UNIVERZITA HRADEC KRÁLOVÉ

PŘÍRODOVĚDECKÁ FAKULTA

KATEDRA INFORMATIKY

Počítačová bezpečnost a ochrana dat

Diplomová práce

Autor: Pavla Skořepová

Studijní program: N1101

Studijní obor: Učitelství matematiky pro střední školy

Učitelství pro střední školy - informatika

Vedoucí práce: doc. RNDr. Štěpán Hubálovský, Ph.D.

Hradec Králové červen

Univerzita Hradec Králové
Přírodovědecká fakulta

Zadání diplomové práce

Autor:	**Pavla Skořepová**
Studijní program:	N1101
Studijní obor:	Učitelství matematiky pro střední školy Učitelství pro střední školy - informatika
Název závěrečné práce:	**Počítačová bezpečnost a ochrana dat**
Název závěrečné práce AJ:	Computer Security and Data Protection

Cíl, metody, literatura, předpoklady:
Cílem teoretické části práce je provést literární rešerši v oblasti problematiky počítačové bezpečnosti a ochrany dat. Budou popsány možnosti zneužití dat a možnosti ochrany dat. Cílem praktické části bude provést dotazníkový průzkum, který bude zjišťovat, jak uživatelé chrání svoje data. Dále bude v praktické části, na základě vyhodnocení průzkumu, navržen optimální způsob zabezpečení dat.

Garantující pracoviště:	Katedra informatiky, Přírodovědecká fakulta
Vedoucí práce:	doc. RNDr. Štěpán Hubálovský, Ph.D.
Konzultant:	
Oponent:	PhDr. Michal Musílek, Ph.D.
Datum zadání závěrečné práce:	23. 2. 2014
Datum odevzdání závěrečné práce:	

Prohlášení

Prohlašuji, že jsem diplomovou práci vypracovala samostatně a že jsem v seznamu použité literatury uvedla všechny prameny, z kterých jsem vycházela.

V Hradci Králové dne Podpis:

Poděkování

Děkuji vedoucímu diplomové práce doc. RNDr. Štěpánu Hubálovskému Ph.D. za odborné vedení diplomové práce, cenné rady a připomínky v průběhu zpracování této práce.

Dále děkuji své rodině a všem, kteří mi během zpracování diplomové práce pomohli nebo poradili.

Anotace

SKOŘEPOVÁ, P. *Počítačová bezpečnost a ochrana dat.* Hradec Králové, 2015. Diplomová práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí diplomové práce doc. RNDr. Štěpán Hubálovský Ph.D. 70s.

Tato diplomová práce se zabývá počítačovou bezpečností a ochranou dat. V teoretické části je vymezen pojem počítačová bezpečnost a její historie. Dále je popsáno dělení ochrany dat, autentizace, řízení přístupu, šifrování a elektronický podpis. Další kapitoly jsou věnovány počítačovým infiltracím a možnostem zabezpečení. Náplní praktické části je provedení dotazníkového průzkumu mezi uživateli, který má za úkol zjistit, jak uživatelé chrání svá data. Dotazníkový průzkum je východiskem k návrhu optimálního způsobu zabezpečení dat.

Klíčová slova

počítačová bezpečnost, ochrana dat, autentizace, řízení přístupu, infiltrace, zabezpečení

Abstract

SKOŘEPOVÁ, P. *Computer virus and antivirus protection.* Hradec Králové, 2015. Diploma Thesis at Faculty of Science University of Hradec Králové. Thesis Supervisor doc. RNDr. Štěpán Hubálovský Ph.D. 70p.

This diploma thesis deals with the computer security and data protection. In the theoretical part is defined the concept of computer security and its history. Also is described the division of data protection, authentication, access control, encryption and electronic signature. Other chapters are devoted to computer infiltration and options of the security. The aim of the practical part is the questionnaire survey among users, which is designed to determine how users protect their data. The questionnaire survey is the beginning for designing the optimal method of data security.

Keywords

computer security, data protection, authentication, access control, infiltration, security

Obsah

Úvod

V dnešní společnosti se počítače staly nedílnou součástí života. S rozšířením a používáním počítačů a Internetu v každodenním životě roste i jejich zneužívání. Počítač dnes využíváme téměř při všech činnostech, při komunikaci, k uzavírání smluv atd. Proto je třeba si uvědomit význam počítačové bezpečnosti a ochrany dat. Počítačové bezpečnosti se začíná v dnešní době věnovat větší pozornost. V předchozích letech se počítačovou bezpečností zabývali pouze odborníci, dnes by se o ní měli zajímat i běžní uživatelé počítačů.

V dnešní době se na uživatele vyvíjejí neustále nové infiltrace a vynalézavost útočníků nezná mezí. Proto by se o zabezpečení počítačů neměly zajímat jen firmy, ale i běžný uživatelé a chránit tak svá data, která by mohla být zneužita. Uživatelé počítačů by měli být seznámeni se základními pojmy a pravidly bezpečnosti a s tím, jak svůj počítač nejlépe zabezpečit a ochránit tak svá data proti různým útokům.

Cíle

Cílem diplomové práce je popsat možnosti ochrany dat a možnosti zneužití dat. Součástí diplomové práce bude i návrh optimálního způsobu zabezpečení dat.

Cíle teoretické části

Dílčími cíli teoretické části práce je:

- definovat pojem počítačová bezpečnost
- popsat různá hlediska ochrany dat
- popsat autentizaci a řízení přístupu
- popsat šifrování a elektronický podpis
- rozdělit útočníky a útoky podle různých hledisek
- popsat druhy infiltrací a možnosti zabezpečení

Těchto cílů bude dosaženo zpracováním, literární rešerše odborné literatury a elektronických zdrojů.

Cíle praktické části

Dílčím cílem praktické části diplomové práce je provést dva dotazníkové průzkumy, kterými bude zjištěno:

- jak uživatelé chrání svá data a dbají počítačové bezpečnosti

Dalším dílčím cílem je navrhnout (doporučit) optimální způsob zabezpečení dat. Východiskem k návrhu (doporučení) ochrany dat bude výše provedený a vyhodnocený dotazníkový průzkum

Teoretická část práce

1 Definice počítačové bezpečnosti

„Počítačová bezpečnost je stav, kdy je dosaženo dostupnosti, integrity, důvěrnosti, odpovědnosti [1].“

- Dostupnost – data jsou dostupná autorizovaným uživatelům.
- Integrita - změnu dat smí provádět pouze autorizovaní uživatelé.
- Důvěrnost - přístup k datům, mají pouze autorizovaní uživatelé.
- Odpovědnost – uživatelé jsou odpovědní za své aktivity [1].

1.1 Historie počítačové bezpečnosti

„Počítačová bezpečnost se postupem času stává problémem, který je nucen řešit stále větší počet uživatelů. Zatímco dříve se tento problém příliš neřešil nebo byl doménou odborníků, dnes se těmito problémy musí zabývat i koncový uživatel [2].“

V roce 1970 byl poprvé v USA vydán odborný článek, který se zabýval otázkami počítačové bezpečnosti. Na počátku 70 let vznikla síť Arpanet předchůdce Internetu. Na začátku bylo k síti připojeno kolem 50 počítačů, které byly převážně armádní. Síť Arpanet se postupem času rozšiřovala a v roce 1980 napadl tuto síť virus, který ji vyřadil z provozu, a docházelo k hlášení prvních bezpečnostních problémů. Na počátku sítě Arpanet byla bezpečnost až na posledním místě. V 80 letech vzrůstal zájem o počítačovou bezpečnost, objevuje se časopis Computers & Security, vznikla asociace Technical Committee on Security and Protection in Information Processing Systems. Vznikaly také i různé organizace hackerů jako třeba Chaos Computer Club. V roce 1981 hacker „Captain Zap“ pronikl do počítačové sítě AT&T a stal se prvním hackerem, který byl odsouzen za počítačovou kriminalitu. Dále se začala vydávat první oficiální kritéria hodnocení bezpečnosti počítačových systémů, dnes známá jako Orange Book. Vznikla první definice počítačového viru a americký kongres přijal Computer Fraud and Abuse Act (1986). Ze začátku se staly obětmi pouze významné společnosti, to se však na počátku 90. let s rozšířením Internetu mezi obyčejné lidi změnilo [3].

2 Ochrana dat

V dnešní době mají téměř všichni lidé a firmy svá data uložena ve formě počítačových souborů na disku. Data bychom měli chránit před kompromitací, modifikací a zničením. Problém ochrany dat je velmi důležitý a lidé by ho neměli podceňovat.

Podle Tomáše Doseděla [4] můžeme ochranu dat rozdělit na fyzickou ochranu dat, na ochranu logického přístupu k datům, ochranu dat před zničením, ochranu uložených dat, ochranu přenášených dat.

2.1 Fyzická ochrana dat

Fyzická ochrana dat zajišťuje, aby se k datům například nedostala neoprávněná osoba. Neoprávněná osoba, která má fyzický přístup k nosičům, na kterých jsou data uložena, může data pomocí fyzické síly zničit. Data je třeba také chránit před přírodními pohromami a před výpadky dodávky energie.

2.1.1 Fyzický přístup k datům

Pro zajištění bezpečnosti je důležité kontrolovat a monitorovat osoby, které mají přístup k datům.

Už při vstupu do budovy by mělo být kontrolováno, zda je osoba oprávněna ke vstupu do budovy. To je zajišťováno například vrátným, čipovými kartami, které umožňují automatické otevírání dveří, bezpečnostními kamerami nebo snímači pohybu. Je velmi důležité vědět, jaká osoba se v budově pohybuje.

Dále by měl být zabezpečen přístup k počítačovým systémům. Ty by měly být umístěny v uzamčených místnostech. Záleží, jak jsou data pro nás důležitá, například server může být umístěn v místnosti bez oken s bezpečnostními dveřmi.

Pevné disky se umísťují nejčastěji do skříní ATX. Do těchto skříní se neoprávněná osoba dostane většinou i pomocí šroubováku. Pevné disky s citlivějšími daty by měly být instalovány do bezpečnějších skříní [5].

2.1.2 Přírodní katastrofy

Přírodní katastrofy se nedají předem předvídat. A tak abychom data před nimi ochránily, je třeba se snažit omezit dopad katastrof na data [5].

Požáry jsou nebezpečné jak pro techniku, tak i pro lidi. Vždy by budova měla obsahovat plán pro evakuaci osob a důležitých dat. Mezi základní protipožární opatření patří automatické hasící systémy a hasicí přístroje. Prostory s technikou by neměly obsahovat lehce hořlavé materiály. Tyto prostory by měly být vybaveny protipožárními stěnami. Důležitá data by měla být uložena v prostorech, které mají vysokou protipožární bezpečnost.

Voda může data ohrozit dvojím způsobem buď záplavami, nebo závadami na vodovodních sítích. Důležité protizáplavové opatření je to, že prostory by měly mít vhodnou polohu. Důležitá data by měla být umístěna v horních patrech budovy a místnost by měla být izolována. Izolovány by měly být i počítačové skříně, ve kterých jsou pevné disky s daty umístěny. Při evakuaci budovy je vhodné jak při záplavách, tak i při závadách na vodovodních sítích mít určeno důležitost dat.

Je také důležité, v jakém prostředí jsou počítačové komponenty umístěny. Komponenty jsou citlivé na velké změny teplot, prach a vlhkost. To lze vyřešit nainstalováním klimatizace, která obsahuje filtrovací zařízení.

Při zemětřesení hrozí pád budov a následné zasypání pevných disků. Měla by být zajištěna odolnost proti prachu a pevné disky být nainstalovány do pevných a odolných skříní. Při menších zemětřesení je třeba dbát hlavně na to, aby byl disk dobře upevněn a nedošlo k pádu či nárazu [5].

2.1.3 Dodávka energie

Do ochrany fyzického přístupu patří také ochrana před výpadky energie a před nestabilními dodávkami energie. Podle Luboše Dobdy [5] zařízení, která dokáží data chránit před těmito vlivy, rozlišujeme podle principu činnosti na záložní zdroj typu off-line a on-line.

„Záložní ***zdroj off-line*** má napájecí výstup, kde jsou připojeny zálohované spotřebiče, je propojen přímo se vstupem do zdroje a energie z akumulátorů je dodávaná pouze při výpadku elektrického proudu.“ Obsahuje akumulátorový podsystém, který se průběžně dobíjí. Mezi výhody patří malé ztráty energie ve zdroji a nízká cena. Mezi nevýhody patří nemožnost filtrování kolísání sítě.

„U ***on-line zdroje*** je vstupní napájení vedeno přes vstupní měnič napětí, který převádí střídavé napětí na jednosměrné, do akumulátorů. Ty se dobíjejí a zároveň se stejnosměrné napětí výstupním měničem převádí zpět na střídavé, na výstup zdroje.“ Pokud dojde k výpadku energie tak nedochází k přepínání jako u zdroje typu Off-line, ale hned je dodána energie z akumulátorů. Mezi nevýhody patří neustále dobíjení akumulátorů, které se mohou přehřívat a dochází ke snížení jejich životnosti. Dochází také k energetickým ztrátám při přeměně elektrického napětí na stejnosměrné a hned znovu na střídavé [5].

2.2 Ochrana logického přístupu

Ochranu logického přístupu se snaží zajistit operační systém. Pomocí operačního systému můžeme nastavit přístupová práva a ověřit identitu uživatele. Nejdříve se uživatel musí identifikovat. Dále probíhá autentizace, v tomto kroku se ověřuje, zda uživatel řekl pravdu o své identitě. Autentizace může probíhat pomocí následujících metod – autentizace pomocí znalostí, vlastností nebo vlastnictví. Pomocí autentizačního protokolu se ověří identita uživatele. Pak už je na řadě systém pro řízení přístupu, který uživateli stanový druh přístupu a přístup k povoleným datům. Autentizaci a autorizaci jsou dále věnovány samostatné kapitoly [4].

2.3 Ochrana dat před zničením

Data mohou být buď poškozena, smazána, anebo může být fyzicky zničen nosič, na kterém jsou data uložena. Aby data nebyla nenávratně ztracena, je potřeba provádět jejich pravidelnou zálohu [4].

Zálohování je kopie vybraných dat, které jsou uloženy na jiném médiu. Pokud dojde ke ztrátě dat z původního média, vybraná data, která byla zálohována, můžeme obnovit. Zálohování by se mělo provádět často a pravidelně, aby nedocházelo k velké ztrátě dat [6].

Existují dvě strategie zálohování celková a inkrementální [6].

Celková strategie – při jejím použití dojde ke kompletní záloze dat. Výhodou celkové strategie je, že se data dají rychle obnovit. Nevýhodou je velká náročnost na výkon systému, dlouhý čas a velký objem dat, pro které musíme využít množství médií nebo velkou kapacitu na úložišti.

Inkrementální strategie – při této strategii budou zálohována pouze data, která se změnila od posledního zálohování. Vytváří se tedy sled datových záloh. Při obnově dat se začíná od nejstarší zálohy až po aktuální stav.

Je možné kombinovat oba dva typy strategií (pravidelně provádět celkovou zálohu a v mezi intervalech provádět inkrementální zálohu) [6].

Záložní kopie by se neměly ukládat a být na stejném místě, jako jsou uložena zálohovaná data. Aby zároveň se zálohovanými daty nebyly smazány i záložní kopie. Záložní kopie by měly být uloženy alespoň na místě, kam nemají přístup všichni, nejlépe uloženy v trezoru. Uživatelé by si měli uvědomit, že na záložní kopii jsou uložena data, která bychom měli chránit více než data uložená v počítači.

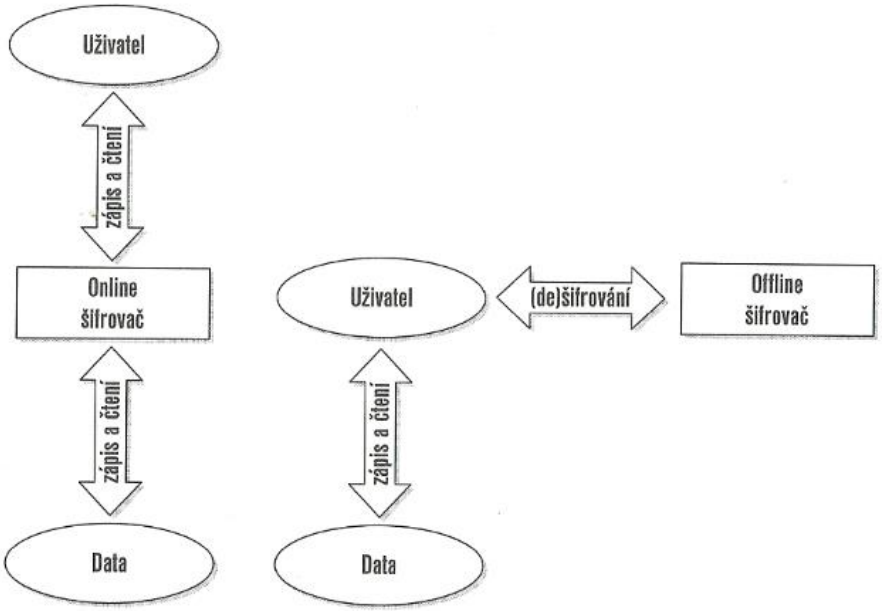
Je také samozřejmostí, že bychom záložní kopie měli pečlivě evidovat. Abychom věděli, které zálohy jsou pro nás ještě důležité a které už můžeme zrušit. Pokud záložní kopii už nepotřebujeme, měla by být nenávratně zničena.

2.4 Ochrana uložených dat

Pokud se útočník dostane k datům i přes fyzickou ochranu a přes autentizaci a autorizaci musíme zajistit ochranu dat ještě jiným způsobem. V tomto případě by měla pomoci kryptografie. Kryptologie se zabývá ochranou dat před jejich zneužitím. Dělíme ji na dvě části kryptografie a kryptoanalýza. Kryptografie se zabývá kódováním a dekódováním dat. Kryptoanalýza analyzuje algoritmy a zašifrovaná data. Při ochraně dat můžeme využít off-line šifrování vybraných souborů, on-line šifrování všech souborů nebo šifrovaný disk.

Off-line šifrování vybraných souborů se provádí pomocí speciálního programu nainstalovaného do systému. Pomocí programu uživatel může vybrat data, která chce zašifrovat.

On-line šifrování všech souborů je podobné off-line šifrování s tím rozdílem, že program je nainstalován do operačního systému. Šifrovány jsou soubory, které splňují určité podmínky, jako např. jsou to všechny soubory odesílány elektronickou poštou nebo soubory uložené ve speciální složce. Při on-line šifrování si uživatel musí zvolit heslo, které bude při šifrování vyžadováno [4].



Obrázek 1: „Ochrana uložených dat: offline šifrování, online šifrování“[4].

Při použití ***šifrovaného disku*** musí mít uživatel v operačním systému nainstalován ovladač, který bude šifrovat všechna data přenášená na disk. Uživatel také bude muset zvolit vhodné heslo.

2.5 Ochrana přenášených dat

Data mohou být přenášena na elektronických médiích, papírových mediích a počítačovou sítí. Nejvíce jsou ohrožena data, která jsou přenášena přes počítačovou síť. Tato data by se měla hlavně chránit před modifikací a kompromitací.

Proti modifikaci dat můžeme použít digitální otisk (hash). Digitální otisk je založen na kontrolním součtu. Porovnávají se kontrolní součty dat před jejich odesláním a dat přijatých příjemcem. Pokud se shodují, tak data při přenosu počítačovou sítí nebyla modifikována. Digitální otisk může být, ale také napaden. Problém vzniká při přenosu digitálního otisku. Jedno z možných řešení je použití digitálního podpisu.

Proti kompromitaci můžeme soubory zašifrovat ještě před odesláním nebo musí být použit dostatečně bezpečný protokol, který data nejen zašifruje, ale zajistí také jejich integritu.

