proto, že je tento cyklus příliš krátký.

Graf 15 – obměna hesla[94]



[94] Vlastní zdroj

8. Doporučení

Cílem této kapitoly je vydat určitá doporučení, jak správně chránit svá data a informace a případně předejít jejich poškození či ztrátě. Celá kapitola je rozdělena na tzv. desatero zásada. Každá z těchto zásad obsahuje základní vlastnost a popis jak ji dosáhnout.

Aktualizace softwaru – pravidelná aktualizace je nutná pro správnou funkčnost programů, ať se jedná o operační systém, antivirové programy, firewall i pro další software. Současné programy již mají v sobě zabudované automatické aktualizace, ale je dobré je kontrolovat, zda jsou prováděny.

Dobře vytvořené heslo – správně vytvořené heslo by mělo mít minimální délku v počtu 8 znaků a více, ale samotný počet nestačí, důležitý je rovněž složení, jestli se jedná o náhodnou kombinaci písmen a číslic či je heslo vytvořeno podle existující osoby nebo předmětu. Heslo by mělo být vytvořené podle určitého klíče, který nelze snadno odhadnout a zároveň vede k lepšímu pamatování.

Změna hesla – obměna hesla by se měla provádět pravidel z bezpečnostních důvodů. Ideální časový cyklus je mezi 3 – 4 měsícem. Ovšem záleží na daném uživateli, jak moc mu záleží na datech chráněná heslem a jeho přístupu k zabezpečení.

Heslo nikomu nesdělujeme – na první pohled se to zdá jako logická věc, ale je dobré si na to dát pozor, jelikož se mohou objevit různé elektronické zprávy vyzívající k zadání vašich přihlašovacích údajů, které jsou podvodně vytvořeny za účelem získání informací. Také poskytování údajů svým přátelům je určitým bezpečnostním rizikem, protože přátelství nemusí vždy vydržet a pak může dojít k zneužití těchto údajů.

Veřejné počítače – se mohou vyskytovat v různých kavárnách či školách, na které má veřejnost přístup. Právě proto jsou tyto počítače nebezpečné, jelikož mohou být infikovány různým škodlivým softwarem získávající přihlašovací údaje uživatelů používající takovýto počítač.

Bezpečnostní programy – jedná se o software, který je zaměřen na detekci a likvidaci škodlivých programů, které se vyskytnou v počítači. Takovýto program by měl být nainstalován v každém počítači, protože poskytuje alespoň určitou úroveň bezpečnosti.

Neznámé odkazy – nejčastěji jsou šířeny elektronickou poštou a lákají příjemce na různé stránky. Avšak je nutné být pozorný, jelikož se může jednat o odkaz ke stažení škodlivého softwaru či přesměrování na podvodné internetové stránky mající za úkol získat důvěrné informace.

Neznámý program – je takový software, u kterého není znám jeho původ. Může se jednat např. o prospěšný software, ale za ním je skryt škodlivý program sbírající různá data (přihlašovací údaje). Pokud si nejsme jistí jeho původem, tak je lepší se tomuto softwaru vyhnout a rozhodně ho nespouštět.

Přenosná média – jedná se především o přenosné pevné disky či paměti flash. Slouží k přenosu dat a informací mezi počítači, ale je nutné si dát pozor při jejich používání. Existuje mnoho druhů škodlivých programů šířící se skrz tyto zařízení. Proto je dobré tyto přenosné paměti kontrolovat bezpečnostním programem.

Přihlašování na internetových stránkách – přihlašování by mělo probíhat tam, kde dobře známe dané stránky, nejlépe pak pokud jsou zabezpečeny (na začátku internetové adresy je http – kde „s“ znamená zabezpečený). Na pozoru bychom měly být, před pro nás neznámé prostředí a zvláště pokud po nás vyžadují osobní údaje.

