Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Komplexní ochrana domácího PC

Martin Kočí

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Martin Kočí

Podnikání a administrativa

Název práce

Komplexní zabezpečení domácího PC

Název anglicky

Complex Security for Home PC

Cíle práce

Cílem této diplomové práce je:
popsat a zhodnotit současný stav zabezpečení domácích PC;
poskytnout informace o možnostech ztráty dat a jejich dopad;
poskytnout běžným domácím uživatelům informace a návody, jak si zabezpečit svůj domácí PC proti uvedeným nebezpečím.

Metodika

Diplomová práce je rozdělena na teoretickou část, jejíž metodika se skládá ze studia odborné literatury, a dále na praktickou část, ve které je metodika založena na dotazníkovém výzkumu, analýze a syntéze a následném vyhodnocení úrovně a znalostí uživatelů domácího PC.

Doporučený rozsah práce

60 – 70 stran

Klíčová slova

Virus, malwar, spyware, antivirus, antispyware, domácí počítač, internet, firewall, hacker, uživatel

---

Doporučené zdroje informací

Bezpečnost domácího počítače: prakticky a názorně, 2006, Král Mojmír, ISBN 9788024714080
Bezpečnost informačních systémů, 2000, Hanáček Petr, Staudek Jan, ISBN 8023854003
Bezpečnost informačních systémů: vybrané kapitoly, 2003, Halbich Čestmír, Brechlerová Dagmar, ISBN 8021310901
Detekce a prevence počítačového útoku, 2005, Endorf Carl F, Schultz Eugene, Mellander Jim, ISBN 8024710358
http://cs.wikipedia.org/
http://technet.idnes.cz/
http://www.viry.cz/
iDNES.cz – Technet
Viry.cz
Wikipedie

Předběžný termín obhajoby

2015/06 (červen)

Vedoucí práce

RNDr. Dagmar Brechlerová, Ph.D.

Elektronicky schváleno dne 31. 10. 2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 17. 03. 2015

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Komplexní zabezpečení domácího PC" jsem vypracoval samostatně pod vedením vedoucí diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2015 _____

Poděkování

Rád bych touto cestou poděkoval především vedoucí mojí diplomové práce RNDr. Dagmar Brechlerové, Ph.D. za konzultace, připomínky a čas, který věnovala mojí práci.

Velký dík také patří mojí přítelkyni Daně Filípkové za motivaci, nekonečnou podporu a toleranci při mém studiu.

Komplexní zabezpečení domácího PC

Complex Security for Home PC

Souhrn

Tato diplomová práce charakterizuje různé hrozby, kterým jsou vystaveny domácí počítače. Uživatelům poskytuje rady a návody, jak se proti takovým hrozbám bránit, případně, jak minimalizovat jejich dopad.

V teoretické části práce jsou vysvětleny pojmy důležité pro pochopení možných hrozeb, uvedeny principy útoků a také popis jednotlivých řešení, které mají počítač chránit.

Praktická část je vypracována pomocí dotazníku. Po vyhodnocení bylo zjištěno, že většina uživatelů má dobré znalosti v oblasti ochrany dat na domácím počítači, ale nejsou vždy využívány všechny potřebné metody.

V poslední části práce uvádí doporučení, která by měla pomoci uživatelům domácích počítačů výrazně zvýšit ochranu jejich dat před ztrátou. Zároveň tato část obsahuje ekonomické náklady jednotlivých řešení.

Summary

This thesis describes the various threats they are exposed home computers. Users are provided with advice and guidance on how to defend against such threats, or how to minimize their impact.

The theoretical part explains the concepts important for understanding potential threats, principles of attacks and description of solutions which protect the computer.

The practical part is developed using a questionnaire. After evaluation it was found that most users have a good knowledge of data protection on home computer, but not always used all necessary methods.

The last part of the thesis provides recommendations that should help users of home computers to significantly increase the protection of their data from loss. At the same time, this section includes the economic costs of individual solutions.

Klíčová slova: Antispyware, antivirový program, domácí PC, firewall, infiltrace, malware, ochrana, útočník, zálohování.

Keywords: Antispyware, Antivirus, Attacker, Backup, Home PC, Firewall, Infiltration, Malware, Protection.