2.6 Auditní záznam

„Hlavní úlohou auditního záznamu (auditní log) je uchování informace o všech z bezpečnostního hlediska zajímavých událostech, ke kterým v informačním systému

docházelo [7].“Auditní záznamy vytváří nejen operační systém, ale i například firewall či web server.

2.6.1 Obsah auditního záznamu

Auditní záznamy nám slouží k tomu, abychom věděli, co se v systému odehrálo. Každý auditní záznam by měl obsahovat čas události, název programu, který danou událost provedl a podrobný popis důvodu, který vedl k dané události. Zaznamenávají se například úspěšné a neúspěšné přihlašování uživatelů, neoprávněné pokusy o změny souborů atd. [7].

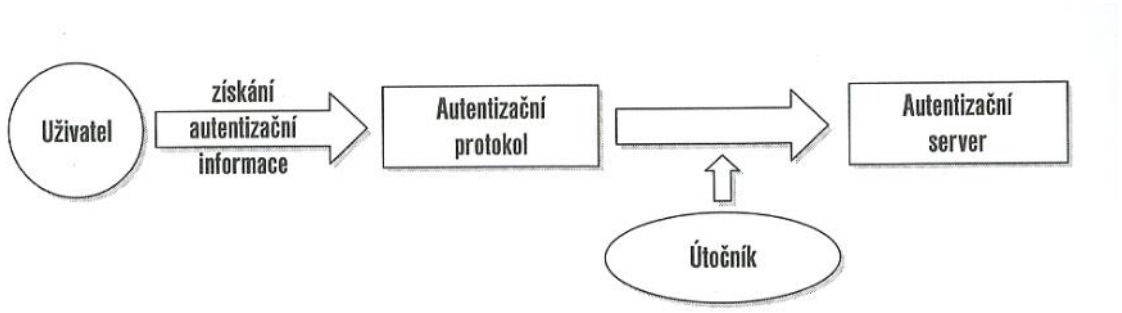
2.6.2 Analýza auditního záznamu

Auditní záznamy by se měly kontrolovat pravidelně a ne až ve chvíli kdy dojde k porušení bezpečnosti. V dnešní době už se auditní záznamy nekontrolují ručně, ale používají se speciální programy. Tyto programy poskytují záznamy ve strukturované podobě, dokáží i rozdělit a zvýraznit položky auditního záznamu, kterým by se měla věnovat větší pozornost. Pro správce systému existují programy, které mu umožňují sjednotit záznamy z více programů a dát záznamy do souvislostí.

Existují také expertní systémy, které umí provést analýzu auditního záznamu skoro automaticky. Tyto systémy obsahují databázi pravidel a logických sekvencí, kterou je potřeba pravidelně aktualizovat. Podle databáze pak probíhá analýza auditních záznamů. Expertní systémy však nemohou plně nahradit správce systému [7].

3 Autentizace

„Autentizace je ověření identity uživatele nebo entity systému, většinou za účelem řízení přístupu ke zdrojům a objektům v systému [4].“ První krok při autentizaci je registrace uživatele v databázi, kde jsou mu nastaveny jeho práva a přiřazena autentizační informace. V druhém kroku uživatel předkládá autentizační informace, které předepisuje autentizační protokol. Získat autentizační informace od uživatele lze pomocí autentizace znalostí, vlastnictví a vlastností. V posledním kroku systém rozhodne, zda povolí nebo zamítne přístup [4].



Obrázek 2: „Schéma činnosti autentizačního protokolu“[4].

3.1 Zisk autentizační informace

Jak uvádí Pavel Šenovský [6] můžeme autentizační informace získat pomocí autentizace znalostí, autentizace vlastností, autentizace vlastnictvím.

3.1.1 Autentizace znalostí

Získání autentizační informace od uživatele probíhá pomocí klávesnice, kdy uživatel zadá např. heslo, PIN, fráze, kombinaci uživatelského jména a hesla. Autentizace pomocí znalostí je zatím nejrozšířenější metodou získávání autentizačních informací.

Nevýhodou této metody je malá bezpečnost. Zadané heslo může být odpozorováno například pomocí kamer, analýzy stisknutých kláves atd. Uživatel by měl také volit vhodná hesla. Hesla by měla být složitá, aby se nedala snadno odhalit (není vhodné volit jména z rodiny, data narození, atd.)a po určitých intervalech by se měla měnit.

Pokud dojde při útoku hrubou silou na heslo, musíme uvažovat, jaká je velikost prostoru, který musí být prohledán. Velikost tohoto prostoru získáme pomocí vzorce:

$$k = p^m$$

Kde k je počet pokusů útočníka, p je počet písmen v abecedě, m je počet znaků hesla.

Uživatelé si často vybírají hesla taková, aby si je snadněji zapamatovali, většinou jsou to slova, která často používají. Pokud útočník zjistí pravidlo, podle kterého si uživatel hesla volí, omezí se mu tak prostor k prolomení hesla [6].

3.1.2 Autentizace vlastnictvím

Dále může být získána autentizační informace pomocí tokenů. Při této autentizaci uživatel musí předložit určité zařízení, které vlastní např. platební kartu, USB token. Při autentizaci se předmět vkládá do čtečky, která získá z předmětu potřebné informace. Uživatel musí neustále mít daný předmět u sebe. Nevýhodou autentizace vlastnictvím je, že pokud dojde ke ztrátě předmětu, může se do systému dostat nálezce předmětu. Proto je vhodné kombinovat autentizaci vlastnictvím například s autentizací znalostí. Uživatel si tedy vloží předmět do čtecího zařízení a zadá k tomu příslušné heslo [6].

3.1.3 Autentizace vlastností

Poslední metodou je autentizace pomocí vlastností, která ověřuje identitu uživatele pomocí biometrických údajů, jako jsou například otisky prstů, oční duhovka, rysy obličeje. Autentizace pomocí biometrických údajů by měla být jednoduchá a rychlá.

Nejčastěji se používají otisky prstů. Autentizace probíhá tak, že je uživateli sejmut otisk prstu a ten se pomocí speciálního softwaru vyhodnotí. Software vyhledá výrazné prvky, které identifikují daného uživatele. Výhody otisků prstů jsou: levné, malé senzory, jednoduché zavedení. Mezi nevýhody patří, že někteří uživatelé nemají dost identifikačních znaků (např. následek úrazu, genetické dispozice).

Dále může probíhat autentizace pomocí žíly na dlani. Při autentizaci se využívá infračerveného spektra. Výhodou je, že žíly na ruce se za celý život nezmění, metoda je bezkontaktní a žíly na ruce je velmi obtížné napodobit.

Využívá se také oční duhovky. Při této metodě se porovnávají takzvané markanty. Výhodou je přesnost. Nevýhodou je, že po dobu snímání sítnice musí stát nehybně.

Autentizace může probíhat také pomocí oční sítnice. „ Sken využívá světelného zdroje o nízké intenzitě, který je projektován na oční sítnici a odraz je ukládán“. Nevýhodou je, že proces trvá 10-15 sekund a uživatel se musí po tuto dobu dívat nehybně do daného bodu [6].

Tabulka 1: „Chybovost“[6].

Chybovost	
oční sítnice	1:10 000 000
oční duhovka	1: 100 000
otisk prstu	1:500

3.2 Útoky na autentizační protokoly

Autentizační protokoly je třeba testovat, aby se odhalilo, jaké útoky lze na ně využít. Na autentizační protokoly lze provést útok opakováním, útok ze středu, útok na hesla, útok na integritu zpráv [4].

3.2.1 Útok opakováním

Při útoku opakováním dochází k odposlouchání komunikace dvou autentizujících stran. Odposlechnutá data (např. zpráva s heslem, celá komunikace) jsou později využita k autentizaci útočníka. Útoku opakováním lze zabránit časovým razítkováním nebo metodou výzva odpověď. Tento útok je snadno realizovatelný, ale těžko odhalitelný.

3.2.2 Útok ze středu

Při útoku ze středu dochází stejně jako při útoku opakováním, k odposlouchání komunikace dvou autentizujících stran. Odposlechnutá data útočník využívá ke spojení s oběma stranami. Obě strany tedy komunikují, aniž by věděly, že jejich zprávy druhé straně jsou upravovány útočníkem.

3.2.3 Útok na integritu zpráv

Tento útok je spojen s nesprávným návrhem autentizačního protokolu. Protokol může řešit neobvyklé situace, které mohou nastat, například špatné zašifrování. Ale nemusí již řešit, zda pole pro zprávu přesahuje danou velikost. V takovémto případě není jasné, jak se bude protokol chovat.

3.2.4 Útok na hesla

Při tomto útoku je uživateli odcizeno heslo. Heslo může být odcizeno například z centrální databáze nebo může být odposlechnuto, když je přenášeno přes počítačovou síť. Heslo může být odcizeno také pomocí slovníkového útoku nebo útoku hrubou silou. Uživatelé se mohou proti útoku na hesla chránit například tím, že nastaví na svém počítači možný počet neúspěšných pokusů o přihlášení [4].

4 Řízení přístupu

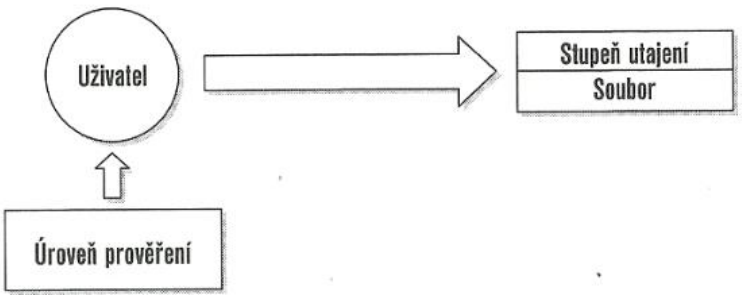
„Řízení přístupu je ochrana informačních zdrojů nebo služeb před přístupem nebo využíváním ze strany nepovolaných entit (organizací, lidí, strojů, procesů). Můžeme tedy říci, že řízení přístupu zabraňuje neautorizovanému využívání určitého zdroje (tzn. tato služba kontroluje a určuje, kdo má přístup k jakým zdrojům, za jakých podmínek k nim může přistupovat a jakým způsobem je může využívat)[8].“Každá entita, která se snaží získat přístup do systému, musí být nejdříve autentizována. Díky autentizaci jsou entitě přidělena přístupová práva.

Nejčastěji se pro řízení přístupu používají seznamy pro řízení pravidel (ACL). Acces control list určuje, jaké entity mají povolení k přístupu k objektu a jaké operace s nimi může provádět. Pokud je systém požádán o provedení operace, tak nejdříve najde v ACL záznam a podle záznamu rozhodne, jestli operace může být provedena. Při použití Acces control list, jsou použity dva seznamy, jeden se využívá pro výstup a druhý pro vstup [8].

Podle Jana Tichého [9] definujeme tři nejpoužívanější modely řízení přístupu: povinné řízení přístupu, nepovinné řízení přístupu a řízení přístupu založené na rolích.

4.1 Povinné řízení přístupu

Povinné řízení přístupu – Mandaroty Access Control – MAC s tímto přístupem se uživatelé téměř nesetkají. MAC klasifikuje objekty a uživatele systému v hierarchických úrovních. Hlavním úkolem hierarchie je, aby objekty, kterým je přiřazen vyšší stupeň, se nedostaly na nižší úroveň. Změny jednotlivých úrovní mohou měnit pouze administrátoři. Každý uživatel může číst pouze objekty ze stejné nebo nižší úrovně, zapisovat může do stejné nebo vyšší úrovně. Každý objekt má nastavenou svoji úroveň [9].



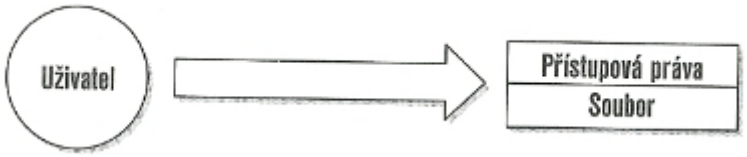
Obrázek 3: „Povinné řízení přístupu“[4].

4.2 Řízení přístupu založené na rolích

Řízení přístupu je založené na rolích uživatele, které mu přidělí administrátor. Administrátor musí správně klasifikovat, jaké potřeby budou jednotlivé role mít a jak velkou náročnost budu klást na zdroje. Administrátor by měl uživatelům přidělit jen takové oprávnění, které doopravdy potřebují. Každá role má svůj profil, ve kterém jsou uvedeny například příkazy, přístupy k informacím. Role jsou uživatelům přidávány buď staticky nebo dynamicky na základě podmínek či událostí [9].

4.3 Nepovinné řízení přístupu

Nepovinné řízení přístupu – Discretionary Access Control – DAC je využívané nejčastěji. Každému uživateli jsou přiřazována přístupová práva k daným objektům. Systém kontroluje požadavky uživatelů na přístup k objektům a na základě specifikovaného povolení je přístup povolen nebo zamítnut. Při nepovinném řízení přístupu může existovat několik super uživatelů (mají jistá omezení), ale jen jeden administrátor. Největší rozdíl od povinného řízení přístupu je v tom, že každý uživatel může u objektů, které vytvoří nastavit přístup ostatním uživatelům a může tyto objekty předávat [9].



Obrázek 4: „Nepovinné řízení přístupu“[4].

5 Šifrování a elektronický podpis

5.1 Kryptologie

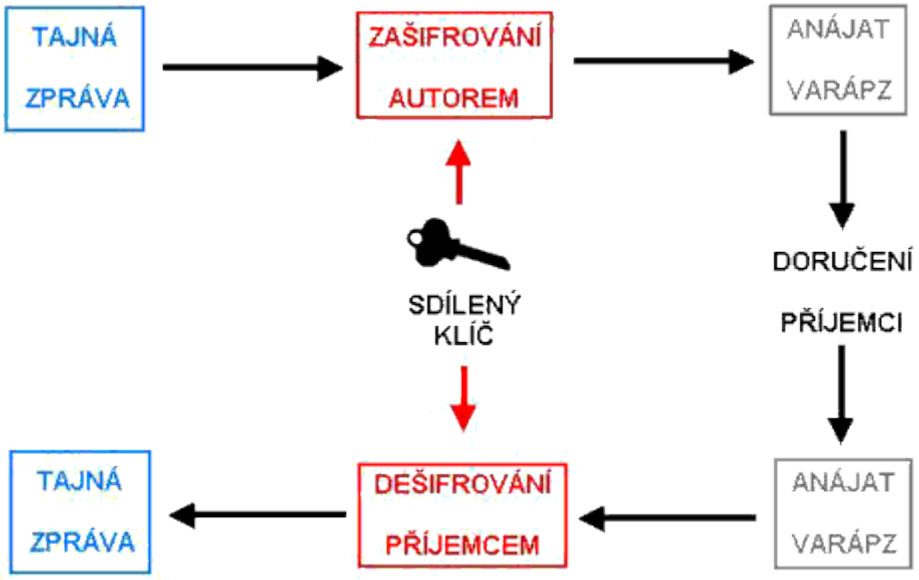
Kryptologie se zabývá ochranou dat před jejich zneužitím. Dělíme ji na dvě části kryptografie a kryptoanalýza. Kryptografie se zabývá kódováním a dekódováním dat. Kryptoanalýza analyzuje algoritmy a zašifrovaná dat.

Data, která jsou v obvyklé podobě, nazýváme jako otevřený text. Přepis otevřeného textu na šifrovací text nazýváme šifrování, opačný proces nazýváme dešifrování.

Při komunikaci vystupují dvě osoby takzvané Alice a Bob. Pokud mají Alice i Bob společný klíč jedná se o symetrické šifrování. Společný klíč je používám jak pro šifrování tak i dešifrování. Pokud má každý z účastníků komunikace dva klíče, které se označují, jako klíčový pár, nazýváme šifrování asymetrické. Jeden klíč je soukromý a používá se pro dešifrování přijatých zpráv. Druhý klíč je veřejný, je přístupný všem. Pomocí něj můžeme šifrovat data, která se odesílají vlastníkovi soukromého klíče [10].

5.1.1 Symetrická kryptografie

Symetrická kryptografie využívá pouze jednoho klíče, který je stejný pro obě strany. Klíč slouží jak k šifrování tak i dešifrování. Symetrické šifrování je rychlejší než asymetrické. Nevýhoda spočívá ve vyšším počtu klíčů a jejich správě. Při tvorbě symetrických algoritmů se využívá substituční a transpoziční metody. Substituční metoda je předpis, který mění znaky na základě substituční tabulky. Transpoziční metoda na rozdíl od substituční využívá změnu pořadí znaků.



Obrázek 5: „Symetrické šifrování [22]“.

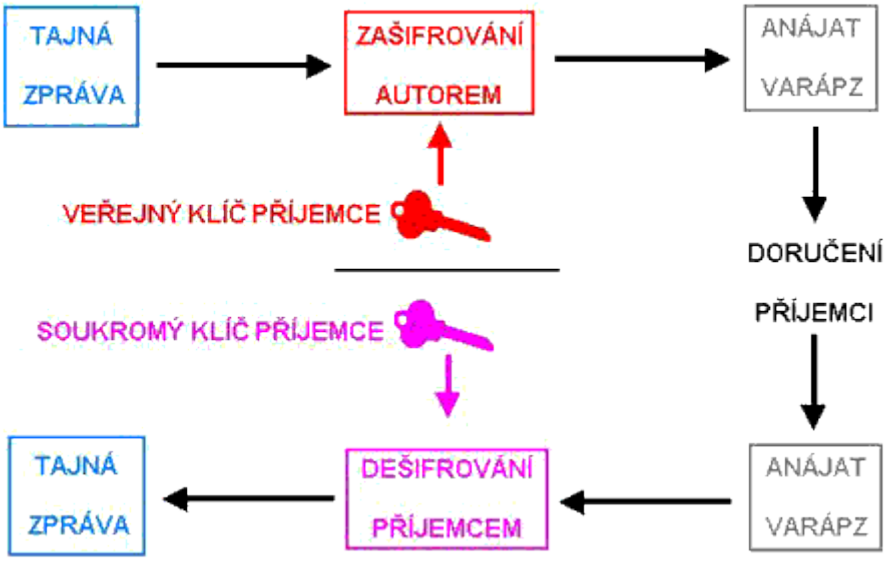
Příklady symetrických šifer

Jako příklad substituční šifry můžeme uvést monoalfabetickou substituční šifru. Pro tuto šifru je důležitá šifrovací tabulka, která slouží pro převod otevřeného textu na šifrovaný text a naopak. Nevýhodou této šifry je nedostatečná odolnost vůči frekvenční analýze. Při dlouhém textu dokáže analýza odhalit, jaké znaky byly za které nahrazovány. Například v angličtině se nejčastěji vyskytuje písmeno E, když v šifrovaném textu nalezneme nejčastěji vyskytovaný znak, bude to nejspíše tedy znak E.

Šifra DES je kombinací substituční a transpoziční šifry. Na otevřený text je aplikována substituce a následně transpozice, a to se opakuje šestnáctkrát. Je to bloková šifra, pracuje s bloky délky 64 bitů a klíčem stejné délky, 8 bitů z klíče je paritních (slouží pro zabezpečení), efektivně využívaná délka klíče je tedy 56 bitů.

5.1.2 Asymetrická kryptografie

Asymetrická kryptografie využívá na rozdíl od symetrické dvou klíčů, tedy každý člověk má dva klíče. Tyto dva klíče jsou spolu svázané. Text zašifrovaný jedním klíčem ze dvojice lze dešifrovat pouze druhým klíčem z dané dvojice. Text zašifrovaný daným klíčem, nejde stejným klíčem dešifrovat. Ale je jedno, zda klíč se použije k šifrování nebo dešifrování. Jeden z těchto klíčů se nazývá soukromý a druhý veřejný.



Obrázek 6: „Asymetrické šifrování [22]“.

Příklady asymetrických šifer

RSA se využívá pro šifrování nebo elektronický podpis. Tato šifra je založena na faktorizaci velkých prvočísel.