Závěr

V úvodu se bakalářská práce zaměřila na všeobecnou definici informační bezpečnosti, na kterou je hleděno jako na praktickou disciplínu informatiky zajišťující tři základní bezpečnostní atributy důvěrnost, dostupnost a integrita. Všechny tyto aspekty tvořící dohromady úroveň bezpečnosti informací, jsou v práci dále podrobněji popsány a jakou hrají roli pro data a informace.

Práce se dále zaobírá osvětlení vybraných pojmů z oblasti informatiky, se kterými se dá setkat, jak v této bakalářské práci, tak i mimo ni. Všechny pojmy jsou stručně a jasně charakterizovány pro snadné pochopení.

Po úvodních kapitolách se bakalářská práce dostává ke svému hlavnímu cíli a tím jsou způsoby, jak zabezpečit a ochránit data a informace. Celá tato kapitola je rozdělena do dvou hlavních částí na fyzickou a softwarovou ochranu dat. Do fyzické kapitoly jsou řazeny ty způsoby ochrany ovlivňující data pomocí určitého technického zařízení. Skrze toto zařízení je realizováno zabezpečení, jedná se např. o snímače otisků prstů, přepěťové ochrany, protipožární zabezpečení a jiné. U softwarové ochrany je práce zaměřena na užití různých programových doplňků zvyšující odolnost vůči nepříznivým jevům, ať úmyslného tak i technického charakteru. Veškeré způsoby ochrany dat a informací v obou kapitolách, jsou stručně charakterizovány pro pochopení jejich základních principů, na kterých fungují. Uvedené způsoby ochrany jsou používány jak v organizacích, tak i běžnými uživateli na jejich domácích počítačích. Tohoto hlavního cíle se mi podařilo dosáhnout pomocí odborné literatury a jiných elektronických zdrojů, včetně cizojazyčných.

Dílčím cílem této bakalářské práce bylo zjištění efektivity norem na vytváření bezpečnostních systémů. Začátkem této kapitoly byla stručná charakteristika normy a subjektů podílející se na jejich vytváření, jež mohou být státního, soukromého charakteru. Dále se tato kapitola zaobírá hodnocením informačního systému a jsou zde stručně charakterizovány určitá kritéria používající se při vytváření určité úrovně bezpečnosti. V této časti je také obsažena podkapitola s názvem analýza rizik. Jedná se o činnost, která má za úkol zjištění, jaká rizika hrozí pro daný počítačový systém a také jaké by měly dopady na data a informace. Při zjištění, jaké nežádoucí jevy mohou hrozit, tak je potřeba proti nim vytvořit protiopatření a záleží jen na majiteli počítače, zda je přijme a kolik do nich bude investovat finančních prostředků. Tato část kapitoly dále charakterizuje konkrétní normu ISO/IEC 27001, její využití a základní funkčnost

tohoto dokumentu. Veškeré bezpečnostní normy jsou zejména využívány pro různé organizace a společnosti, jež zajišťují určitou úroveň bezpečnosti a využití těchto norem v „domácím prostředí“ by bylo nevhodné či dokonce nemožné.

Poslední kapitolou teoretické části jsou zákonné předpisy. Úvodem této části jsou uvedeny základní pojmosloví související s právním pojetím. Jedná se o duševní právo, autorské právo a softwarový patent. Jednotlivé pojmy jsou stručně charakterizovány z právního pohledu. Dále se tato kapitola zaobírá právními předpisy související s problematikou okolo bezpečnosti informací. Zákony jsou citovány tak, aby byla vyložena jejich základní myšlenka.

Praktická část bakalářské práce je zaměřena na vyhodnocení dotazníkového šetření získané elektronickou formou od respondentů na sociálních sítích. Celý dotazník je složen z 15 uzavřených otázek týkající se bezpečnosti informací. Jednotlivé otázky zjišťují postoj respondentů k dané problematice. Jedná se např. o: sdílení počítače s jinými uživateli, pohyb v internetovém prostředí, práce s neznámým softwarem či různé varianty otázek ohledně používaného hesla. Celý dotazník byl vyplněn 288 respondenty, kde u jednotlivých uzavřených otázek měly na výběr z předem daných možností, jež pouze jedna z nich mohla být vybrána. Na konec dotazníku jsou vydána doporučení, jak chránit své údaje či případně jak se vyhnout nežádoucím situacím, např. ztrátě hesla. Vyhodnocením dotazníku, byly vytvořeny grafy a stručný popis jednotlivých otázek. Také byl zjištěn postoj respondentů k této problematice. Uvědomují si rizika, která jim hrozí, jež neberou na lehkou váhu a snaží se chránit své údaje. Lze tedy říci, že úroveň ochrany dat a informací u respondentů je na vysoké úrovni.