Obsah

1. Úvod

V současné době jsou osobní počítače rozšířeny do téměř každé domácnosti. Z tohoto důvodu padla volba při výběru tématu na „komplexní zabezpečení domácího PC“. Dalším důvodem bylo to, že jsem od roku 1992 nejen aktivním uživatelem osobního počítače, ale i technikem a poradcem při sestavování, konfiguraci a provozu desítek osobních počítačů převážně v domácím použití. Přicházím proto poměrně často do kontaktu s různě vzdělanými uživateli v oblasti počítačů a rozhodl jsem se zaměřit na oblast zabezpečení.

V dnešní době, kdy je možnost infiltrace uživateli mnohem blíže než dřív, je toto téma velmi aktuální. Práce se zaměřuje na zlepšení informovanosti uživatelů a také bude vodítkem pro zvýšení bezpečnosti jejich počítače, potažmo dat. Také bude navrženo řešení, jak lze počítač ochránit, včetně cenové kalkulace.

2. Cíl práce a metodika

Cílem této diplomové práce je:

- charakterizovat a zhodnotit současný stav zabezpečení domácích PC;
- poskytnout informace o možnostech ztráty dat a jejich dopad;
- poskytnout běžným domácím uživatelům informace a návody, jak si zabezpečit svůj domácí PC proti uvedeným nebezpečím.

Metodika:

Diplomová práce se skládá z teoretické části, která je tvořena z rešerše odborné literatury a vlastních názorů a zkušeností autora, a dále z praktické části, která je založena na dotazníkovém výzkumu úrovně znalostí uživatelů domácího PC.

3. Přehled řešené problematiky

3.1. Zabezpečení domácího PC

Zabezpečením domácího PC rozumíme jeho ochranu před hrozbami, které mohou mít za následek poškození hardwarového vybavení počítače nebo ztrátu dat.

Vzhledem k povaze a použití domácího PC se tato práce nezabývá omezením přístupu k počítači, protože to je doména spíše firemních počítačů a serverů, stejně jako zpracování a implementace bezpečnostní politiky a dalších opatření.

3.2. Domácí počítač

Domácí počítač lze charakterizovat jako osobní počítač, který je určen k soukromému použití v domácnosti a který tudíž neslouží ke komerčním účelům. Vzhledem k tomu, že každý uživatel má jiné preference ohledně vybavení a výkonu domácího počítače, nebude se tato práce zabývat jeho hardwarovým vybavením ani fyzickým vzhledem.

Domácí počítač, v této práci popisovaný a zmiňovaný, může být stolní nebo přenosný, musí minimálně splňovat požadavky pro práci s kancelářským softwarem MS Office, přehrávačem multimediálního obsahu Windows Media Player a internetovým prohlížečem Internet Explorer, vše ve verzích aktuálních pro rok 2014.

3.2.1. Výzkum Českého statistického úřadu

Český statistický úřad pravidelně zkoumá stav informačních a komunikačních technologií v českých domácnostech. Z posledního šetření[1], které probíhalo v roce 2014, vyplývá, že ve druhém čtvrtletí bylo počítači vybaveno 3,1 milionu domácností, což je 72% z celkového počtu domácností[2]. Stále je však Česká republika pod průměrem států Evropské unie[3].

[1] Český statistický úřad. *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci 2014* [online]. 2014-12-02 [cit. 2015-01-10]. Dostupné na www: <http://www.czso.cz/csu/2014edicniplan.nsf/p/062004-14>.
[2] viz příloha č. 1
[3] viz příloha č. 2

Připojením k internetu disponovaly prakticky všechny domácnosti, které byly vybaveny počítačem. Pouhých 10 tisíc z celkového počtu 3,1 milionu nemělo k počítači připojení k internetu.

Dále také bylo výzkumem zjištěno, že poměrně významným prvkem ve vybavenosti domácností počítačem je přítomnost dětí. Zatímco bezdětné domácnosti disponovaly počítačem z 65%, u domácností s dětmi to bylo již 94%[4].

Zajímavý je také podíl stolních počítačů (45%) a přenosných počítačů (52%)[5]. Toto zjištění je důležité ve vztahu k zabezpečení, což bude řešeno v dalším textu.