ECC je algoritmus zaměřený na řešení úlohy diskrétního logaritmu v grupách na eliptických křivkách. ECC je oproti RSA bezpečnější i při použití kratšího klíče [10].

5.2 Elektronický podpis

„Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě [12]“.

Elektronický podpis se používá pro podepisování dokumentu libovolného obsahu a libovolné délky. Elektronický podpis by měl plnit následující funkce: identifikace, autentizace, integrita, nepopiratelnost.

- ***Identifikace*** – lze jednoznačně určit, kdo dokument podepsal
- ***Autentizace*** - lze zjistit, kdo je autorem daného dokumentu
- ***Integrita*** – znamená, že od vytvoření elektronického podpisu nebyl podepsaný dokument změněn či poškozen

- ***Nepopiratelnost*** – autor podepsaného dokumentu nemůže popřít, že dokument nevytvořil

5.2.1 Asymetrická kryptografie a elektronický podpis

Pro elektronický podpis se využívá kryptovací asymetrické algoritmy, nejčastěji RSA a DSA.

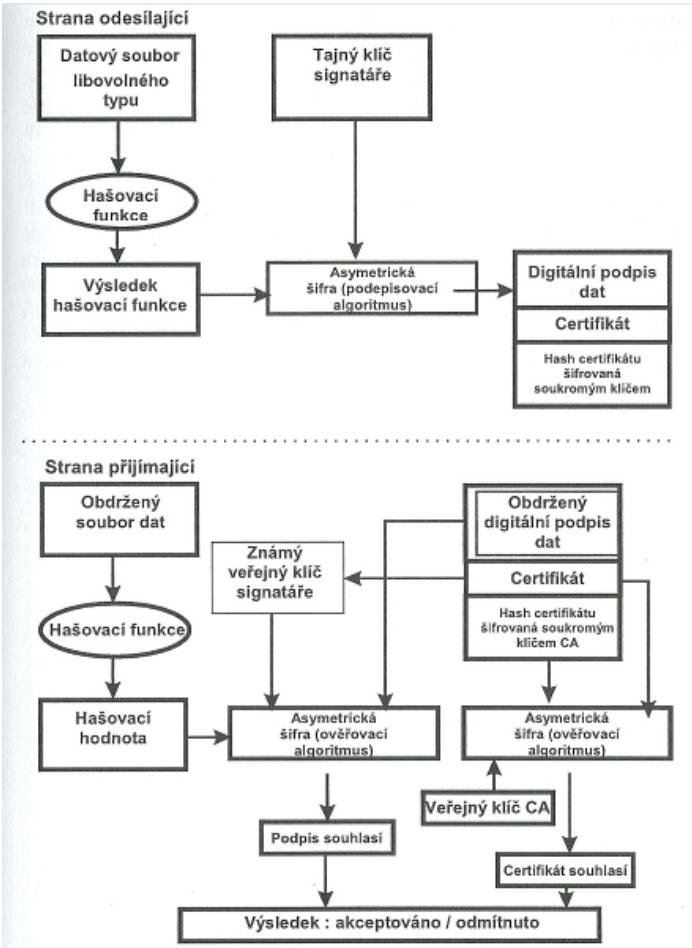
Postup při podepisování a ověřování dokumentu je následující. Zprávu, kterou chceme podepsat, necháme projít přes hashovací funkci pomocí, které získáme zkrácený otisk zprávy. Ke zkrácenému otisku připojíme pomocí soukromého klíče elektronický podpis. Zprávu odešleme příjemci. Příjemce, který zná veřejný klíč, si může zkontrolovat pravost elektronického podpisu. Pokud příjemce zjistí, že je ověření podpisu v pořádku tak si může být jistý, že po umístění elektronického podpisu nedošlo ke změně přijaté zprávy [10].

5.2.2 Hashovací funkce

Nevýhodou asymetrické kryptografie je její rychlost. Podepisování velkých zprávy by při jejím použitím trvalo příliš dlouho. Při elektronickém podepisování dokumentů se proto používá hashovací funkce.

Hashovací funkce je jednosměrná matematická funkce. Vstup této funkce je otevřený text a výstupem je jeho otisk o dané velikosti. Hashovací funkce musí splňovat určité požadavky – výstup má přesně danou délku, rozdílné vstupy nemají stejné výstupy, při znalosti výstupu nelze dopočítat vstup.

Při elektronickém podpisu se nejčastěji využívají hashovací funkce MD5 a SHA-1. Funkce MD5 má výstup o délce 128 bitů a funkce SHA-1 má výstup o délce 160 bitů [10].



Obrázek 7: „Schéma tvorby a ověření elektronického podpisu“[10].

5.2.3 Certifikovaný klíč

Nebezpečí při elektronickém podpisu je, že může být odcizena databáze veřejných klíčů. A pak tedy osoba, která klíče odcizila, může zneužít elektronického podpisu pomocí těchto klíčů. Řešením jsou certifikace veřejných klíčů. Certifikát, je dokument, který vydává certifikační autorita, která stvrdí, že daný veřejný klíč patří konkrétní osobě. Certifikát je připojen k vlastnímu podpisu. Příjemce dokumentu ověří podpis v certifikátu, když je vše v pořádku. Dále ověří údaje odesílatele uvedené v certifikátu. Pokud je i tady vše v pořádku, může pomocí veřejného klíče ověřit podpis vlastní zprávy.

Certifikační autorita je při komunikaci dvou stran důvěryhodná třetí strana. Certifikační autorita vydává certifikáty, které spojují podepsanou osobu s jejím elektronickým podpisem. Certifikát obsahuje údaje o subjektu a veřejný klíč subjektu [10].

Tabulka 2: „Obsah certifikátu“[4].

Obsah certifikátu veřejného klíče	
Položka	**Popis**
ID certifikátu	Jednoznačné sériové číslo
Datum vydání	Kdy byl certifikát vydán
Platnost do	Časové omezení platnosti
Omezení certifikátu	Účel, pro který lze certifikát použít (např. podepisování)
ID certifikační autority	Kdo certifikát vydal
Algoritmy CA	Jaké algoritmy používá pro podepisování certifikační autorita
Veřejný klíč CA	Nemusí být součástí certifikátu
ID vlastníka	Rodné číslo či IČO
Veřejný klíč vlastníka	Vlastní certifikovaný klíč
Podpis	Předchozí data jsou podepsána soukromým klíčem CA

5.2.4 Druhy elektronického podpisu

Jak uvádí Jiří Peterka [13], rozlišujeme dva druhy elektronických podpisů: uznávaný a zaručený elektronický podpis.

Uznávaný elektronický podpis má pro úřady stejnou váhu jako vlastnoruční podpis, a jak plyne z názvu, musí ho uznávat. Uznávaný elektronický podpis je založen na kvalifikovaném certifikátu, vydaném akreditovanou certifikační autoritou. Kvalifikovaný certifikát se může vydat jen osobě, u níž byla ověřena její totožnost.

Na rozdíl od uznávaného elektronického podpisu, zaručený elektronický podpis už úřady nemusí akceptovat. U zaručeného elektronického podpisu je zajištěna jeho integrita, tedy že se od podepsání dokument nezměnil. Není už ale zjistitelné, komu podpis patří, údaje o podepsané osobě nemusí být pravdivé. Zaručený elektronický podpis nemusí být založen na základě kvalifikovaného certifikátu [13].

6 Normy

Pro bezpečnou komunikaci je zapotřebí používat normy. Normy vydávají národní i mezinárodní agentury a stanovují tak standardy informačních systémů. V České republice se vydáváním norem zabývá Český normalizační institut (ČNI), jehož normy se označují ČSN. Normy můžeme rozdělit do následujících skupin: národní (definované a uznaná daným národním úřadem), mezinárodní (uznávané mezinárodně), oborové (definovány oborovou organizací), de facto standardy (vytvořené odborníky a publikovány na internetu) [14].

Tabulka 3: Přehled norem

Název normy	Zkratka	Zařazení normy
International Organisation for Standardisation	ISO	Mezinárodní
International Electrotechnical Commision	IEC	Mezinárodní
Mezinárodní telekomunikační unie	ITU	Mezinárodní
American National Standars	ANSI	Národní (USA)
Deutsche Institut Normung	DIN	Národní (Německo)
Internet Engineering Task Force	IETF	Oborové
Institu of Electrical and Electronic Engineers	IEEE	Oborové

De facto standart je standart, který vytváří sám výrobce a jiní výrobci tento standart dobrovolně použijí i ve své organizaci. Výrobci sami nemohou vydávat oficiální normy. Může, ale nastat situace kdy výrobce vytvoří vlastní řešení, které se následně stane de facto standardem, a nakonec ho agentury stanovující standardy informačních systémů převezmou. Například koncepce sítí Ethernet vytvořila firma Xerox, následně se koncepce sítí Ethernet stala standardem de facto a po malých úpravách dokonce oficiální normou (IEEE 802.3) [15].

7 Útočníci

„Útočník či narušitel je osoba, která získá, případně se snaží získat větší než přidělená práva nebo neoprávněný přístup k informačnímu systému [8].“ Útočníky můžeme dělit z hlediska polohy útočníka, odbornosti a cíle útoku [8].

Z hlediska polohy útočníka existují dva typy útočníků Insider a Outsider.

Insider je útočník, který se připojuje do počítačové sítě zevnitř. Insider je tedy oprávněný uživatel, který se snaží o neautorizovaný přístup nebo se snaží o zneužití jemu přístupných dat.

Ousider je útočník, který nemá oprávněný přístup do sítě. Do sítě se snaží proniknout využitím bezpečnostních chyb a různých nedostatků.

Z hlediska odbornosti útočníka existují dva typy útočníků amatéři a profesionálové.

Amatéři mají nižší úroveň znalostí, nedostatečné vybavení a tak provádí útoky méně nebezpečné. Amatéři například zkouší proniknout do systému pomocí již na internetu popsané bezpečnostní chyby.

Profesionálové mají vysokou úroveň znalostí a dostatečné vybavení, jsou schopni provádět velice nebezpečné útoky.

Z hlediska cíle útoku existují dva typy útočníků hacker a cracker.

Hacker.„Jedná se o člověka, který využívá své draze nabyté odborné znalosti ku prospěchu celku.“. Hacker není člověk, který má krást či zničit data. Hackeři mají pro své chování pravidla.

Cracker, „podle jedné z definic se jedná o člověka, který obchází protipirátské ochrany počítačových programů. Dokáže z nich získat sériové číslo, případě program upravit tak, aby zadání tohoto čísla (nebo jiný druh ochrany) nevyžadoval.“ Crackeři jsou často nazýváni hackary [8].

7.1 Útoky

„Útok je úspěšný nebo neúspěšný pokus o narušení bezpečnosti informačního systému [1].“ Jak uvádí Eliška Odchodková [16] máme tyto formy útoků:

Přerušení – patří mezi aktivní útoky na dostupnost dat (např. ztráta, vymazání, poškození dat).

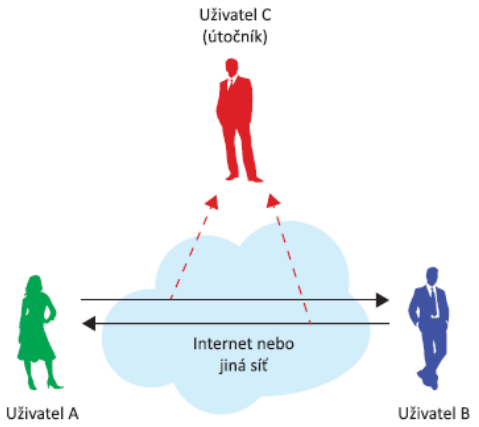
Odposlech – patří mezi pasivní útoky na důvěrnost, neoprávněný přístup k datům (např. odposlech přenášených dat počítačovou sítí, kopírování programu či dat).

Modifikace – patří mezi aktivní útoky na integritu dat, neoprávněná změna dat (např. změna přenášených či uložených dat).

Přidání hodnoty – patří mezi aktivní útok na integritu dat nebo na autenticitu (např. podvržení dat)[16].

Útoky můžeme dělit na aktivní a pasivní.

Při ***pasivním útoku*** jde o získání nebo využití informace. Při pasivní útoku dochází buď k odposlouchávání, nebo k analýze provozu. K odposlouchávání dochází při komunikaci, ve které jsou přenášena nezašifrované zprávy. Odposlechu lze zabránit, pokud je použito šifrování přenášených zpráv. Při analýze provozu se zachycují a zkoumají přenášené zprávy. Zachycení a zkoumání přenášené zprávy je možno provádět, i pokud jsou zprávy zašifrované[16].

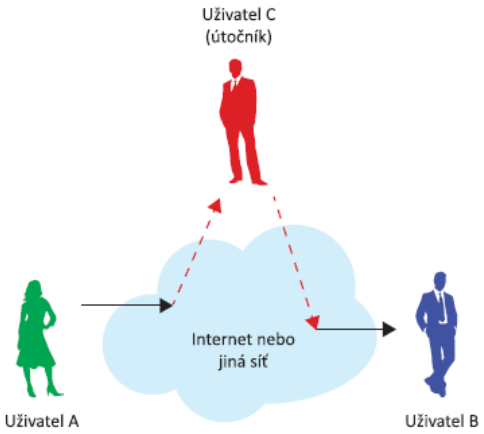


Obrázek 8: „Model pasivního útoku“[8].

Při ***aktivním útoku*** jde o změnu systémových prostředků nebo o ovlivnění jejich provozu. Při útoku útočník změní, odstraní či přidá data.

Útočník může změnit data například tak, že změní číslo účtu. Pro odhalení tohoto útoku se může použít kontrolního součtu nebo digitálního podpisu.

Při aktivním útoku se útočník může pokusit ukrást identitu tím, že získá autentizační informace nebo převezme vzniklou autentizovanou komunikační relaci. Aby k tomuto útoku nedocházelo, je vhodné použít protokoly, které zabraňují krádeži identity. Útočník může také zničit přenášená data [16].



Obrázek 9: „Aktivní útok s pozměněním zpráv“[8].

Útoky lze dělit také podle jejich cíle:

Útok na hardware může nastat při útoku přerušením (např. odcizení, zničení, přírodní havárie), odposlechem (např. krádež místa v paměti), přidáním hodnoty.

Útok na software může nastat při útoku přerušením, kde rozlišujeme útoky úmyslné (např. úmyslné smazání programu) a neúmyslné (např. neúmyslní smazání programu), odposlechem (např. kopírování programu), přidáním hodnoty (infiltrace programů).

Útok na data může nastat při útoku přerušením (např. poškození dat), odposlechem (např. odposlech dat přenášených počítačovou sítí), změnou (např. změna přenášených dat) a přidáním hodnoty [16].

8 Infiltrace

„Počítačová infiltrace je jakýkoliv neoprávněný vstup do počítačového systému, a tím i do jeho dat (dokumenty, programy, atd.).“ Uživatelé počítačů často používají pojem virus pro jakoukoliv počítačovou infiltraci [17].

„Počítačový ***vir*** je program, který může infikovat jiný počítačový program takovým způsobem, že do něj zkopíruje své tělo, čímž se infikovaný program stává prostředkem pro další aktivaci viru.“ Autorem této definice je jeden z antivirových průkopníků Fred B. Cohen [18].

Červy se šíří pomocí počítačových sítí. Červy buď využívají síťových služeb, nebo využívají aplikační programy (např. emailové klienty). Červy se šíří pomocí síťových paketů. Síťový paket je odesílán z již infikovaného systému pomocí sítě do jiného systému, je to buď náhodné, nebo podle pravidla či klíče. Využívají bezpečnostních děr operačního systému pomocí, kterých se do systému dostanou. Systém mohou infikovat nebo využít k dalšímu šíření. Pro antivirový program je pak téměř nemožné detekovat červa. Červy můžeme dělit na: souborové (pro své šíření vytvářejí soubory v systémových adresářích), IRC (využívají vlastností IRC, posílají data ve spustitelných souborech), skriptové červy [19].

Trojské koně se liší od virů a červů tím, že nejsou schopny samy své replikace. Nejčastěji se šíří pomocí spustitelných souborů.EXE. Trojské koně se vydávají za užitečné programy, které jako vedlejší činnost ničí data nebo provádějí jinou škodlivou činnost. Trojské koně nejsou v dnešní době tak rozšířené jako viry a červy [19].

Zadní vrátka („backdoor“) jsou druh trojských koní. V počítači se uloží a začnou provádět škodlivou činnost, až když se k počítači připojí útočník a začne s ním komunikovat. Pomocí zadních vrátek může útočník modifikovat či zničit data. Zadní vrátka mají dvě části klientskou a serverovou. Serverová část je ta část, která je uložená v infikovaném počítači. Pomocí klientské se útočník připojuje k serverové části a ovládá počítač [17].

DoS jsou útoky typu odmítnutí služby. Tyto útoky zabraňují přístupu uživatele k nějaké službě v počítači nebo síti. DoS útoky můžeme rozdělit na lokální a vzdálené. Při lokální útoku potřebuje útočník přístup k počítači, na který se chystá zaútočit, při vzdáleném útoku ne. Příkladem DoS útoku je obsazení přenosové kapacity větším

množstvím požadavků, přivlastnění systémových zdrojů atd. Útočník při útoku DoS nemůže modifikovat ani mazat data [17].

Bot je program, který umožňuje útočníkovi pomocí vzdáleného přístupu ovládat systém. Počítačům, které jsou napadeny programem Bot, se říká „zommbie“, můžou sloužit například k rozesílání spamu [17].

Jako ***Hoax*** je označována poplašná zpráva. Tyto zprávy mohou obsahovat varování před neexistujícími viry, různé nabídky produktů či služeb za nízkou cenu nebo také šíření emailů, kterými například můžete získat štěstí. Hoax šíří uživatelé, kteří email dostanou a přeposílají ho dál. Mezi typické znaky hoaxu patří: oslovení příjemce, odvolávání se na důvěryhodné zdroje, podrobné charakteristiky např. nebezpečí viru a výzva k dalšímu odeslání [20].

Jako ***spyware*** označuje programy, které sbírají informace (např. seznam navštěvovaných stránek) o uživateli a následně je odesílají pomocí internetu. Většinou jsou sbírána statistická data, která slouží k zjištění potřeb a zájmů uživatele. Informace jsou pak využity například pro cílenou reklamu. Nejčastěji se spyware šíří pomocí sharewarových programů [19].

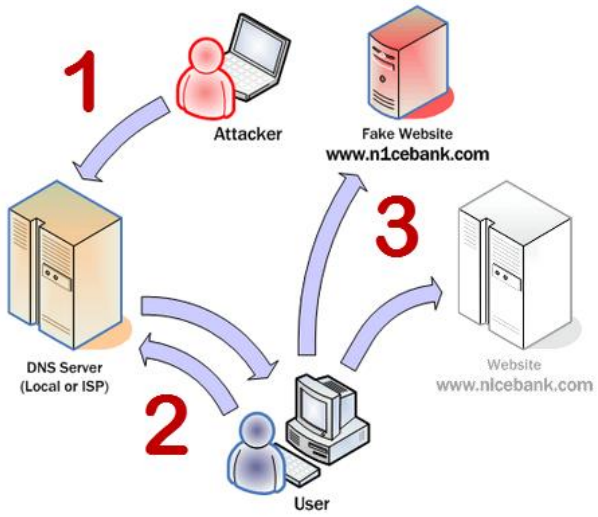
Adware jsou programy, které se instalují většinou společně s různými freewarovými programy. Uživateli pak nabízejí různé reklamy například pomocí vyskakovacích oken. Adware dokáže také sledovat uživatele a může tak překládat cílené reklamy podle zjištěných informací [19].

8.1 Sociální inženýrství

Pomocí sociálního inženýrství útočník manipuluje s lidmi za účelem proniknutí do počítače nebo získání citlivých dat. Jako nejčastější prostředky jsou pro sociální inženýrství využívány emaily, telefony a reklamy.