Splnění hypotéz

Hypotéza 1: Počet respondentů využívající jakýkoliv bezpečnostní program je vyšší než 70%. Tato hypotéza je splněna. Celkový počet získaný dotazníkem je73%.

Hypotéza 2: Více jak 70% respondentů nesdílí svůj počítač s jinými uživateli. Tato hypotéza je splněna. Celkem 72% nesdílí svůj počítač.

Hypotéza 3: Své heslo nemění více jak 50% respondentů. Tato hypotéza je nesplněna. Respondenti v počtu 38% si nechávají stejné heslo.

Seznam použité literatury

Literární zdroje

1. ČSN ISO/IEC 27001. *Systém managementu bezpečnosti informací*. Praha : Český normalizační úřad, 2006. 35 s. Třídící znak 36 9790.
2. DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.
3. GASSER, M. *Building a Secure Computer System.* Ney York : Van Nostrand Reinhold, 1988. 236 s. ISBN 0-442-23022-2.
4. HOWLETT, T. *Open source security tools.* New Jersey : Pearson Education, 2005. 578 s. ISBN 0-321-19443-8.
5. JAŠEK, R. *Informační a datová bezpečnost*. Zlín : Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 8073184567
6. KURTZ, G., MCLURE, S., SCAMBRAY, J. *Hacking bez tajemství.* Praha : Computer Press, 2002. 625 s. ISBN 80-7226-644-6.
7. MOJMÍR, K. *Bezpečnost domácího počítače.* Praha : Grada, 2006. 336 s. ISBN 80-247-1408-6.
8. PETERKA, J. *Báječný svět elektronického podpisu*. Praha : CZ.NIC, 2011, 304 s. ISBN 978-80-904248-3-8.
9. POŽÁR, J. *Informační bezpečnost.* Plzeň : Aleš Čeněk, 2005. 311 s. ISBN 80-86898-38-5.
10. ŠTĚDROŇ, B. *Ochrana a licencování počítačového programu.* Praha : Wolters Kluwer, 2010. 220 s. ISBN 978-80-7357-555-7.

Elektronické zdroje

1. *Antivirove centrum* [Online]. 1998 - 2014 [cit. 2014-2-13]. Dostupný z WWW: <http://www.antivirovecentrum.cz/antispyware.aspx>.
2. *Autorské právo* [Online]. 2011 [cit. 2014-3-15]. Dostupný z WWW: <http://www.autorske-pravo.info/pojem-autorskeho-prava>.
3. *Biometrický identifikační systém* [Online]. 2006 - 2008 [cit. 2014-1-4]. Dostupný z WWW: <http://www.vlastnicesta.cz/clanky/informace-a-bezpecnost/>.
4. *Clever and Smart* [Online]. 2008-2014 [cit. 2014-1-2]. Dostupný z WWW: <http://www.cleverandsmart.cz/informacni-bezpecnost/>.