3.2.2. Uživatel domácího počítače

Základní charakteristika *uživatele* v oblasti počítačů označuje osobu, která používá počítačový systém. Uživatele domácího počítače je tedy možno charakterizovat jako člověka, který používá takovýto počítačový systém k získávání informací, výuce, k zábavě a podobně, aniž by musel mít dostatečné technické či programátorské znalosti pro úplné pochopení tohoto systému.

Tato skutečnost umožňuje používat domácí počítač prakticky každému uživateli, aniž by rozuměl tomu, jak počítač a software funguje a zda to, co dělá, je bezpečné. V tomto ohledu lze ještě rozdělit uživatele domácích počítačů na začátečníky a na pokročilé uživatele.

Právě uživatelům na úrovni začátečník by měla být tato diplomová práce vodítkem a nápovědou, jak se chovat v oblasti bezpečného používání počítače, jaké programy a postupy by měli používat.

3.2.3. Ztráty a jejich dopad

Možné ztráty mohou být **materiálního charakteru**, kdy přestane být funkční některá součást či celý počítač, nebo **datového charakteru**, při kterém dojde ke ztrátě dat. V prvním případě lze obvykle nefunkční část nebo celý počítač nahradit, ale v případě ztráty dat je to možné jen pokud jsou zálohována. V některých případech sice lze data

[4] viz příloha č. 3
[5] viz příloha č. 4

zachránit využitím specializovaných firem, to však s sebou nese poměrně velké náklady s nejistým výsledkem.

Dopady ztráty materiálního charakteru jsou zejména finanční, někdy i časové. U domácích počítačů může problém nastat s náhradou staršího hardwaru, který se již nevyrábí a je tudíž potřeba nahradit celý počítač, což s sebou nese výrazně vyšší náklady.

Dopady ztráty dat jsou zejména pro domácí uživatele velmi nepříjemné, protože často obsahují nejen výsledky práce či studií, ale především vzpomínky ve formě digitálních fotografií nebo videí. To jsou nejcennější data a jejich ztráta je nejnepříjemnější. Bohužel až po ztrátě takto cenných dat se uživatelé poučí a zabezpečí se proti další ztrátě.

3.3. Druhy hrozeb

3.3.1. Vnitřní hrozby

Vnitřní hrozby jsou takové hrozby, které jsou vyvolány faktory působícími přímo na počítač. Dělíme je na:

- **hrozby technické povahy:**
  - náhlý výpadek napětí – přerušení dodávky elektrické energie může mít za následek ztrátu dat, v některých případech i poškození hardwarového vybavení počítače, zejména pevného disku;
  - působení živlů – požár, voda (záplava či vytopení), vichřice. Pro počítač a především data na něm uložená často mívají fatální následky;
  - havárie pevného disku – v důsledku stáří, případně dalších okolností může dojít k jeho částečnému nebo úplnému selhání, při kterém zpravidla dojde i ke ztrátě dat, které jsou na něm uloženy;
  - selhání či kolize ostatního hardwarového vybavení počítače – ať už v důsledku opotřebování, nebo v důsledku manipulace samotným uživatelem. Při těchto selháních obvykle nedochází přímo ke ztrátě dat, vzhledem k povaze použití domácího počítače ale může být odstranění závady poměrně komplikované, protože obvykle nejsou k dispozici materiální či znalostní zdroje;

- **hrozby uživatelské a softwarové povahy:**
  - selhání uživatele – bývá velmi častou příčinou ztráty dat. Samotné selhání či chyba uživatele je téměř vždy dáno jeho neznalostí či neopatrností, a to jak v souvislosti s používáním určitého softwaru, tak zejména v samotném přístupu k zabezpečení počítače;
  - selhání softwaru – v důsledku nekompatibility, programových chyb nebo nastavení uživatelem může dojít až k úplnému pádu softwaru nebo operačního systému. Důsledkem může být jen ztráta času při nápravě, ale také ztráta dat v případě obnovy operačního systému.

3.3.2. Vnější hrozby

Za vnější hrozby považujeme ty, které nejsou vyvolány uživatelem či majitelem osobního počítače.

Jedná se o:

- krádež počítače či jeho příslušenství – u domácích PC dochází ke krádežím nahodile, prakticky vždy dojde ke ztrátě dat jako součásti počítače;
- počítačovou infiltraci – neoprávněné zavedení škodlivých programů do počítače **útočníkem.**

3.3.2.1. Útočník

„*Důležité je si uvědomit, kdo může útočit. Útočník může být vnější, ale v organizaci se často vyskytuje i vnitřní útočník.*“[6]

Pro domácí počítač je málo pravděpodobné, že by mohl působit i vnitřní útočník, takovou situaci ale vyloučit nelze a je třeba s ní počítat.