Pomocí ***Phishingu*** se útočníci snaží za pomoci webových stránek či emailů dostat z uživatelů citlivá data (např. hesla a čísla účtů). Mezi známé phishingové útoky patří email od banky, kde útočníci nabádají k tomu, aby uživatelé klikli na odkaz v emailu, který je přesměruje na falešné stránky banky. Na falešných stránkách je po tom od uživatele požadováno heslo a číslo účtu, pokud uživatel tyto informace vyplní, útočníci pak získají potřebná data, která mohou zneužít [20].

Pharming je velmi podobný phishingu. Jako pharming se považuje, pokud útočníci napadnou DNS server, na kterém přenastaví IP adresy. Tyto IP adresy pak na vyžádání uživatelů jsou rozesílány. Útočník tak uživatele může přesměrovat na falešné stránky, kde z uživatelů vyláká citlivá data. Útočník může také napadnout přímo počítač uživatele. Ve webovém prohlížeči jsou seznamy navštěvovaných IP adres, které útočník přepíše [20].



Obrázek 10:Pharming“[21].

9 Zabezpečení

Následující podkapitoly o firewallu a dělení antivirových programů jsou doslovně převzaty z mé bakalářské práce [23].

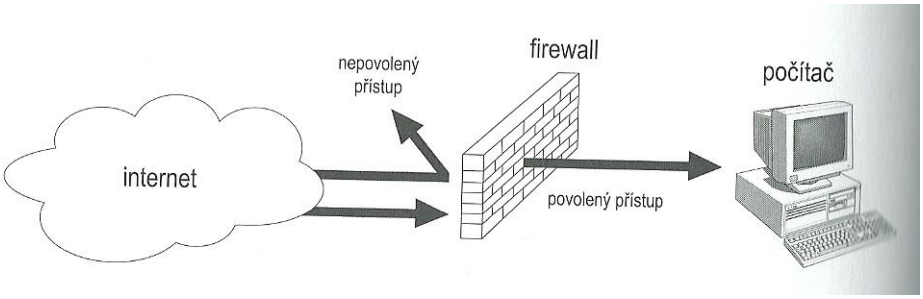
9.1 Firewall

Firewall je buď hardwarové nebo softwarové zařízení, které sleduje provoz počítače, a to ve směru z Internetu do počítače a naopak. Je nainstalován mezi počítačem a Internetem. V domácích sítích se nejčastěji setkáváme se softwarovým firewallem, který je připojen na aktivní síťové rozhraní. To je pak připojené k Internetu, takže přes něj projde každý paket.

Hardwarový firewall je především určen firmám, které využívají pro svou práci Internet. Aby tento firewall správně fungoval, je nutné ho umístit mezi router a venkovní síť. Tím se zajistí ochrana počítačů, které se nacházejí za routerem.

Firewall hlídá přístup do a z vašeho počítače, když se nějaký program pokusí o takový přístup, firewall zobrazí dotaz a nabídne vám tři možnosti:

- Povolit – chcete-li spustit program nebo umožnit přístup, zvolte toto pravidlo
- Zakázat – pokud nechcete spustit nebo umožnit přístup, potom klepněte na toto tlačítko
- Vytvořit pravidlo pro tuto komunikaci a příště se již nedotazovat.



Obrázek 11: Princip práce firewallu.

9.1.1 Rozdělení firewallů

Základní technologie firewallů jsou tři: jednoduchý ip filtr, stavový ip filtr, proxy.

Jednoduchý IP filtr

Tato technologie funguje na základě pravidel, která zakazují provoz na daných portech. Nevýhodou je to, že všechny nezakázané porty jsou povolené. Abychom tedy zamezili veškerému nebezpečí, musíme zakázat mnoho portů. Nevýhodou IP filtru je, že nedokáže vyhodnocovat procházející data.

Stavový IP filtr

Stavový filtr, který je vylepšením IP filtru. Stavový filtr dokáže sledovat provoz v síti. Filtr sleduje hlavně komunikaci protokolů TCP a UDP. Povoluje přenos paketů do internetu, ale opačně povoluje jen pakety, které jsou následkem zevnitř vyvolané relace.

Proxy

Pokročilejší technologií, která slouží při tvorbě firewallů, je aplikační server proxy. „Jedná se o jeden konkrétní protokol, který filtruje pakety podle toho, která aplikace a na kterém portu s nimi pracuje.“ Proxy má oproti IP filtru mnoho výhod, např. vyšší úroveň bezpečnosti, rychlejší konfiguraci.

Demilitarizovaná zóna

Demilitarizovaná zóna je část sítě, která není tak dokonale chráněna jako ostatní části sítě. V této zóně jsou umístěny servery (např. poštovní, webový server). Demilitarizovaná zóna je propojena s firewallem, který do ní pouští jen komunikaci, která je určena serverům, které jsou v ní umístěny např. komunikace na portech poštovního protokolu, port 80.

9.2 Dělení antivirových programů

Antivirové programy se mohou dělit podle různých kritérií. Podle Igora Háka [9] můžeme dělit antivirové programy na jednoúčelové antivirové programy, on-demand skenery, antivirové systémy.

Jednoúčelové antivirové programy

Tyto antivirové programy slouží pro detekci a také dezinfekci daného viru nebo menší skupiny virů. Jednoúčelové antivirové programy neslouží jako stálá antivirová ochrana, jde pouze o jednorázovou ochranu. Tyto programy většinou poskytují antivirové firmy, nabízejí je na svých stránkách většinou zdarma.

On-demand skenery

On-demand skenery se využívají především pro detekci virů, popřípadě dezinfekci počítačů, když operační systém nelze spustit běžným způsobem.

Alternativou jsou internetové on-line skenery, které nabízejí někteří výrobci antivirových programů. Jedná se o skript, který pomocí internetového prohlížeče prohledá váš pevný disk, aniž byste tento antivirus instalovali do svého počítače.

Antivirové systémy

Jedná se o nejčastější používané antivirové programy. Antivirový systém dokáže sledovat všechna místa (např. elektronická pošta, vyměnitelná média), kterými by mohl vir do počítače proniknout. Tyto systémy potřebují aktualizace, aby mohly aktualizovat své virové databáze.

9.3 Antivirový hardware

Antivirový hardware se zaměřuje na vstupy virů do systému. Je schopen na rozdíl od antivirového softwaru chránit počítač již při zavádění systému. Hardwarová ochrana může zabránit zápisu na mechaniky pevných disků, může chránit paměť atd.

Hardwarová ochrana se v dnešní době moc nepoužívá. Uživatelé nechtějí do svých počítačů dávat přídavný hardware a rozšiřuje se používání notebooků, u kterých není tak jednoduché nainstalovat přídavné hardwarové karty [24].

9.4 Antispyware a antispam

Antispyware je program, který slouží k detekci a odstranění spywaru. Antispyware je dnes zahrnut do antivirových systémů. Pracuje stejně jako antivirový program, po připojení počítače do sítě, zajišťuje ochranu a zabraňuje infikování počítače.

Antispam je program, pomocí kterého je odhalen a následně smazán spam. Antispam lze rozdělit pomocí dvou kategorií – aplikace určená pro konkrétního klienta, aplikace určená pro jakéhokoliv klienta. Antispamovému programu můžou uživatelé pomoci rozeznávat spam, pokud nebyly zprávy označeny za spam, může uživatel tyto zprávy sám označit za spam [24].

Praktická část práce

10 Dotazníkový průzkum

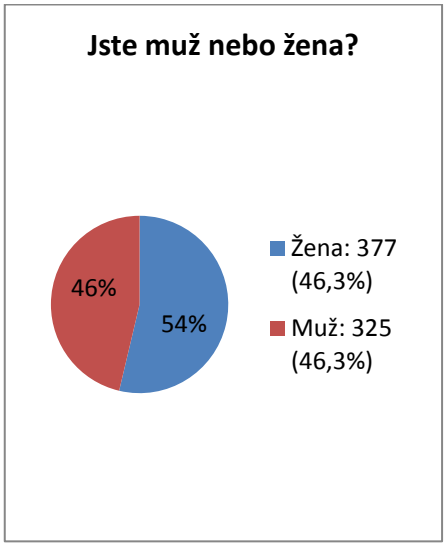
Jedním z cílů praktické části diplomové práce je provést průzkum, kterým bude zjištěno, jak uživatelé chrání svá data. Pro získání informací k průzkumu byla použita dotazníková metoda.

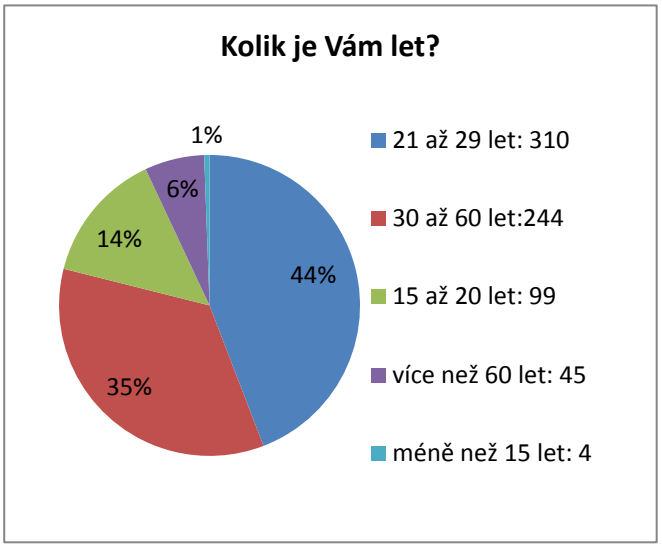
Dotazník byl šířen v elektronické podobě. Byl umístěn na portálu www.vyplnto.cz. Portál vyplnto.cz umožňuje vytvoření on-line dotazníku s možností větvení otázek, propagaci dotazníků, vyhodnocení dotazníků. Dotazníky je možno publikovat jako veřejné, které propaguje portál vyplnto.cz, nebo neveřejné, u kterých si uživatel musí zajistit propagaci sám.

10.1 Vyhodnocení dotazníku

Dotazník obsahuje 24 otázek, z toho je 17 otázek uzavřených, 6 polozavřených a 1 otázku otevřenou, kde respondent doplní krátký text (Příloha A).

Dotazník byl umístěn na webu jeden měsíc a zúčastnilo se ho 702 respondentů. Z toho 325 mužů a 377 žen různého věku.



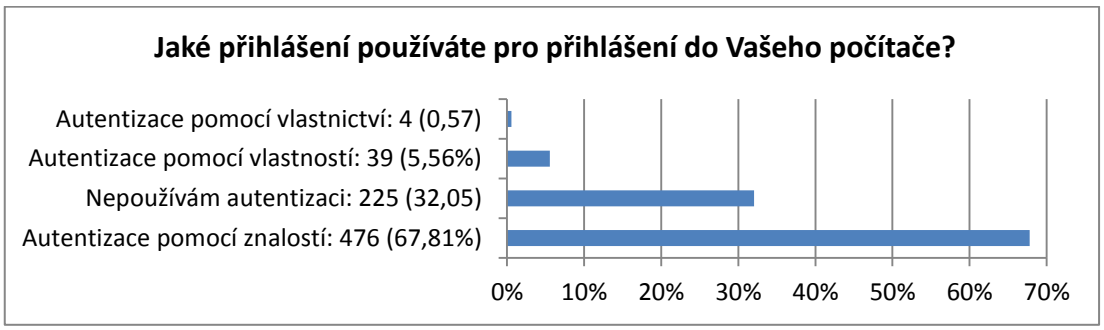


Obrázek 11: Jste muž nebo žena?

Obrázek 12: Kolik je Vám let?

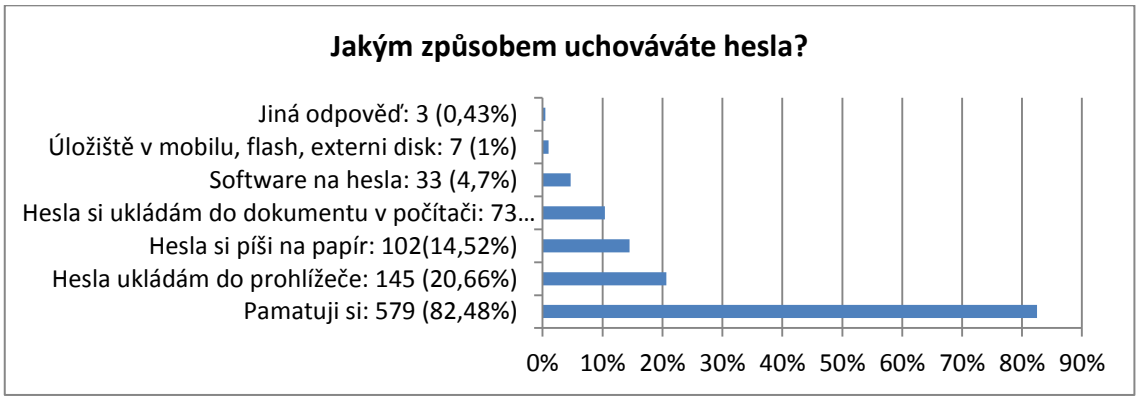
Cílem této otázky bylo zjistit, jak respondenti chrání svůj vlastní počítač při přihlašování. Ukázalo se, že nejvíce respondentů používá pro přihlášení do počítače autentizaci pomocí znalostí (67,81%), dále pak vůbec nepoužívá autentizaci (32,05%),

v nejmenším zastoupení je autentizace pomocí vlastností a vlastnictví. Pokud uživatelé používají kombinace uvedených autentizací, tak využívají nejčastěji kombinaci autentizace pomocí znalostní a vlastností. Většina respondentů pro svůj počítač používá některou z uvedených autentizací, ale 225 respondentů pro vstup do svého počítače žádné přihlašování nepoužívá. Tyto respondenti tedy svá data v počítači nezabezpečují už od samého začátku přihlášení do počítače. Pravděpodobně nepovažují za důležité ochraňovat svá data autentizací při vstupu do počítače.



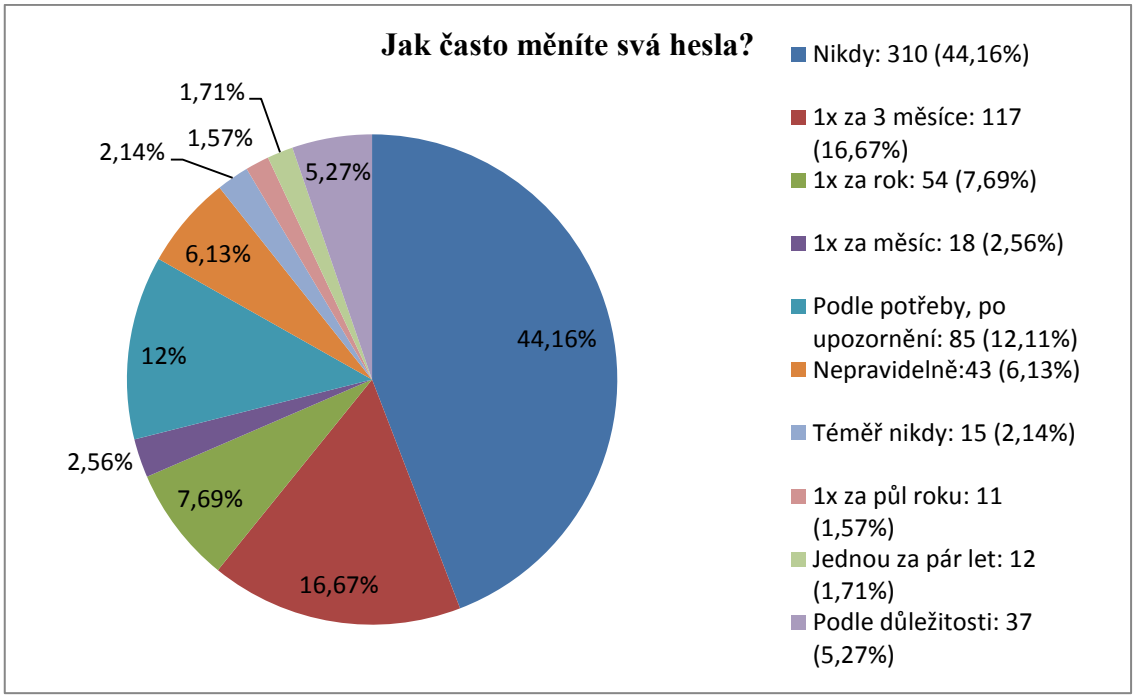
Obrázek 13: Jaké přihlášení používáte pro přihlášení do Vašeho počítače?

Uchovávání hesel je pro bezpečnost uživatelských účtů podstatné. Nejvíce si respondenti svá hesla pamatují (82,48%). Respondenti si svá hesla nejčastěji pamatují, pokud se jedná o jednoduchá hesla nebo jde o hesla, která slouží například pro přístup k bankovnímu účtu. Dále si 20,66% respondentů ukládá svá hesla do prohlížeče. Pokud útočník získá například přístup k počítači nebo využije bezpečnostních děr prohlížeče, může tedy hesla z prohlížeče snadno získat a využít je ke škodlivé činnosti. Respondenti si svá hesla píší také na papír (14,52%) a do dokumentu v počítači. Pro uchovávání hesel taky využívají k tomu určený software 4,7% respondentů, jako jsou například klíčenky. V klíčenkách mají svá hesla uložena a za pomoci hesla nebo speciálního souboru se, ke všem uložených heslům dostanou.



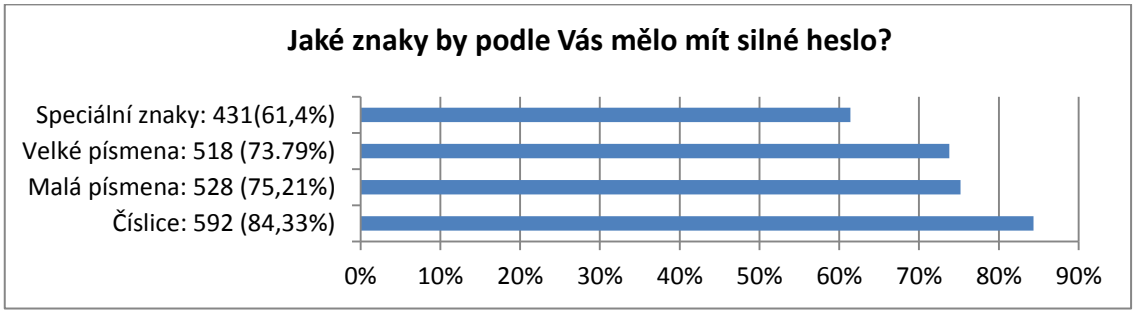
Obrázek 14: Jakým způsobem uchováváte hesla?

Často diskutovanou otázkou je, jestli měnit či neměnit hesla. Někde je po uživatelích vyžadováno měnit heslo po určité době. Někteří se ale domnívají, že je to zbytečné. Protože pokud útočník odhalí heslo, zneužije ho ihned a časté změny hesla mohou vést k tomu, že uživatelé heslo zapomenou. Anebo aby ho nezapomněli, napíšou si ho raději na papír. Nikdy nemění svá hesla 44,16% respondentů, jednou za tři měsíce mění hesla 16,67% respondentů, tato doba je častou dobou exspirací hesla. Podle potřeby mění svá hesla nebo po upozornění mění svá hesla 12,11% respondentů. Ostatní skupiny jsou velmi malé.



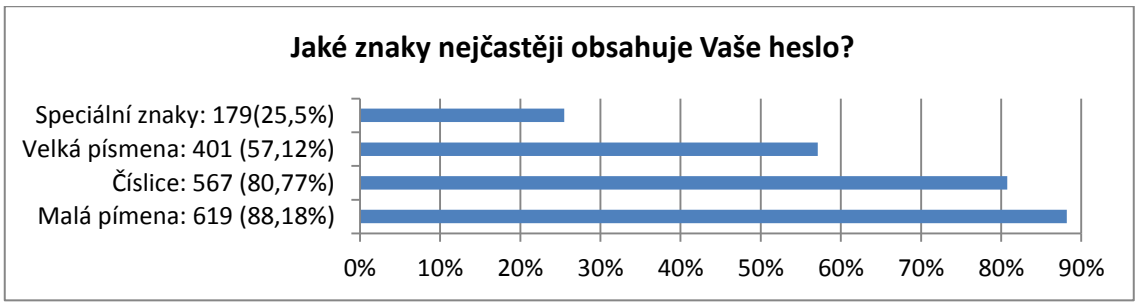
Obrázek 15: Jak často měníte svá hesla?