5. C*snonline* [Online]. [cit. 2014-3-14]. Dostupný z WWW: <http://csnonlinefirmy.unmz.cz/html_nahledy/36/76533/76533_nahled.htm>.
6. *Czeplinn* [Online]. 2010 [cit. 2014-3-15]. Dostupný z WWW: <http://www.czeplinn.eu/cs/articles/mental-property/110-duevni-vlastnictvi>.
7. *Elektrodynamika* [Online]. 2010 [cit. 2014-1-16]. Dostupný z WWW: <http://kdf.mff.cuni.cz/vyuka/elektrodynamika/doku.php?id=experimenty:faradayova_klec>.
8. *Hoax.cz* [Online]. 2000 - 2014 [cit. 2014-2-14]. Dostupný z WWW: <http://www.hoax.cz/cze/>.
9. HOMÉR. *Zálohování a ochrana dat* [Online]. 2009[cit. 2014-2-20]. Dostupný z WWW: <http://uloz.to/xm9XdZo/zalohovani-a-ochrana-dat-doc/>.
10. *Ikaros* [Online]. 1997-2013 [cit. 2014-1-2]. Dostupný z WWW: <http://www.ikaros.cz/bezpecnost-dat-v-informacnich-systemech>.
11. *Informace a bezpečnost* [Online]. 2011 [cit. 2014-1-4]. Dostupný z WWW: <http://www.vlastnicesta.cz/clanky/informace-a-bezpecnost/>.
12. *Lupa.cz* [Online]. 1998 - 2014 [cit. 2014-2-14]. Dostupný z WWW: <http://www.lupa.cz/clanky/denial-of-service-dos-utoky-zaplavove-typy/ >.
13. MINISTR, J. *Informační bezpečnost.* Karviná : SOŠ ochrany osob a majetku s.r.o., 2011. s. 81
14. *Muj soubor* [Online]. 2012 [cit. 2014-2-14]. Dostupný z WWW: <http://mujsoubor.cz/magazin/nejlepsi-antivirove-programy>.
15. *Patlalca site* [Online]. 2010 [cit. 2014-3-14]. Dostupný z WWW: <http://patlalca.wz.cz/2010/03/RIZENI-JAKOSTI-VE-STREDNIM-PODNIKU.html>.
16. *PC security* [Online]. [cit. 2014-2-14]. Dostupný z WWW: <http://pc-security.cz/slovnik-pojmu/malware//>.
17. *Počítačová bezpečnost a ochrana dat* [Online]. [cit. 2014-2-14]. Dostupný z WWW: <http://marlib.cmsps.cz/bezpecnost/bezpecnost.html/>.
18. *Počítačová bezpečnost a ochrana dat* [Online]. [cit. 2014-2-14]. Dostupný z WWW: <http://marlib.cmsps.cz/bezpecnost/bezpecnost.html/>.
19. *Root.cz* [Online]. 1998 - 2004 [cit. 2014-2-14]. Dostupný z WWW: <http://www.root.cz/slovnicek/>.
20. *Viry.cz* [Online]. 2014 [cit. 2014-2-14]. Dostupný z WWW:<http://www.viry.cz/firewall-vs-bezny-uzivatel/>.

21. *Wordpress* [Online]. 2010 [cit. 2014-2-14]. Dostupný z WWW:<http://stipek.wordpress.com/slovnik/>.
22. *ZCU* [Online]. [cit. 2014-3-5], Dostupný z WWW: <http://home.zcu.cz/~gabra6/>.

Legislativní dokumenty

1. ČESKO. Zákon č. 101 ze dne 4. Dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In *Sbírka zákonů České republiky*. 2000, částka 32, Dostupné také z WWW:<http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00101&cd=76&typ=r>.
2. ČESKO. Zákon č. 106 ze dne 8. Června 1999 o svobodném přístupu k informacím. In *Sbírka zákonů České republiky*. 1999, částka 39, Dostupné také z WWW:<http://eagri.cz/public/web/mze/legislativa/pravni-predpisy-mze/tematicky-prehled/Legislativa-ostatni_uplna-zneni_zakon-1999-106-pristup-k-informacim.html>.
3. ČESKO. Zákon č. 365 ze dne 14. Září 2000 o informačních systémech veřejné správy. In *Sbírka zákonů České republiky*. 2000, částka 99, Dostupné také z WWW:<http://www.zakonyprolidi.cz/cs/2000-365>.
4. ČESKO. Zákon č. 412 ze dne 21. Září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In *Sbírka zákonů České republiky*. 2005, částka 143, Dostupné také z WWW:<http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/uplne-zneni-zakona-c-4122005/>.
5. ČESKO. Zákon č. 499 ze dne 30. Června 2004 o archivnictví a spisové službě a o změně některých zákonů. In *Sbírka zákonů České republiky*. 2004, částka 173, Dostupné také z WWW:<http://www.zakonyprolidi.cz/cs/2004-499>.