[6] HANÁČEK, P., STAUDEK, J., *Bezpečnost informačních systémů*, s. 16

Obrázek č. 1: Útočník

Zdroj: CIO Business World.cz. *Drahá e-špionáž* [online]. 2014-01-18 [cit. 2015-01-10]. Dostupné na www: < http://businessworld.cz/bezpecnost/draha-e-spionaz-11408>.

Útočník je definován jako **osoba, která se snaží proniknout do počítače** a to z jakéhokoliv důvodu. Útočníky lze rozdělit například podle toho, kdo útočí, jak uvádí Král[7], na:

1. Hacker – policie *„definuje hackera jako osobu, která proniká do chráněných systémů, kde je jeho cílem ukázat vlastní kvality bez toho, aby měl zájem na získání nebo zničení informací obsažených v systému. Nejdůležitější je pro něj překonání ochrany systému, což je pokládáno za zábavu nebo dobrodružství. Hackerovi ke spokojenosti stačí to, když se o jeho činu hovoří alespoň ve vlastní komunitě. Hacking je jeho koníčkem, u počítače vysedává dlouhé hodiny a získaná data nebo programy využívá pro svou potřebu nebo pro potřebu kolegů nebo přátel.“*[8] V dnešní době je často pojem **hacker** zejména v médiích zkreslován či špatně vysvětlován. Podle nich je *„hacker člověk, který ničí internetové stránky, snaží se narušit informační systémy nebo získat choulostivé osobní údaje jiných uživatelů.“*[9] Taková představa je ale mylná a pramení z neznalosti a z touhy po senzaci. Bohužel takto média zcela překroutila úlohu hackerů ve vývoji informačních technologií a jejich neoddiskutovatelný přínos v oblasti bezpečnosti informačních systémů. Vždy záleží na tom, na jaký „typ“ hackera uživatel narazí. Původní hackeři dodržovali

[7] KRÁL, M., *Bezpečnost domácího počítače*, s. 18
[8] JIROVSKÝ, V., *Kybernetická kriminalita*, s. 51
[9] Tamtéž, s. 51

zásady hackerské etiky a významně přispěli například ke zrodu internetu. V současné době se dělí hackeři na tyto typy:

- White hats – hackeři, kteří se hlásí k hackerské etice a uznávají ji. Díky tomu jsou zaměstnáváni ve firmách, které se zabývají bezpečností informačních systémů, aby pomáhali připravit tyto systémy na případné útoky. Také bývají často najímáni firmami provozujícími počítačový systém, aby ho napadli a dostali se do něj – cílem je následná analýza slabých míst a jejich odstranění dříve, než dojde k napadení jiným hackerem;
- Black hats – hackeři, kteří hackerskou etiku neuznávají. Mají schopnosti srovnatelné s White hats, ale nevyužívají je ke zlepšení zabezpečení, ale ku prospěchu svému nebo svého zaměstnavatele. Takový zaměstnavatel může být konkurence (v tomto případě se jedná obvykle o průmyslovou špionáž, hacker se nechá zaměstnat u konkurence a postupně sbírá a odesílá nashromážděná data), extremistická skupina nebo dokonce teroristická organizace;
- Grey hats – noví hackeři a hackeři, kteří nemají jasno v tom, zda a jak hackerskou etiku uznat a jak přistoupit k problému. Tato skupina je na pomezí mezi výše uvedenými.