Silné heslo by se mělo skládat z různých znaků. Nejvíce uživatelé zvolili, že by silné heslo mělo mít číslice (84,33%), dále pak malá písmena (75,21%) a velká písmena (73,79%), nejméně uživatelé volili speciální znaky (61,4%). Respondenti jsou si tedy vědomi, že by se silné heslo měla skládat z různých znaků.



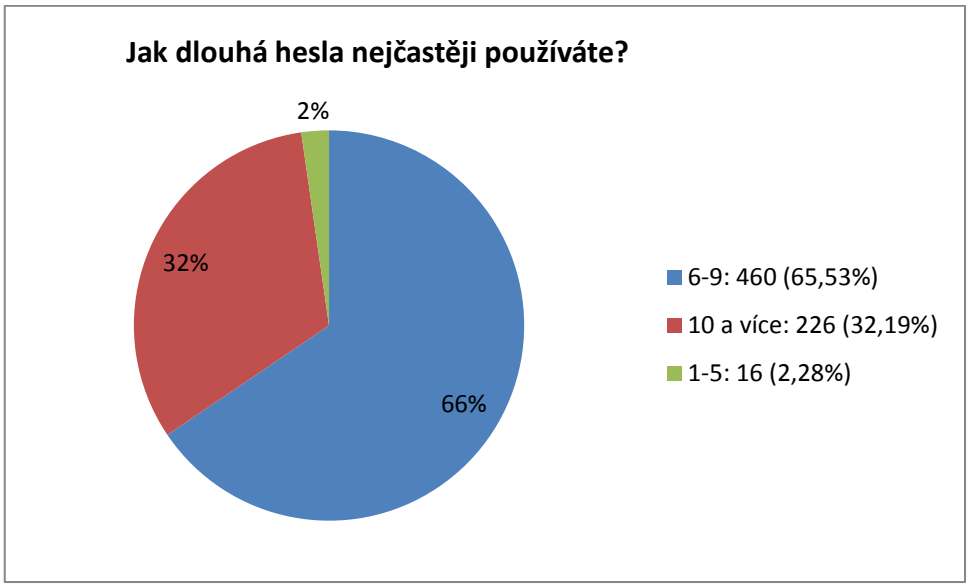
Obrázek 16: Jaké znaky by podle Vás mělo mít silní heslo?

Uživatelé tedy mají představu o silném hesle. Dále se dotazník zabýval otázkou složením znaků hesla uživatelů. Až u 88,18% respondentů se v hesle nejčastěji objevují malá písmena a u 80,77% se objevují v heslech číslice. U více než poloviny respondentů se v hesle vyskytují velká písmena a u 25,5% speciální znaky. Respondenti tedy nejvíce využívají kombinaci malých písmen a číslic.



Obrázek 17: Jaké znaky nejčastěji obsahuje Vaše heslo?

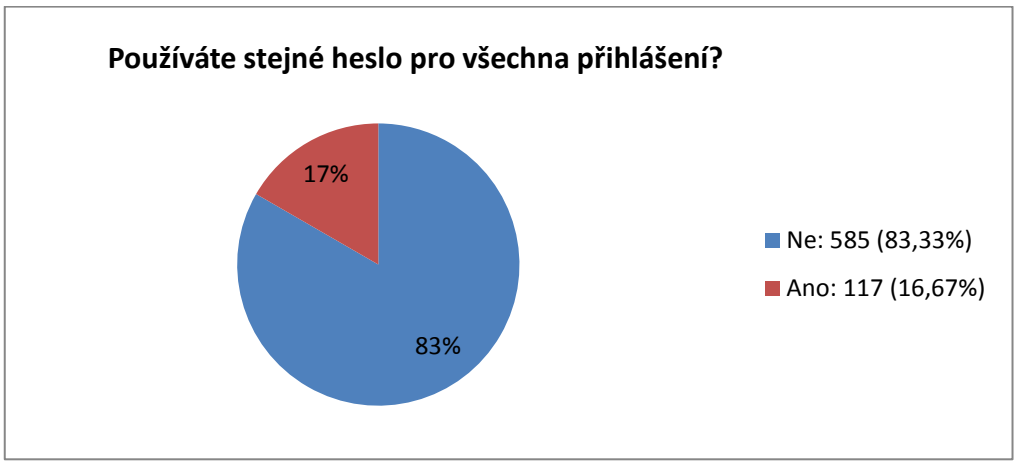
Délka hesla je důležitá, protože na délce hesla společně s použitými znaky v hesle závisí, za jak dlouhou dobu je útočník schopen heslo odhalit. Doporučená délka hesla je kolem 10 znaků. Respondenti nejvíce používají hesla o délce 6-9 znaků (65,56%). Deset a více znaků v hesle používá 32,19% respondentů, zbylé 2% respondentů používají hesla o délce 1-5 znaků.



Obrázek 18: Jak dlouhá hesla nejčastěji používáte?

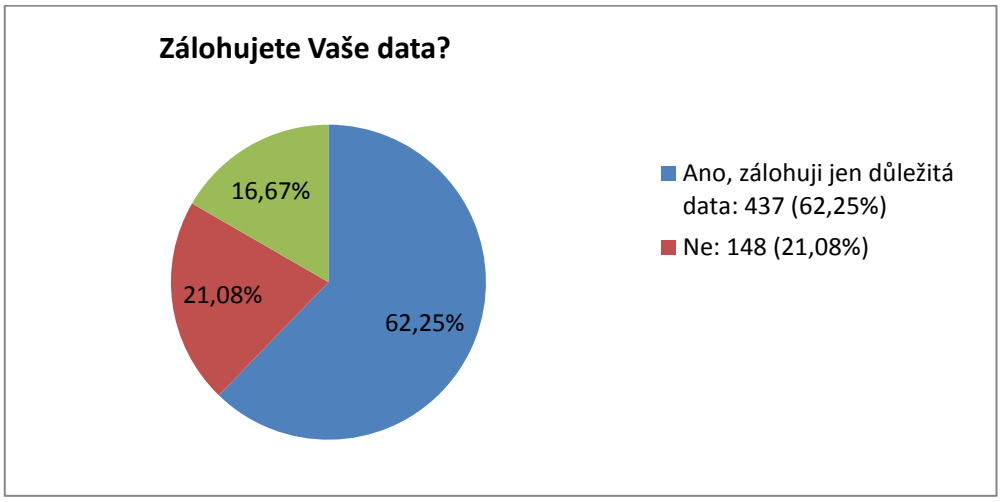
Pokud by respondenti používali pro všechna přihlášení stejná hesla, byly by jejich uživatelské účty více ohroženy. Útočníkovi by stačilo odhalit pouze jedno heslo a dostal by tak přístup ke všem účtům uživatele. Je tedy vhodné používat různá hesla. Z dotazníku vyplynulo, že 83% dotázaných uživatelů nepoužívá stejné heslo pro

všechna přihlášení. Což je dobré, protože pokud útočník odhalí nějaké heslo uživatele, neznamená to, že by měl po odhalení přístup ke všem účtům uživatele.



Obrázek 19: Používáte stejné heslo pro všechna přihlášení?

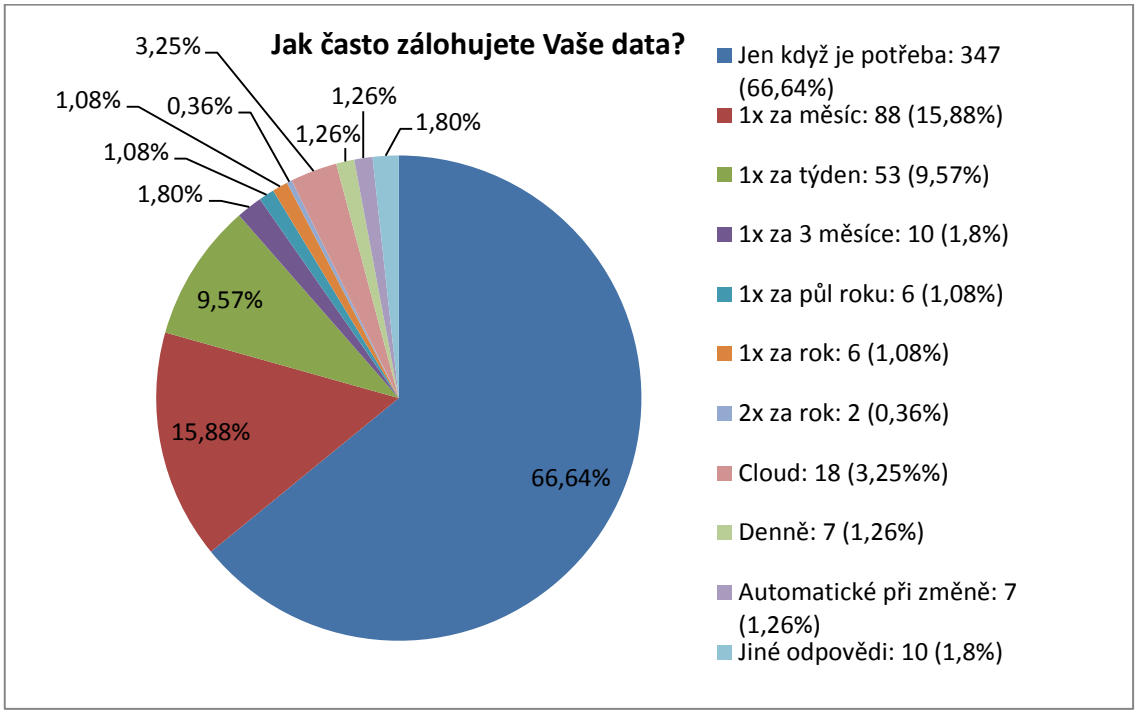
Záloha dat by se měla stát přirozenou aktivitou uživatele. Pokud dojde například k fyzickému poškození disku, na kterém jsou data uložena, mohou být nenávratně ztracena. Proto by data měla být ještě uložena na jiném záložním médiu. Zálohovaná by měla být hlavně data, které uživatel sám vytvořil a jsou pro něj důležitá. Až 21% respondentů vůbec svá data nezálohuje. Zbytek respondentů, 16,67% zálohuje všechna data a 62,25% zálohuje jen důležitá data. Většina respondentů tedy považuje zálohu dat za nutnou součást práce s počítače.



Obrázek 20: Zálohujete Vaše data?

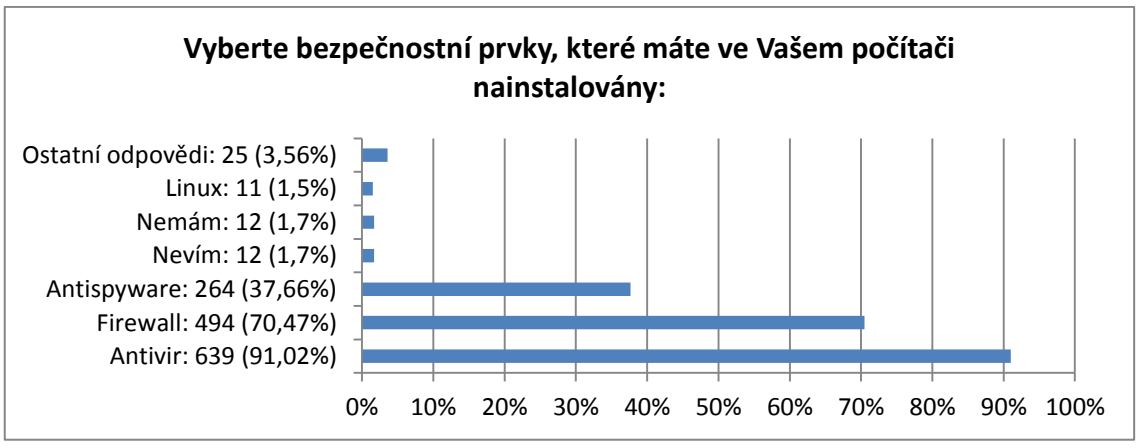
Pokud uživatelé svá data zálohují. Tak se dotazník zabýval otázkou, jak často zálohují. Nejvíce respondentů odpovědělo, že data zálohují, když je potřeba (66,47%). Dále odpovídali respondenti, že data zálohují jednou za měsíc 15,88% a jednou za týden 9,57%. Další, ale o hodně méně početnou skupinou, byla skupina respondentů, kteří

odpověděli, že zálohují pomocí cloudu. Zálohy by měly probíhat u důležitých dokumentů uživatele po každé změně.



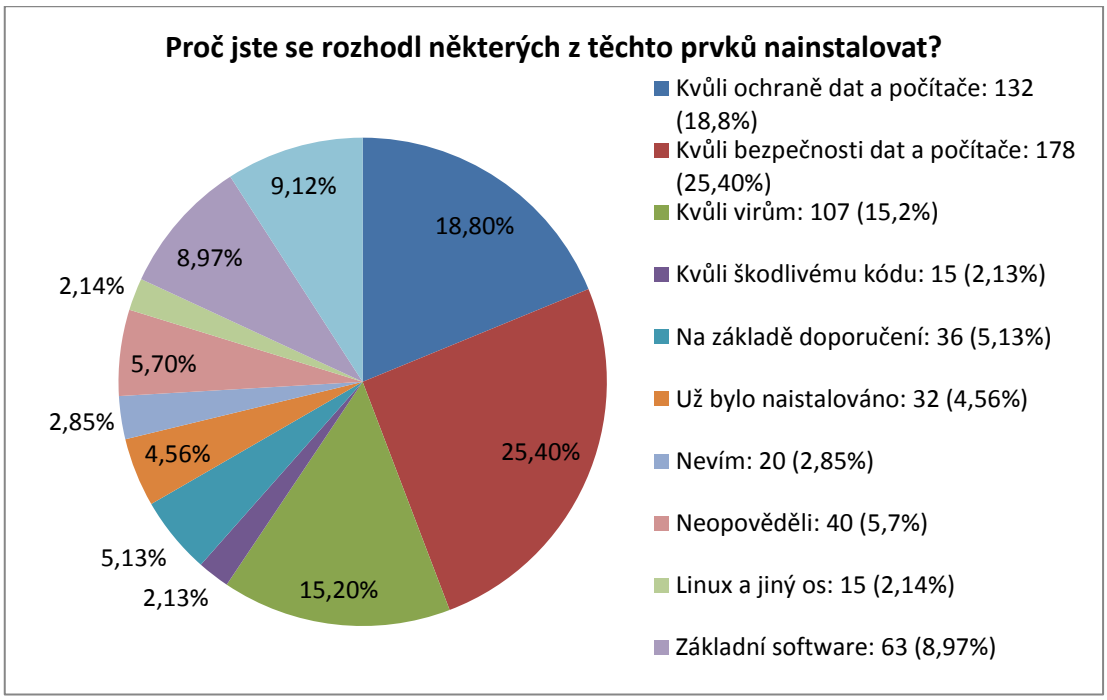
Obrázek 21: Jak často zálohujete Vaše data?

Nejvíce respondenti 91% mají ve svém počítači nainstalovaná antivirový program. Dále pak 70% respondentů má nainstalován firewall a 37,66% respondentů antispyware. Další respondenti nevědí, co mají ve svém počítači nainstalováno (1,7%) anebo nemají nainstalovaný žádný z bezpečnostních prvků. Někteří respondenti v této otázce uvedli jako bezpečnostní prvek operační systém Linux. Operační systém Linux není u nás tak rozšířený a proto není pro útočníky tak zajímavý jako nejvíce u nás rozšířený operační systém Windows.



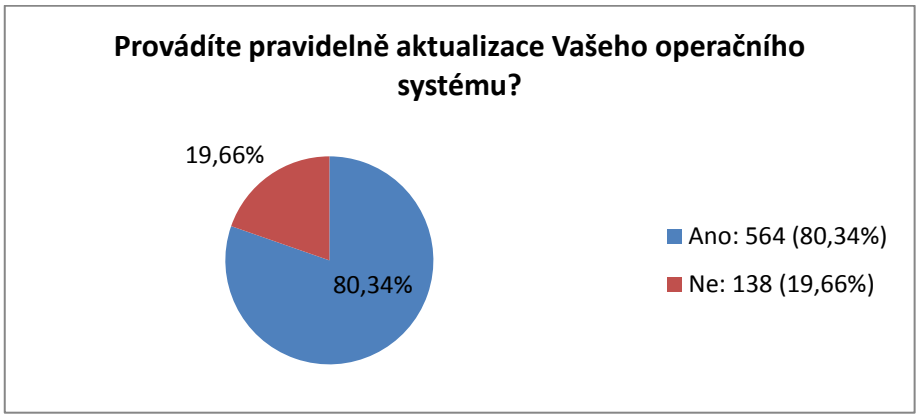
Obrázek 22: Vyberte bezpečnostní prvky, které máte ve Vašem počítači nainstalovány

Nejvíce respondentů se rozhodlo nainstalovat některý z bezpečnostních prvků hlavně kvůli ochraně (18,8%) a bezpečnosti dat a počítače (25,4%). Dále pak hlavně kvůli ochraně před viry 15,2%. Jako základní software považuje nainstalování bezpečnostních prvků 8,97% respondentů. Někteří respondenti instalovali bezpečnostní software na základě doporučení (5,13%) a 4,56% byl software nainstalován někým jiným.



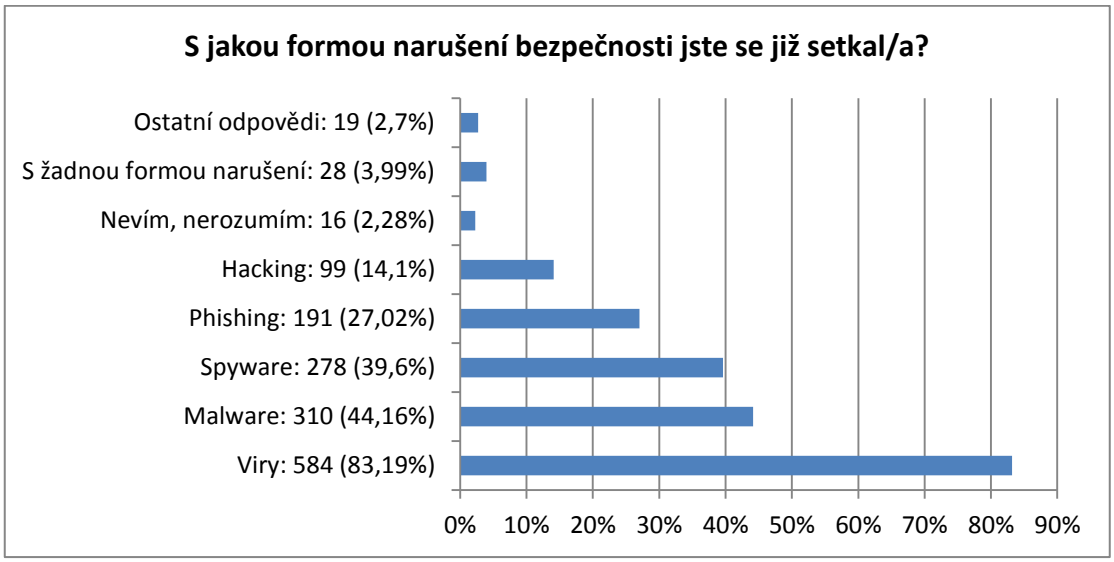
Obrázek 23: Proč jste se rozhodl některých z těchto prvků nainstalovat?