Seznam tabulek, grafů a obrázků

Seznam příloh

Příloha I.

Dotazník počítačové gramotnosti v oblasti zabezpečení dat a informací

Dobrý den, prosím Vás o vyplnění tohoto dotazníku, který se věnuje zabezpečením dat a informací v informačních technologiích. Celý dotazník se skládá z uzavřených otázek a jeho vyplnění by mělo zabrat nejvíce 5min. Výsledky šetření budou použity v bakalářské práci na téma: Bezpečnost informací v informačních technologiích. Předem Vám děkuji za Váš čas a spolupráci.

Věková skupina
- Do 15 let
- 15 – 22 let
- 23 – 30 let
- 31 – 38 let
- 39 – 46 let
- 47 a více let

Sdílíte počítač s ostatními uživateli?
- Ano, sdílím, každý uživatel má svůj osobní účet
- Ano, sdílím, pro všechny uživatele je vytvořen společný účet
- Ne, počítač využívám sám

Přihlašujete se na internetové účty na veřejných počítačích (kavárny, škola)?
- Ano, přihlašuji se pravidelně
- Ano, přihlašuji se výjimečně
- Ne, nepřihlašuji

Využíváte více internetových účtů (e-mail, on-line hry, sociální profily)?
- Ano, používám stejné přihlašovací údaje pro všechny účty
- Ano, pro některé účty používám stejné přihlašovací údaje
- Ano, pro každý účet používám jiné přihlašovací údaje
- Ne, mám jeden internetový účet

Setkali jste se s případem odcizení internetového účtu?
- Ano, mám svou osobní zkušenost
- Ano, stalo se to mému kamarádovi/kamarádce
- Ne, chráním si své přihlašovací údaje
- Ne, nevěnuji tomu pozornost

Navštěvujete internetové stránky, které jsou označeny jako nedůvěryhodné?
- Ano, navštěvuji
- Ne

Stahujete či jinak pracujete se softwarem, u kterého si nejste jistí jeho důvěryhodností?
- Ano, pokud není označen bezpečnostním programem jako škodlivý software
- Ano, i když je označen bezpečnostním programem jako škodlivý software
- Ano, nezajímá mě původ softwaru
- Ne

Provádíte pravidelné aktualizace softwaru (operační systém, antivirové programy)?
- Ano, aktualizuji denně
- Ano, aktualizuji týdně
- Ano, aktualizuji měsíčně
- Neprovádím

Využíváte nějaké programy k ochraně dat a informací na svém počítači?
- Ano, používám placený software

Ano, používám software, který je zdarma
Ne, nevyužívám

Jak často provádíte testování počítače na škodlivý software?
Denně
Týdně
Měsíčně
Automaticky prováděné testování
Netestuji počítač

Používáte programy pro správu softwaru (defragmentace, čištění registru)?
Ano
Ne, žádné takové programy nepoužívám

Jako druh hesla používáte pro vaše účty?
Kombinace písmen, znaků a číslic
Kombinace písmen a číslic
Kombinace písmen
Kombinace číslic

Jaká je skladba vašeho hesla?
Heslo je sestaveno z náhodné kombinace
Heslo je sestaveno z existujícího slova
Heslo se skládá z logicky jdoucí řady

Jaká je délka vašeho hesla?
Méně než 4 znaky
4 - 6 znaků
7 – 9 znaků
10 a více znaků

Měníte své heslo pravidelně?
Ano, každý měsíc
Ano, každý půl roku
Ano, jak uznám za vhodné
Ne, své heslo neměním

Děkuji Vám za vyplnění dotazníku a přeji hezký zbytek dne.