Většina respondentů 80,34% odpověděla ohledně aktualizace operačního systému kladně. Aktualizace jsou pro bezpečnost potřebné, pomocí bezpečnostních děr se do počítače mohou dostat útočníci, proto je potřeba tyto bezpečnostní díry záplatovat, aby se omezilo vniknutí útočníků do počítače.



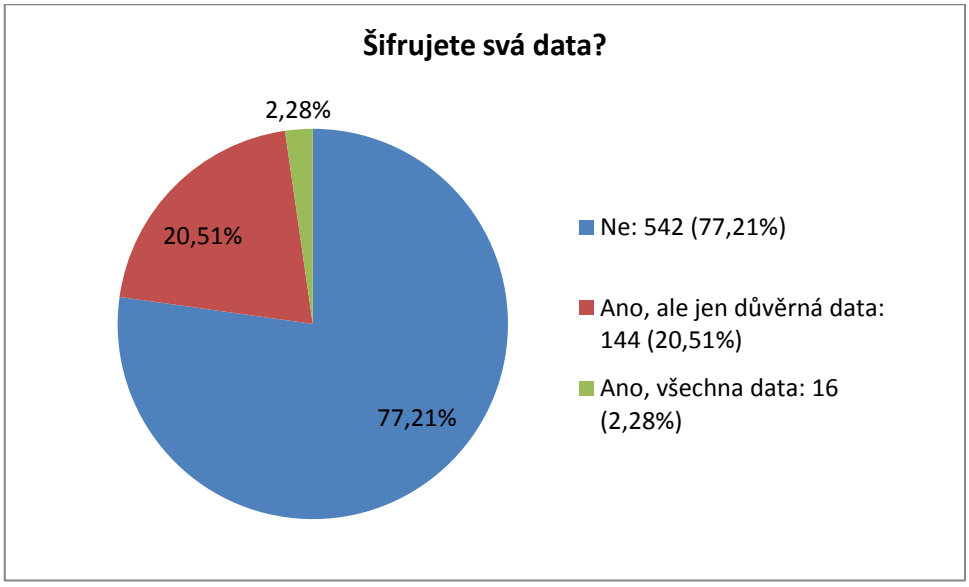
Obrázek 24: Provádíte pravidelně aktualizace Vašeho operačního systému?

Nejvíce se respondenti setkávají s viry 83,19%. Dále pak respondenti uvedli, že se setkali s různým malwarem (44,16%), samostatně uvedli spyware 39,6% respondentů. Další častou formou narušení je phishing (27,2%) a hacking (14,1%)



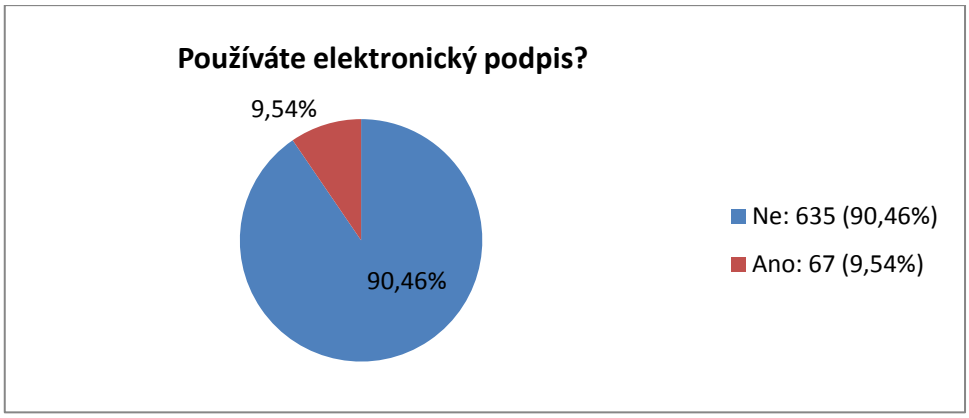
Obrázek 25: S jakou formou narušení bezpečnosti jste se již setkal/a?

Šifrování dat není podle dotazníků u respondentů obvyklé. Svá data nešifruje 77,21% respondentů. Pouze důležitá data šifruje 20,51% a všechna data 2,28% respondentů. Respondenti nejspíše nejsou seznámeni s tím, že se data dají šifrovat a jakým způsobem se data šifrují.



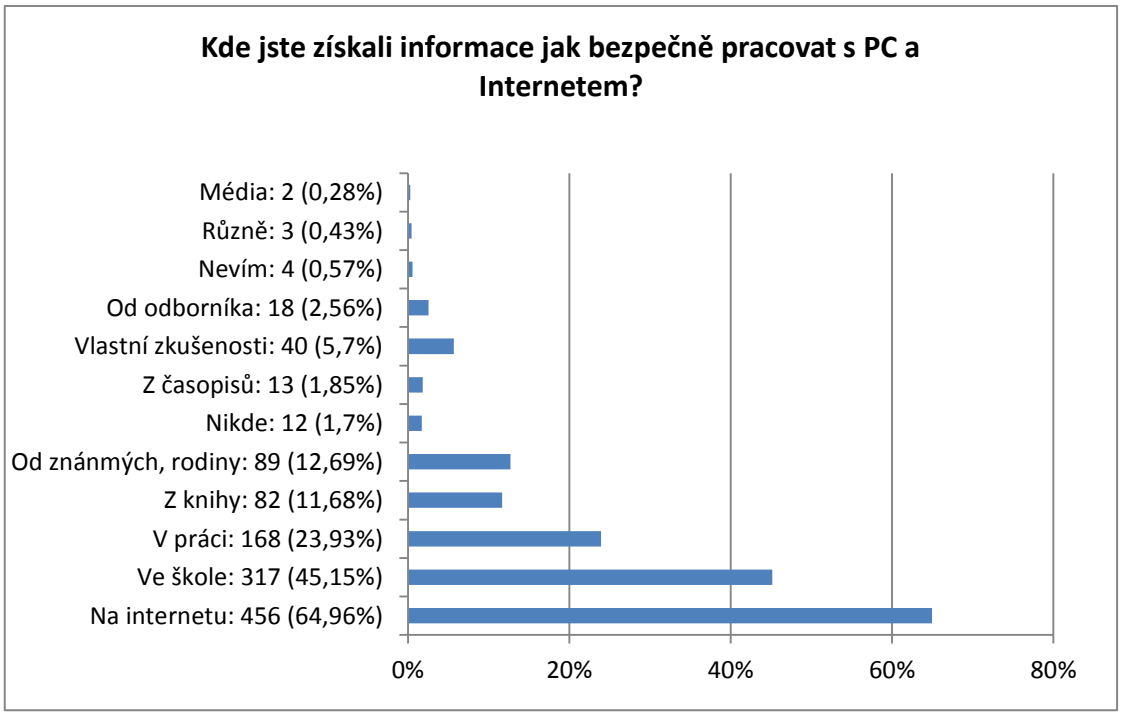
Obrázek 26: Proč jste se rozhodl některých z těchto prvků nainstalovat?

Pouze 9,54% uživatelů používá elektronický podpis. Elektronický podpis není tedy mezi uživateli příliš rozšířený pro běžnou komunikaci. Zatím se především používá při komunikaci se státní správou či bankami.



Obrázek 27: Používáte elektronický podpis?

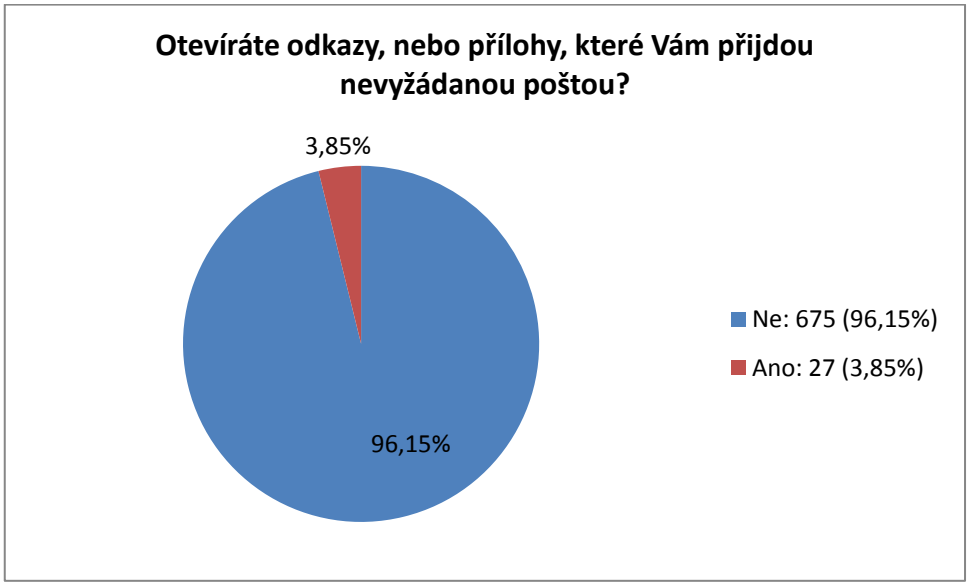
Informace o tom, jak bezpečně pracovat s počítačem získali nejvíce respondenti 64,96% na Internetu, dále pak ve škole 45,15% a 23,39% v práci. Respondenti také získávají informace z knih, od rodinných příslušníků a známých. Je dobré, že jsou respondenti seznamováni s pravidly bezpečnosti nejen ve škole, ale i v práci. Dotazník ukázal, že by většina respondentů měla mít přehled alespoň o základní bezpečnosti práce s počítačem a Internetem.



Obrázek 28: Kde jste získali informace jak bezpečně pracovat s PC a Internetem?

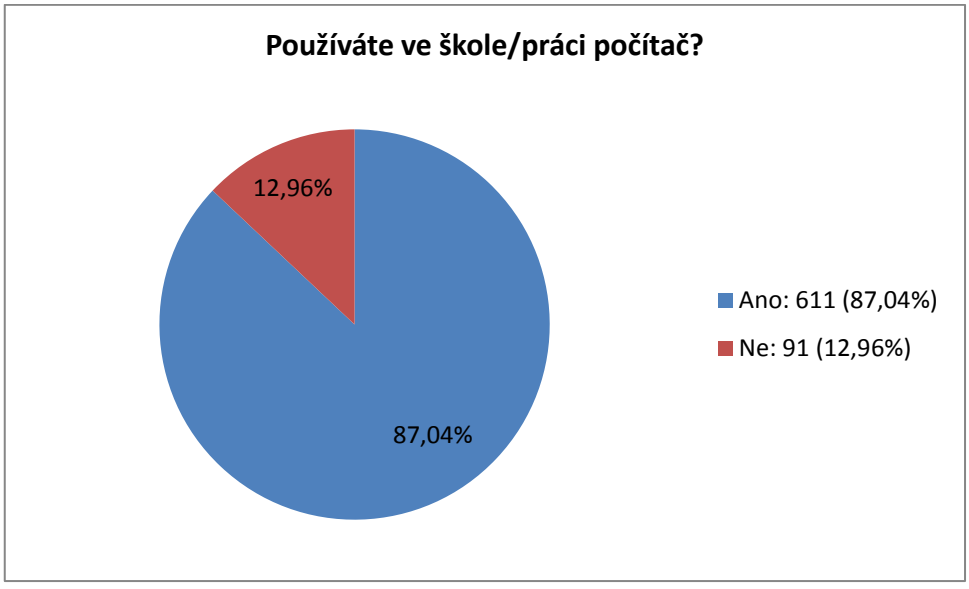
V dnešní době se mnoho nebezpečí šíří pomocí elektronické pošty. Šíří se různé poplašné zprávy, které si mezi sebou uživatelé přeposílají. Také se šíří emaily, které se snaží z uživatelů vylákat citlivá data, proto by uživatelé měli dbát při používání elektronické pošty zvýšené opatrnosti. Z dotazníků vyplynulo, že 96,15% respondentů

nereaguje na vyžádanou poštu, takže většina uživatelů je o hrozbách šířících se přes email nejspíše poučena.



Obrázek 29: Otevíráte odkazy, nebo přílohy, které Vám přijdou nevyžádanou poštou?

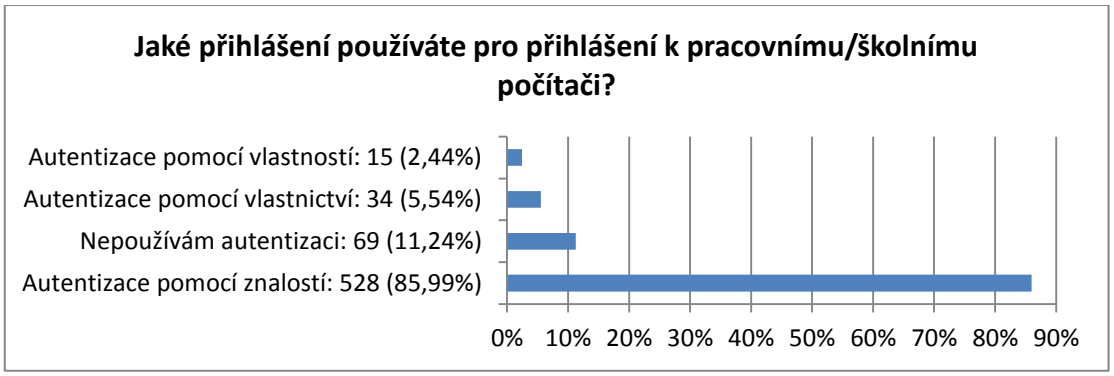
Tato otázka byla rozhodující, jestli respondent mohl pokračovat dále v dotazníku, pokud respondent odpověděl ne, byl dotazník ukončen, pokud odpověděl ano, pokračoval dále ve vyplňování.



Obrázek 30: Používáte ve škole/práci počítač?

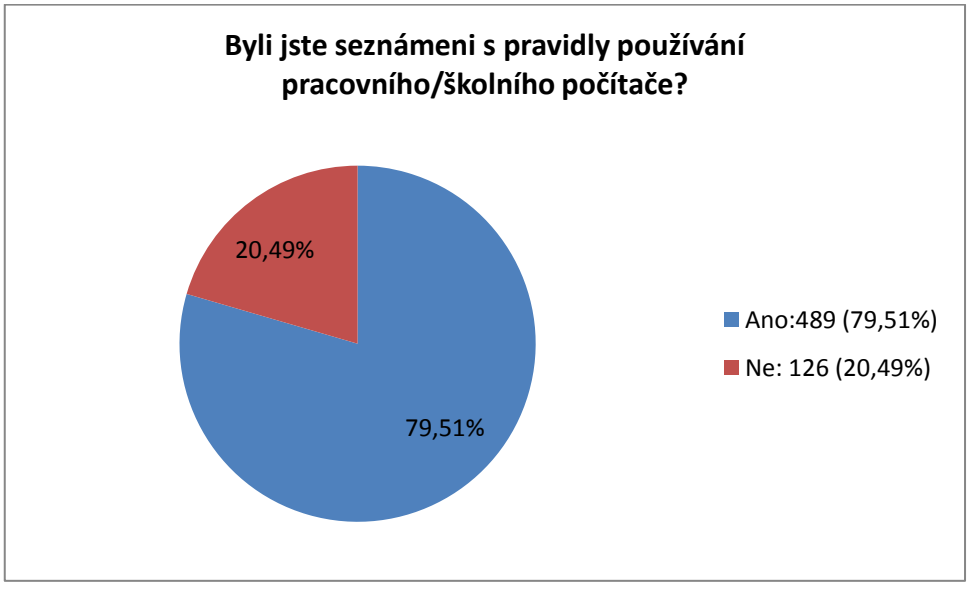
Ve škole i v práci by měl být počítač zabezpečen pomocí autentizace, aby se do sítě nemohli přihlásit nepovolaní uživatelé. Nejvíce respondenti využívají pro přihlášení autentizaci pomocí znalostí (85,99%), dále pak 11,24% respondentů nepoužívá autentizaci. Dále pro přihlášení využívají také autentizaci pomocí vlastnictví (5,54%) a

autentizaci pomocí vlastností (2,44%). Tato otázka předpokládala, že uživatelé využívají jiný počítač než domácí ve škole i v práci. Respondenti, kteří nepoužívají autentizaci, nejspíše buď využívají svůj domácí počítač, nebo nepracují ve firmě, která nemá svou vlastní vnitřní síť.



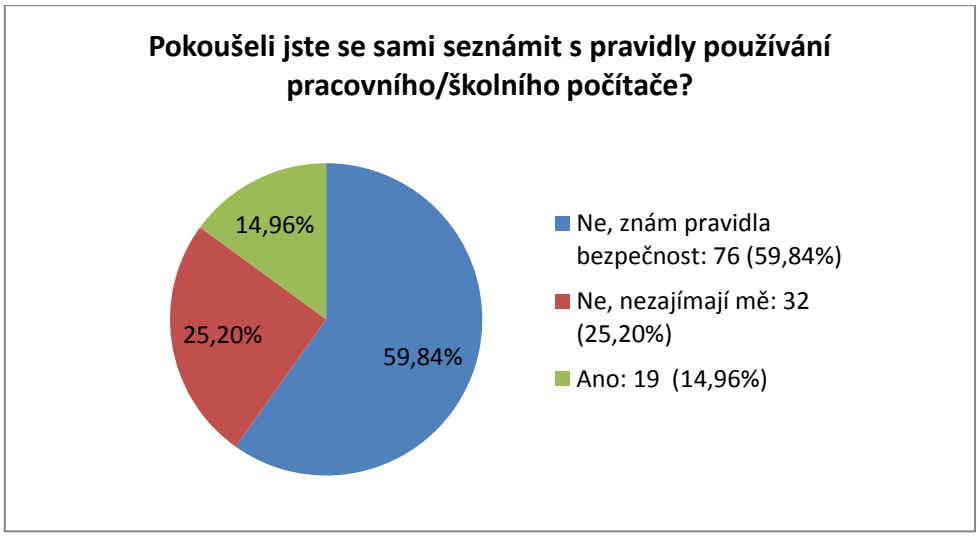
Obrázek 31: Jaké přihlášení používáte pro přihlášení k pracovnímu/školnímu počítači?

Ukázalo se, že většina respondentů (79,51%) byla seznámena s pravidly používání pracovního/školního počítače. Tedy i pro zaměstnavatele je důležité, aby zaměstnanci měli vědomosti o bezpečném používání počítače. Pokud odpověděli respondenti, že nebyli seznámeni s pravidly používání počítače, následovala otázka, jestli se pokoušeli sami s nimi seznámit.



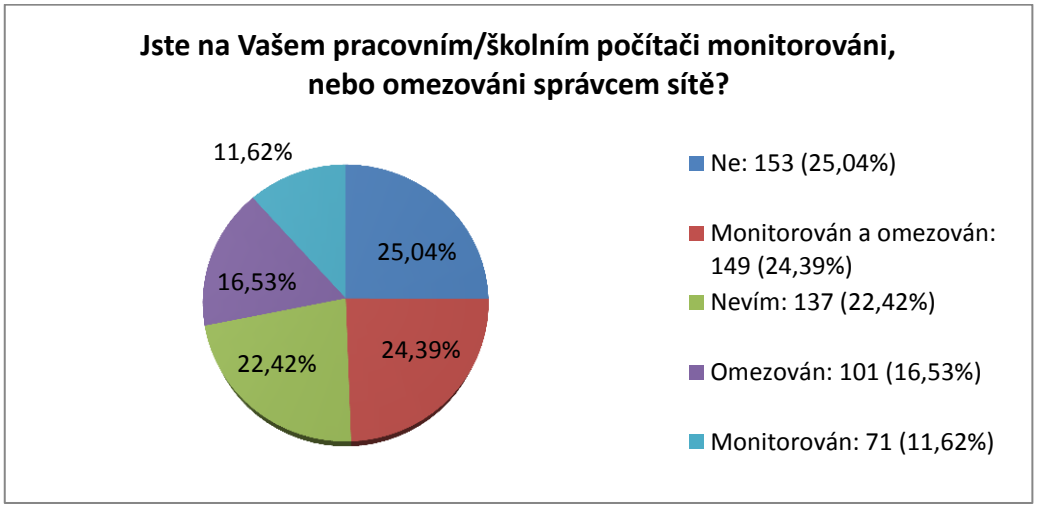
Obrázek 32: Byli jste seznámeni s pravidly používání pracovního/školního počítače?

Jen 14,6% respondentů, kteří nebyli seznámeni s pravidly používání pracovního/školního počítače se s nimi samo pokoušelo seznámit. Ostatní uvedli, že znají pravidla bezpečné práce s počítačem (59,84%) a 25,2% respondentů tyto pravidla vůbec nezajímají.



Obrázek 33: Pokoušeli jste se sami seznámit s pravidly používání pracovního/školního počítače?

Monitorování a omezení uživatelů správcem sítě zajišťuje větší bezpečnost. Pomocí monitorování může správce například zjistit spouštěné aplikace, přihlašování a odhlašování uživatelů. Omezováním určí, co mohou uživatelé provádět, například zda mohou či nemohou instalovat programy. Z dotazníkového průzkumu vyplynulo, že nejvíce 25,04% uživatelů není ani omezováno ani monitorováno, jedná se nejspíše o uživatele, kteří používají svůj vlastní počítač na práci. Další skupina respondentů 24,39% je omezována i monitorována. Pouze omezováno je 16,53% uživatelů a pouze monitorováno 11,62% uživatelů, ostatní uživatelé nevědí, zda jsou omezování a monitorováni.



Obrázek 34: Jste na Vašem pracovním/školním počítači monitorováni, nebo omezováni správcem sítě?

10.2 Závěry dotazníkového průzkumu

Z dotazníkového průzkumu vyplynulo, že většina uživatelů má povědomí o počítačové bezpečnosti. Svůj počítač chrání už při přihlášení nejčastěji pomocí autentizace znalostí

(67,81%). Nejvíce si hesla uživatelé pamatují (82,48%), ale také si hesla často někam zaznamenávají například do prohlížečů, na papír, což může být pro útočníky ulehčení k napadení jejich účtu. Uživatelé vědí, že by silné heslo mělo být tvořeno z různých znaků tedy nejčastěji z malých, velkých písmen a číslic. Také taková hesla používají, která jsou tvořena z různých kombinací znaků.

Pro respondenty je z hlediska bezpečnosti a ochrany dat samozřejmostí, mít nainstalovaný antivirový program a používat firewall. Nejvíce se uživatelé setkávají s viry. Je otázkou zda uživatelé znají i jiné počítačové infiltrace a jestli všechna napadení, se kterými se setkají, nenazývají počítačovým virem.

Dotázaní uživatelé vědí, že zálohy jsou pro uchování jejich dat důležité. Většina uživatelů svá data zálohuje. Hlavně data, která jsou pro ně důležitá. Pro respondenty zatím není příliš obvyklé využívat elektronického podpisu či šifrování dat.

O počítačové bezpečnosti získali respondenti nejvíce informací na internetu, dále pak také ve škole a v práci. Je dobré, že jsou žáci ve školách upozorňováni na možnosti zabezpečení počítače a možnostech napadení.

11 Návrh zabezpečení

Důležitou roli v počítačové bezpečnosti hraje sám uživatel. Většina počítačů je ohrožena kvůli chybě či nevědomosti uživatele. Uživatelé by měli dbát hlavně na prevenci počítačové bezpečnosti. Měli by vědět, jakými druhy útoku a škodlivého kódu může být jejich počítač ohrožen a také, jak nejlépe svůj počítač zabezpečit. Z dotazníkového průzkumu vyplynulo, že většina uživatelů chrání alespoň nějak svá data. Na následujících stránkách bude shrnuto, jak by se uživatel měl správně chovat, aby nejlépe ochránil a zabezpečil svůj počítač.

11.1 Aktualizace

Aktualizace softwaru jsou velmi důležité. Útočníci využívají bezpečnostních děr, pomocí kterých například mohou infikovat počítač. Prováděním aktualizací uživatelé předcházejí hrozbám z Internetu a počítačové sítě. Aktualizace uživatel buď může provádět manuálně, nebo povolit automatické aktualizace. Pro uživatele je nejjednodušší povolit automatické aktualizace, v tomto případě se totiž nemůže stát, že by je uživatel zapomněl provést.

Aktualizovat by se měl hlavně software, který může být napaden z Internetu jako například internetové prohlížeče, skype, icq atd. Záplaty by se měly provádět i v operačních systémech. V operačních systémech se mohou objevit bezpečnostní díry, pomocí nichž může být operační systém ohrožen. A tyto bezpečnostní díry jsou pomocí záplat odstraněny.

Důležité jsou také aktualizace antivirového programu, který si pomocí aktualizací doplňuje svoji virovou databázi, pomocí které odhaluje viry.

Doporučení

- Pravidelně aktualizujte.

11.2 Tvorba hesla a nakládání s heslem

Uživatelé by při tvorbě hesel měli využívat následující doporučení. Uživatelé by měli volit vhodnou délku hesla, nesdělovat svá hesla a hesla by měla obsahovat různé znaky.

Podle dotazníku se ukázalo, že uživatelé vědí, podle jakých pravidel by měli tvořit hesla. S nakládáním hesel už uživatelé, ale tak opatrní nejsou.

Heslo by mělo mít vhodnou délku. Při pokusu útočníka odhalit uživatelské heslo záleží jeho úspěch také na délce hesla. Pokud je heslo dostatečně dlouhé má útočník menší šanci heslo zjistit. Jako vhodná délka hesla se uvádí cca 10 znaků. Čím je heslo delší, tím útočníkovi trvá déle ho prolomit.

Znaky, ze kterých je heslo složeno, jsou také důležité. Uživatelé často volí hesla jako je datum narození, číslo domu, jména svých příbuzných. Tyto hesla nejsou vhodná, i když jsou pro uživatele snadno zapamatovatelná. Heslo by mělo být tvořeno z různých znaků, z malých a velkých písmen, číslic či speciálních znaků. Nedoporučuje se, při tvorbě hesel používat diakritiku a používat písmena y a z, kvůli rozložení znaků české a anglické klávesnice.

Jak vyplynulo z dotazníku, uživatelé si svá hesla často zapisují na papír. U některých uživatelů dokonce jsou vidět hesla na papírku nalepená na monitoru. Je důležité, aby heslo zůstalo tajné. Uživatel by si své heslo měl nechat jenom pro sebe a nikomu ho nesdělovat. Dále vyplynulo z dotazníkového průzkumu, že někteří uživatelé používají, pro uchovávání hesel takzvané klíčenky. Klíčenky jsou programy určené k uchovávání hesel. Uživatel se k heslům uložené v klíčence dostane za pomocí hesla nebo daného souboru anebo kombinace hesla a souboru. Klíčenky jsou rozhodně vhodnější než psaní hesel na papír či uchovávání v prohlížeči. Hesla jsou, ale nejlépe chráněna, pokud je má uživatel pouze ve své hlavě.

Jako klíčenku lze doporučit Keepass, klíčenka umožňuje generování a správu hesel, kterou uváděli respondenti v dotazníku. Keepass je bezplatný program, kam uživatel může umístit všechna hesla do jedné databáze, která je šifrovaná pomocí AES a Twofish. Do databáze hesel se uživatel může dostat pomocí hesla nebo klíčového souboru. Může také pro zvýšení bezpečnosti využít kombinaci hesla a klíčového souboru. Keepass také uživateli nabízí generátor hesel. Dále nabízí export do různých podporovaných formátů, které jsou zašifrovány a synchronizaci databáze

Zda hesla měnit či ne, je dlouho diskutovanou otázkou. Někteří jsou toho názoru, že pokud je heslo odhaleno, útočník ho okamžitě zneužije a není tedy potřeba ho měnit. Změna hesla také může vést k jeho častému zapomínání, pak se uživatelé uchylují k tomu, že hesla zapisují na různá místa. Většina serverů, ale nutí uživatele hesla pravidelně měnit v určitých intervalech.

Doporučení

- Používejte hesla o délce cca 10 znaků.
- Používejte hesla složená z různých znaků (malá, velká písmena, číslice).
- Hesla si pamatujte, popřípadě používejte software pro bezpečné ukládání hesel.
- Hesla nikomu nesdělujte.
- Nepoužívejte stejná hesla pro všechna přihlášení.
- Používejte aplikace pro správu hesel

11.3 Antivirové zabezpečení

Antivirové programy jsou pro zabezpečení počítače důležité. V dnešní době je velmi rozšířený různý malware a spyware. Počítač by měl právě proti malwaru a spywaru chránit antivirový program.

Po instalaci antivirového programu by měl uživatel provést kontrolu celého počítače, aby antivirový program vyloučil přítomnost škodlivého softwaru. Dále je nutné antivirový program nastavit, je vhodné ponechat zapnutou kontrolu spuštěných programů, emailové komunikace, otevíraných dokumentů. Jednou za čas by měl uživatel pomocí antivirového programu provést kompletní kontrolu celého počítače.

Uživatelé mají k dispozici placené a neplacené antivirové programy. Výrobci antivirových programů nabízejí možnost vyzkoušet programy před zakoupením. Uživatel tedy může sám posoudit antivirový program například z hlediska ovládání, rychlosti atd. Může, ale také vybrat antivirový program pomocí testů těchto programů, které lze nalézt například na internetu a v časopisech.

Z neplacených antivirových programů lze doporučit Avira Free Antivirus a z placených Avira Internet Security. Instalace antiviru Avira Free je jednoduchá. Po dokončení instalace provede antivir automaticky kontrolu pevného disku. Nevýhodou tohoto antiviru je, že není k dispozici v češtině. Při internetových updatech program otevírá okno s reklamou pobízející uživatele ke koupi placené verze. Avira zatěžuje počítač minimálně a má dobré výsledky v odhalování škodlivého kódu.

Funkce Avira Free Antivirus

AntiAdware a Antispyware – ochrana před špionážním softwarem a dalšími druhy nežádoucího kódu.

Antirootkit - dokáže v počítači odhalit škodlivý kód, který se skrývá a maskuje.

Ochrana v reálném čase – neustálá ochrana proti virům, červům, trojským koním.

Website Safety Advisor – vyhodnocuje bezpečnost webových stránek pomocí vyhledávačů.

Tracking Blocker – chrání uživatele před sledováním jejich činnosti na internetu.

Funkce navíc Avira Internet Security

Antibot - ochrana před hackery a jejich pokusy o ovládnutí počítače

AHeAD technologie - detekuje neznámé hrozby - podezřelý soubor spustí v odděleném paměťovém prostoru, a zamezí tak možnost průniku infekce do počítače

AntiSpam – chrání uživatele před nežádoucí poštou.

AntiPhishing - uživatele chrání před odcizením osobních informací (uživatelská jména, hesla, údaje o kreditních kartách, atd.).

GameMode – při hraní her není uživatel vyrušován aktualizacemi antiviru.

Firewall - blokuje nepovolené přístupy k počítači a útoky hackerů.

AntiDialer – chrání před přesměrováním internetového připojení.

WebGuard – chrání uživatele před stažením nebezpečných souborů z internetu.

Záchranný disk – poskytuje možnost vytvoření startovacího disku, ze kterého lze nastartovat počítač v případě infekce.

Rodičovská kontrola - vyhodnocuje obsah webových stránek a nabízí možnost jejich zablokování.

Doporučení

- Používejte antivirový program.
- Antivirový program správně nastavte.
- Provádějte antivirovou kontrolu celého počítače.

11.4 Ochrana proti spywaru a adwaru

Spyware shromažďuje v tichosti o uživateli informace, jako jsou například seznam navštívených webových stránek, uživatelská jména a hesla. Na rozdíl od toho adware zobrazuje uživateli reklamu. Většinou je adware a spyware součástí nějakého programu, který si uživatel nainstaloval.

Uživatel by si proto měl pečlivě před nainstalováním programu přečíst údaje o programu, licenční smlouvu apod., kde by informace o adwaru měly být uvedeny. Aby se uživatel vyhnul spywaru a adwaru, neměl by také stahovat software z nedůvěryhodných internetových stránek a od neznámých osob.

Uživatel může poznat, že v jeho počítači je spyware nebo adware pokud se v prohlížeči otvírají vyskakovací okna, webové stránky obsahují více reklamy, došlo ke zpomalení počítače nebo počítač zamrzá.

Pokud dojde k napadení počítače, existují speciální programy k odstranění spywaru a adwaru. Například program SpyBot – Search & Destroy. Tento program umožňuje skenování celého počítače nebo jednotlivých souborů, škodlivé soubory umístí do karantény. Uživateli také nabízí zprávy a protokoly všech skenů. Při instalaci je uživatel vyzván k aktualizaci a dále pak k vytvoření zálohy systému, aby se nestalo, že program odstraní důležité věci.

Doporučení

- Jednou za čas proveďte kontrolu proti adware a spywaru.

11.5 Elektronická pošta

Při používání elektronické pošty by uživatelé měli být také velmi opatrní. V dnešní době dochází pomocí elektronické pošty k šíření škodlivého kódu a je také využívána k sociálnímu inženýrství. Pomocí emailu se útočníci snaží z uživatelů dostat citlivá data,

jako například přihlašovací údaje k bankovnímu účtu, které pak zneužijí ve svůj prospěch. K emailu může být také přiložena neznámá příloha, která po stažení a následném otevření může infikovat počítač.

Emaily jsou často zaplavovány spamem. Spam uživatelům chodí, pokud se dostali do spamerské databáze. V dnešní době si útočníci opatřují emailové adresy tím, že je ukradnou z nějaké databáze. Ale mohou emailové adresy získat z internetových stránek či různých internetových diskusí, na kterých uživatel zveřejní svoji emailovou adresu, tu si pak robot procházející internetové stránky uloží do databáze.

Uživatelé by proto měli dbát na prevenci. Tedy nereagovat na emaily a neotvírat přílohy od neznámých odesílatelů. Uživatelům také mohou pomoci antivirové programy, které dnes již ve většině obsahují antispamovou kontrolu. Jak vyplynulo z dotazníkového průzkumu, většina uživatelů nereaguje na emaily od neznámých odesílatelů. Pokud uživatelům, přijde neobvyklý nebo nějak jinak podezřelý email, mohou se informovat na různých webových stránkách, kde mohou zjistit, zda se jedná o podvodný email.

Emaily putují internetem jako prostý text, takže je útočník může zachytit a číst. Pokud uživatel využívá pro emailovou komunikaci webové prohlížeče nelze posílané emaily šifrovat. Pokud chce uživatel chránit svoje soukromí na emailu, měl by si na počítači nainstalovat emailového klienta jako například Thunderbird a k tomu OpenPGP šifrování. Je nutné, aby obě dvě komunikující strany měly nainstalované OpenPGP šifrování. OpenPGP šifrování zabrání tomu, aby si nikdo jiný kromě příjemce zprávy, nemohl email dešifrovat a přečíst.

Doporučení

- Neotvírejte a nestahujte neznámé přílohy.
- Informujte o rozesílaných podvodných emailech, než na ně začnete reagovat.
- Emaily s citlivými daty šifrujte.

11.6 Uživatelské účty, práva a oprávnění

Čím více lidí přistupuje k počítači, tím více nebezpečí ohrožuje počítač. Řešením je vytvoření uživatelských účtů a nastavení práv a oprávnění.

Měl by být jeden správce počítače, který vytvoří uživatelům jejich účty a nastaví přístupová práva. Správce má neomezená práva, může instalovat, odinstalovat programy, měnit nastavení, zřizovat účty pro ostatní uživatele a přiřadit jim oprávnění. I samotný správce by měl mít vytvořený účet, v němž bude na počítači pracovat.

Pomocí systému Windows by měl správce nastavit požadavky pro tvorbu hesla uživatele. Požadavky by měly kladeny na délku hesla (heslo by mělo mít požadovanou minimální délku), složitost hesla (uživateli by nemělo být povoleno jednoduché heslo, ale kombinace různých znaků), historii použitých hesel (uživatel by neměl mít možnost zvolit heslo, které už bylo použito), určení doby platnosti hesla. Správce by také měl nastavit počet možných pokusů přihlášení do počítače. Nastavení těchto pravidel by mělo lépe zabezpečit uživatelská data.

Každý uživatel bude mít pro přihlášení do počítače tak nastaveno svoje uživatelské jméno a heslo, a budou mu přiřazena práva a oprávnění. Oprávnění je možnost přístupu k daným objektům a právo dovoluje provádět systémové akce.

Přístupová práva slouží k tomu, aby nedocházelo například ke krádeži dat mezi uživateli, nebo aby nedošlo ke smazání uživatelova důležitého souboru. Přístupová práva jsou uživateli přiřazena na základě autentizace.

Lze také využít speciální programy, které zaznamenávají a analyzují aktivitu v počítači. Tyto programy mohou sloužit například ke sledování a zamezování činnosti dětí, ale také pro kontrolu uživatelů, aby věděli, například v jakém programu se často pohybují.

Například placený program Spytech SpyAgent monitoruje práci s počítačem. Provádí záznam stisků kláves, spuštěných aplikací, navštěvovaných webových stránek, použitých hesel atd. Záznam si může uživatel nechat zasílat na email.

Doporučení

- Do počítače přistupujte pod jiným účtem než administrátor.
- Nastavte uživatelům jejich práva a oprávnění.

11.7 Přihlašování k počítači

Podle dotazníkového průzkumu nejvíce uživatelé využívají pro přihlášení ke svému počítači autentizaci pomocí znalostí. Někteří uživatelé používají i kombinace přihlášení autentizace pomocí znalostí a vlastnictví.

Pokud má uživatel v počítači data, která chce zabezpečit proti zneužití, měl by využívat kombinace některých přihlášení. Například může přitom využít autentizaci pomocí znalostí (např. heslo) a autentizaci pomocí vlastnictví (např. USB disk). Tím lépe zabezpečí svá data uložená v počítači, útočník totiž potřebuje znát heslo, ale také k tomu potřebuje USB disk.

Doporučení

- Pro přihlášení k počítači používejte kombinaci autentizací.

11.8 Firewall

Dalším důležitým prvkem pro ochranu počítače je firewall. Firewall chrání počítač před útoky ze sítě a monitoruje i provoz v počítači. Na neobvyklé akce v počítači upozorní a umožní uživateli buď akci povolit, nebo zakázat. Ze začátku je tedy nutné firewall naučit rozpoznat běžné akce v počítači a povolit je, aby firewall takové akce neblokoval. Součástí systému Windows je i firewall.

Existuje celá řada placených a neplacených firewallů. Mezi neplacené patří ZoneAlarm Free od firmy Zone Labs, který je pro domácí využití zcela zdarma a placené ZoneAlarm Extreme Security. Instalace je jednoduchá. Při instalaci musí uživatel uvést jméno, jméno organizace a emailovou adresu.

Funkce ZoneAlarm Free

Two-Way Firewall – zneviditelní počítač před hackery a zastaví spyware

Advanced Firewall – monitoruje programy, sleduje podezřelé chování a zastavuje nové útoky, obcházející antivirovou ochranu

Privacy & Security Toolbar – poskytuje ochranu osobních údajů, soukromé prohlížení a další.

Identity Protection – sleduje zabezpečené nakládání s platebními informacemi a kontroluje, zda nedochází v rámci sledovaných služeb k jejich zneužití.

Funkce navíc ZoneAlarm Extreme Security

Antivirus/Anti-Spyware Engine – detekuje a odstraňuješ viry, spyware, trojské koně, červy a další

Advanced Real-Time Antivirus – updatuje datatabázy antivirových signatur

Enhanced Browser Protection – blokuje internetové hrozby

Parental Controls – dokáže filtrovat a blokovat webové stránky, omezovat čas na nich strávený

Threat Emulation – analyzuje stahování a upozorní, pokud je stahovaný soubor nebezpečný

Find My Laptop – dokáže vyhledat ztracené či ukradené notebooky na mapě, obnoví důležité soubory na dálku

PC Tune-up - optimalizuje počítače pro rychlejší a vyšší výkon.

Doporučení

- Používejte firewall

11.9 Zálohování

Pro většinu respondentů z dotazníku patří zálohování mezi běžně prováděnou práci na počítači.

Aby se uživatelé zabránili ztrátě dat, je potřeba data zálohovat. Zálohovaná data by měl uživatel uložit na jiném médiu, než na kterém se původní data nacházejí. Důležitá data může uživatel zálohovat na CD, DVD, externí disky, online úložiště atd. Média, na kterých jsou zálohovaná data uložena, by měla být uložena na jiném místě než počítač s původními daty.

Na jaké médium bude uživatel zálohovat, by se měl rozhodnout podle toho, jaké množství dat bude zálohovat, zda bude k zálohovaným datům často přistupovat, zda bude zálohovaná data měnit.

CD, DVD

Jejich použití se hodí pro zálohování dat, které uživatel již nebude chtít měnit. Kapacita těchto médií je omezená a dnes již často nedostatečná. U těchto médií je nutné opatrné zacházení a skladování.

Flash disky

Vhodné pro zálohování dat o menším objemu, ke kterým chce uživatel často přistupovat.

Externí disky

Jsou vhodné pro použití, pokud se uživatel chystá zálohovat data o velkém objemu. Je nutné opatrné zacházení, aby nedošlo k mechanickému poškození.

Online úložiště

V dnešní době uživatelé také pro zálohování, jak ukázal dotazníkový průzkum, využívají online úložiště. Online úložiště slouží především pro sdílení dat mezi uživateli, ale lze je také využít pro zálohu dat. Tato úložiště je vhodné použít, pokud se uživatel chystá zálohovat data o menším objemu dat a chce mít přístup k datům z míst připojených k internetu. V dotazníku uživatelé uváděli jako jimi využívané online úložiště například SkyDrive, Dropbox.

Uživatel při zálohování nemusí zálohovat celý obsah pevného disku. Je zbytečné zálohovat například programy, které uživatel může snadno znovu nainstalovat. Důležité je zálohovat data, která jsou pro uživatele důležitá a také ta, co sám vytvořil. Například fotografie, smlouvy, zprávy, emaily atd.

Zálohy je třeba evidovat. U záloh je třeba uvést datum vytvoření zálohy. Uživatel tak bude vědět, kdy provedl poslední zálohu dat a jestli došlo od jejího provedení ke změně zálohovaných dat.

Doporučení

- Zálohujte svá data, především ta co jsou pro vás důležitá.
- Zálohy provádějte pravidelně.
- Čím jsou data důležitější, tím větší počet záloh provádějte.

11.10 Fyzická ochrana dat

Počítač je třeba chránit i před fyzickým útokem, proti krádeži a zničení. Například servery jsou ukládány do speciálních uzamčených místností, aby nedošlo k jejich poškození. V práci nebo ve škole by se mělo monitorovat například pomocí kamer, čipových karet, osoby vstupující do budov a místností.

Pro osobní počítač uživatelů to, ale není příliš praktické. Běžný uživatel by měl dávat pozor na to, kdo má přístup a používá jeho počítač. Záložní média, na kterých má uživatel uložená svá data, by měl ukládat na bezpečné místo, například do trezoru, aby nemohlo jen tak dojít k jejich odcizení nebo zničení. Pokud by došlo například k přírodní katastrofě jako je třeba povodeň či požár. Záložní média by neměla být zničena. Počítač je třeba chránit i před přepětím, při kterém může k poškození základní desky, zdroje nebo třeba také pevného disku. Při výpadku proudu může uživatel přijít o data, která právě vytvářel. Uživatel by měl proto používat přepěťové ochrany a záložní zdroje.

Doporučení

- Hlídejte, kdo má přístup k vašemu počítači.
- Záložní média ukládejte na bezpečné místo.

11.11 Informovanost

Aby uživatelé svůj počítač zabezpečili, měli by být seznámeni s tím, co nebo kdo může počítač ohrozit.

Z dotazníkového průzkumu vyplynulo, že o bezpečné práci s počítačem se uživatelé dozvídají nejvíce na internetu, dále pak ve škole a v práci. Uživatelé by tedy měli mít alespoň nějaké informace o ochraně a zabezpečení svého počítače.

Mezi uživateli například neustále kolují různé pomocí emailu šířené hoaxy. Přitom existuje řada stránek na, kterých se mohou informovat o aktuálně šířených infiltracích a jejich projevech. Například na stránkách http://www.hoax.cz/cze/ může uživatel zjistit, jaké druhy podvodných emailů se rozesílají, pokud mu tedy přijde email, může se podívat do databáze a zjistit zda se nejedná o hoax.

Uživatel by měl také vědět, jak se může projevit, pokud je jeho počítač napaden škodlivým kódem.

- Zpomalení počítače a spuštěných úloh.
- Zamrzání počítače.
- Spouštění nevyžádaných programů.
- Spouštění vyskakovacích oken a reklam.
- Nevyžádané panely, změna domovské stránky v prohlížeči.
- Nelze spustit nástroje jako např. ovládací panely, správce úloh

Doporučení

- Informujte se o šířených infiltracích.

11.12 Šifrování dat

Podle dotazníku není šifrování dat uživatelů příliš obvyklé. Uživatelé nemusí šifrovat všechna svá data, ale měli by šifrovat data, která jsou pro ně nějakým způsobem důležitá. Pokud jsou data zašifrována a pro jejich dešifrování je potřeba například heslo (šifrovací klíč). Šifrovací klíč je důležité uchovat v tajnosti. V případě, že by uživatel posílal někomu přes síť zašifrovaná data, rozhodně by neměl společně se zašifrovanými daty posílat i šifrovací klíč. To by šifrování ztratilo smysl. Klíč by měl odesílatel dat sdělit jinou formou.

Pro šifrování dat se mohou využít různé programy, které lze snadno najít na internetu, například program TrueCrypt je zdarma a umožňuje i šifrování celého disku. Pokud by došlo k odcizení některých dat, tak útočník se k šifrovaným datům bez šifrovacího klíče nedostane.

I při komunikaci na internetu se uživatel setkává se šifrováním. Běžná komunikace na internetu probíhá nešifrovaně. Pokud se chce uživatel přihlásit ke svému účtu, měla by být komunikace šifrovaná. Šifrované spojení pozná uživatel tím, že webová stránka začíná https:\\. Pokud je stránka zašifrovaná, tak je uživatelské heslo před odesláním

zašifrováno. Pokud zadá uživatel heslo přes nezašifrované spojení, přenese heslo v nešifrované podobě, útočník ho může odposlechnout a následně zneužít.

Doporučení

- Šifrujte důvěrná data.
- Šifrujte data posílaná přes síť.

11.13 Elektronický podpis

Elektronický podpis slouží uživatelům k tomu, aby měli jistotu při elektronické komunikaci, že nedošlo ke změně odeslaných dat a věděli, pravou identitu odesílatele.

Jak vyplynulo z dotazníkového průzkumu, respondenti elektronický podpis zatím využívají velmi málo. Elektronický podpis se zatím využívá především ve státní správě, bankovnictví apod. Při běžné komunikaci se nepoužívá.

Pokud uživatelé používají elektronický podpis, měli by bezpečně nakládat se svým soukromým klíčem. V případě, že by získal někdo jejich soukromý klíč, mohl by se klidně za ně vydávat. Pokud je tedy podezření, že byl klíč odcizen, měla by být ihned informována certifikační autorita.

Jestliže se uživatel rozhodně, že chce zřídit zaručený elektronický podpis, měl by si zařídit zaručený elektronický podpis, pomocí kterého může jednat i se státní správou. Zaručený elektronický podpis si uživatel může zařídit u ověření certifikační autority. V České republice to jsou První certifikační autorita (I. CA), PostSignum (Česká pošta), Eldentity.

Závěr

V současné době by měli být všichni uživatelé seznámeni s počítačovou bezpečností a ochranou dat. Uživatelé by měli vědět, jak ochránit a zabezpečit svá data. A s tím kdo a co, může jejich data ohrozit a jak se proti tomu bránit. Předmětem této diplomové práce je popsat druhy ochrany dat a počítačovou bezpečnost.

V teoretické části je vymezen pojem počítačová bezpečnost a její historie. Je zde popsáno dělení ochrany dat na fyzickou ochranu dat, ochranu logického přístupu, ochranu dat před zničením, ochranu přenášených dat. Tyto jednotlivé druhy ochrany jsou v teoretické části podrobně popsány.

Teoretická část se také zaměřuje na autentizaci a řízení přístupu. Jsou popsány podrobně typy získávání autentizačních informací od uživatele. Dále jsou popsány, jakými způsoby může útočník zaútočit na autentizační protokoly. Řízení přístupu je, zde rozděleno na tři modely na povinné, nepovinné a řízení přístup založené na rolích, které jsou následně popsány. Samostatné kapitoly jsou dále věnovány kryptologii a elektronickému podpisu.

V teoretické části jsou rozděleni útočníci z hlediska polohy útočníka, odbornosti, cíle útoku a také druhy útoků, se kterými se uživatel může setkat. Samostatná kapitola je věnována počítačovým infiltracím, kde jsou popsány jednotlivé druhy a cíle jejich útoku.

Dále je teoretická část zaměřena na zabezpečení počítače pomocí firewallu, antivirových programů, antispywaru a antispamu. Jsou uvedeny druhy antivirových programů a firewallů.

Náplní praktické části je provedení a vyhodnocení dotazníkového průzkumu o počítačové bezpečnosti a ochraně dat. Z dotazníkového průzkumu vyplynulo, že většina uživatelů má povědomí o počítačové bezpečnosti. S počítačovou bezpečností jsou seznamováni nejčastěji na Internetu, ale také již ve škole a v práci. Svůj počítač chrání už při přihlášení nejčastěji pomocí autentizace znalostí. Svá hesla si uživatelé nejčastěji pamatují, ale také si hesla často někam zaznamenávají, to z hlediska počítačové bezpečnosti není správné. Pro dotázané uživatele je samozřejmostí mít nainstalovaný antivirový program a firewall. Nejčastěji se setkali s napadením počítače virem. Většina

dotázaných svá důležitá data zálohuje. Respondenti využívají zatím velmi málo elektronického podpisu a šifrování dat.

Dalším cílem bylo provést doporučení z hlediska zabezpečení dat. Východiskem k doporučení ochrany dat byl výše provedený a vyhodnocený dotazníkový průzkum.

Diplomová práce přináší přehled možností, jak uživatelé mohou svá data chránit. Přehled infiltrací, se kterými se mohou setkat a možnosti zabezpečení. Doporučení pro ochranu dat.

Zdroje

[1] ČECH, Pavel a Josef ZELENKA. *Ochrana dat: informační bezpečnost - výkladový slovník*. Vyd. 1. Hradec Králové: Gaudeamus, 2002. ISBN 80-7041-197-X.

[2] *Zpravodaj ÚVT MU Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě* [online]. 2005 [cit. 2015-02-06]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/342.html

[3] *Vladimír Burger* [online]. 2011 [cit. 2015-02-06]. Dostupné z: http://www.burger.sk/kis/2rocnik/virus-1027.htm#

[4] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.

[5] DOBDA, Luboš. *Ochrana dat v informačních systémech*. 1. vyd. Praha: Grada Publishing, 1998, 286 s. ISBN 80-716-9479-7.

[6] ŠENOVSKÝ, Pavel. *Počítače a ochrana dat* [online]. 2. vydání, VŠB-TUO: Ostrava 2007, 56str., Dostupné z:
http://homel.vsb.cz/~sen76/CMS/data/uploads/skripta/pocitace-a-ochrana-dat.pdf

[7] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 80-868-9838-5.

[8] SORIANO, Miguel. *Zabezpečení informací a sítí*. Vyd. 1. V Praze: České vysoké učení technické. ISBN 978-80-01-05296-9.

[9] TICHÝ, Jan. *Jan Tichý* [online]. 2007 [cit. 2015-02-06]. Dostupné z: http://www.jantichy.cz/diplomka/pozadavky/autorizace#

[10] ZELENKA, Josef, Jan ČAPAK, FRANCEK a Hana JANÁKOVÁ. *Ochrana dat: Kryptologie*. Vyd. 1. Hradec Králové: Gaudeamus, 2003. ISBN 80-704-1737-4.

[11] NÁDENÍČEK, Petr. Pravdy o elektronickém podpisu a šifrování. *Svět sítí - informace ze světa počítačových sítí* [online]. 2003, č. 1 [cit. 2015-02-06]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Pravdy-o-elektronickem-podpisu-a-sifrovani-1-zakladni-pojmy-1252003

[12] KOCMAN, Rostislav a Jakub LOHNISKÝ. *Jak se bránit virům, spamu, dialerům a spyware*. vyd. 1. Brno: CP Books, 2005, 148 s. ISBN 80-251-0793-0.

[13] PETERKA, Jiří. Uznávaný, nebo jen zaručený elektronický podpis?. *Computerworld*. 2012, č. 3. Dostupné z: http://www.earchiv.cz/b12/b0209001.php3

[14] http://www.fi.muni.cz/usr/staudek/vystavelova/

[15] VONDRUŠKA, Pavel. Standardy a normy. In: *Jiří Tůma* [online]. 2004 [cit. 2015-02-06]. Dostupné z: http://www.karlin.mff.cuni.cz/~tuma/nciphers/standardy_normy_s-1.pdf

[16] ODCHODKOVÁ, Eliška. *Eliška Ochodková Home Page* [online].[cit. 2015-02-06]. Dostupné z: http://www.cs.vsb.cz/ochodkova/

[17] KRÁL, Mojmír. *Bezpečnost domácího počítače: prakticky a názorně*. 1. vyd. Praha: Grada, 2006, 334 s. ISBN 80-247-1408-6.

[18]JALŮVKA, Josef. *Moderní počítačové viry: podstata, prevence a ochrana*. 1. vyd. Praha: Computer Press, 1996, 217 s. ISBN 80-858-9664-8.

[19] ZELENKA, Josef a Igor HÁK. *Ochrana dat: škodlivý software*. Vyd. 1. Hradec Králové: Gaudeamus, 2005. ISBN 80-704-1594-0.

[20] *HOAX* [online]. 200-2015 [cit. 2015-02-06]. Dostupné z: www.hoax.cz

[21] 6 tips for shopping online without getting scammed. In: *Tutorials, opinions, previews and more - Softonic* [online]. 1997-2015 [cit. 2015-02-07]. Dostupné z: http://features.en.softonic.com/6-tips-for-shopping-online-without-getting-scammed

[22] NÁDENÍČEK, Petr. Pravdy o elektronickém podpisu a šifrování (1) - základní pojmy. *Svět sítí* [online]. 2000-2015, č. 1 [cit. 2015-04-20]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Pravdy-o-elektronickem-podpisu-a-sifrovani-1-zakladni-pojmy-1252003

[23] SKOŘEPOVÁ, Pavla. *Počítačové viry a antivirová ochrana*. Hradec Králové, 2013. Bakalářský práce. Univerzita Hradec Králové. Vedoucí práce doc. RNDr. Štěpán Hubálovský, Ph.D

[24] AntiSpyware. *Antivirové centrum* [online]. 1998-2015 [cit. 2015-02-06]. Dostupné z: http://www.antivirovecentrum.cz/antispyware.aspx

[25] Avira Operations GmbH & Co. KG. [online]. 2015 [cit. 2015-04-20]. Dostupné z: www.avira.com

[26] *ZoneAlarm* [online]. 2015 [cit. 2015-04-20]. Dostupné z: http://www.zonealarm.com/

.

Přílohy

Příloha A – Dotazníkový průzkum

Příloha A – Dotazníkový průzkum

Vážení respondenti,

chtěla bych Vás požádat o vyplnění následujícího dotazníku. Tento dotazník je součástí mé diplomové práce na téma „Počítačová bezpečnost a ochrana dat“. Dotazník bude sloužit k mému výzkumu v praktické části práce, bude východiskem mého návrhu ochrany dat. Předem Vám moc děkuji za vyplnění dotazníku a za Váš čas.

Pavla Skořepová
Studentka Přírodovědecké fakulty
Univerzita Hradec Králové

1) Jaké přihlášení používáte pro přihlášení do Vašeho počítače?(lze vybrat více odpovědí)
   - Autentizace pomocí vlastnictví (např. pomocí karty, flash disku)
   - Autentizace pomocí vlastností (např. pomocí otisku prstu)
   - Autentizace pomocí znalostí (např. heslo, piny)
2) Jakým způsobem uchováváte hesla? (lze vybrat více odpovědí)
   - Hesla ukládám do prohlížeče
   - Hesla si píši na papír
   - Hesla si ukládám do dokumentu v počítači
   - Pamatuji si
   - Jinak
3) Jak často měníte svá hesla?
   - Nikdy
   - 1x za měsíc
   - 1x za tři měsíce
   - jinak
4) Jaké znaky by podle Vás mělo mít silné heslo? (lze vybrat více odpovědí)
   - Malé
   - Velké
   - Speciální znaky
   - Číslice
5) Jaké znaky nejčastěji obsahuje Vaše heslo? (lze vybrat více odpovědí)

- Malé
- Velké
- Speciální znaky
- Číslice

6) Jak dlouhé heslo používáte?
   - 1-5
   - 6-9
   - 9 a více
7) Používáte stejné heslo pro všechna přihlášení?
   - Ano
   - Ne
8) Zálohujete Vaše data? (rozdělující otázka)
   - Ano, zálohuji všechna data
   - Ano, zálohuji jen důležitá data
   - Ne
   - Nevím
9) Jak často zálohujete Vaše data? (pokud ano)
   - 1x za týden
   - 1x za měsíc
   - Jen když je to potřeba
   - Jinak
10) Vyberte bezpečnostní prvky, které máte ve Vašem počítači nainstalovány: (lze vybrat více odpovědí)
    - Antivir
    - Antispyware
    - Firewall
11) Proč jste se rozhodl některých z těchto prvků nainstalovat?
12) Provádíte pravidelně aktualizace Vašeho operačního systému?
    - Ano
    - Ne
13) S jakou formou narušení bezpečnosti jste se již setkal/a? (lze vybrat více odpovědí)
    - Hacking
    - Phishing

- Malware
- Spyware
- Viry

14) Šifrujete svá data?
    - Ano, ale jen důvěrná data
    - Ano, všechna data
    - Ne
15) Používáte elektronický podpis?
    - Ano
    - Ne
16) Kde jste získali informace jak bezpečně pracovat s PC a internetem? (lze vybrat více odpovědí)
    - Na internetu
    - Z knihy
    - V práci
    - Ve škole
    - Jinak
17) Otevíráte odkazy, nebo přílohy, které Vám přijdou nevyžádanou poštou?
    - Ano
    - Ne
18) Používáte ve škole/práci počítač?(rozdělující otázka)
    - Ano
    - Ne
19) Jaké přihlášení používáte pro přihlášení k pracovnímu/školnímu počítači?(lze vybrat více odpovědí)
    - Autentizace pomocí vlastnictví (např. pomocí karty, flash disku)
    - Autentizace pomocí vlastností (např. pomocí otisku prstu)
    - Autentizace pomocí znalostí (např. heslo piny)
20) Byli jste seznámeni s pravidly používání pracovního/školního počítače?(rozdělující otázka)
    - Ano
    - Ne

21) Pokoušeli jste se sami seznámit s pravidly používání pracovního/školního počítače?(pokud ne)
    - Ne, nezajímají mě
    - Ano
    - Ne, znám pravidla bezpečnost
22) Jste na Vašem pracovním/školním počítači monitorováni, nebo omezováni správcem sítě?(lze vybrat více odpovědí)
    - Monitorován
    - Omezován
    - Monitorován i omezován
    - Není ani monitorován ani omezován
23) Jste muž nebo žena?
    - Muž
    - Žena
24) Kolik je Vám let?
    - méně než 15 let
    - 15 až 20 let
    - 21 až 29 let
    - 30 až 60 let
    - více než 60 let