2. Cracker – člověk, který prolamuje ochrany počítačových systémů s využitím metod hackerů. V počítačových systémech, do kterých pronikne, může způsobovat destrukční či jinou nežádoucí činnost. Crackeři také upravují komerční programy tak, aby bylo možné je používat bez platné licence. Motivací crackera je obvykle vlastní zisk nebo jiný ekonomický přínos.
3. Lamer – člověk, který nemá dostatek znalostí, schopností a prostředků na to, aby podnikal útoky na firmy či servery a tak se zaměřuje na běžné počítače. Od lamera hrozí běžným uživatelům PC větší nebezpečí než od hackera, protože lamer se do počítače zkouší příležitostně dostat a „něco“ tím dokázat a přitom ani nezná hackerskou etiku.
4. Sniffer – člověk, který odposlouchává síťovou komunikaci a poté ji analyzuje. Jeho hlavním cílem je získávání údajů o bankovních kontech, telefonních čísel, přístupových hesel a dalších, pro uživatele citlivých dat.
5. Phracker – druh hackera, který zneužívá počítače a databáze telefonních společností, aby získal bezplatný přístup k telefonním službám. Toho dosahuje tak,

že napadne a infiltruje programy, které dávají telefonní společnosti zdarma svým zákazníkům.

6. Joyrider – člověk, který se snaží napadnout a proniknout do cizích počítačů za účelem zábavy, případně vyzkoušení či naučení nových technologií. Nezřídka jsou joyrideři studenti.
7. Skript kiddie – začínající útočník, který hledá různé škodlivé kódy, které někdy modifikuje a následně je použije.
8. Softwarový pirát – člověk, který neoprávněně (bez licence) užívá, kopíruje či šíří dalším uživatelům počítačový (komerční) software. U softwaru, který používá nějaké druhy ochrany proti neoprávněnému použití či kopírování, spolupracuje s crackerem, který je schopný takovou ochranu identifikovat a následně software modifikovat. Cílem softwarového piráta je jak vlastní prospěch (užívání softwaru bez platby za licenci k němu), tak zpřístupnění zdarma použitelného počítačového softwaru dalším uživatelům. Ačkoliv se samotný softwarový pirát nesnaží infiltrovat do počítačových systémů, často se díky jeho činnosti různé formy infiltrace rozšiřují mezi uživatele, a proto bývá prakticky všemi autory za útočníka považován.

Jak uvádí Hanáček[10], útočníky také rozdělujeme podle jejich znalostí a vybavenosti do tří následujících kategorií:

1. útočníci slabé síly – jde o amatéry útočící náhodně, využívající náhodně objevená zranitelná místa, často i neúmyslně. Tito útočníci nemají dostatek znalostí, příležitostí a prostředků, proto proti nim stačí přijmout relativně slabá bezpečnostní opatření s minimálními náklady;
2. útočníci střední síly – jde především o hackery, jejichž cílem je dostat se k systémům, ke kterým nemají přístup. Útočníci tohoto typu mají hodně znalostí, nemají však dostatek prostředků ani zjevných příležitostí k běžným útokům. Z uvedených důvodů je nutné přijmout středně silná bezpečnostní opatření;
3. útočníci velké síly – do této kategorie se řadí již profesionální útočníci, kteří mají vysokou úroveň znalostí, získanou obvykle jako počítačoví profesionálové a odborníci. Také mají dostatek prostředků a času k provádění útoků, které se

[10] HANÁČEK, P., STAUDEK, J., *Bezpečnost informačních systémů*, s. 16

vymykají běžné praxi. Proti takovým útočníkům je nutné přijmou silná bezpečnostní opatření, které jsou také adekvátně nákladné.

3.3.2.2. Počítačová infiltrace

„*Počítačová infiltrace je jakýkoliv neoprávněný vstup do počítačového systému, a tím i do jeho dat (dokumenty, programy atd.). V povědomí široké počítačové veřejnosti se pro počítačovou infiltraci mylně rozšířil pojem (počítačový) virus, který se používá vlastně pro jakýkoliv druh napadení počítače (samozřejmě, kromě napadení hrubou fyzickou silou).*“[11]

Přesnější výraz pro počítačovou infiltraci je **malware**. Tento pojem „*se vžil pro označení jakýchkoliv škodlivých (nežádoucích) programů, které se (většinou) bez vědomí uživatele dostaly do jeho počítače.*“[12]

Obrázek č. 2: Malware

Zdroj: Svět hardware. *Počítačová havěť – vývoj a rozdělení malware* [online]. 2009-02-12 [cit. 2015-01-10]. Dostupné na www: <http://www.svethardware.cz/pocitacova-havet-vyvoj-a-rozdeleni-malware/25680>.

Mezi škodlivé programy řadíme:

1. počítačové viry;
2. trojské koně;

[11] KRÁL, M., *Bezpečnost domácího počítače*, s. 20
[12] Tamtéž, s. 20

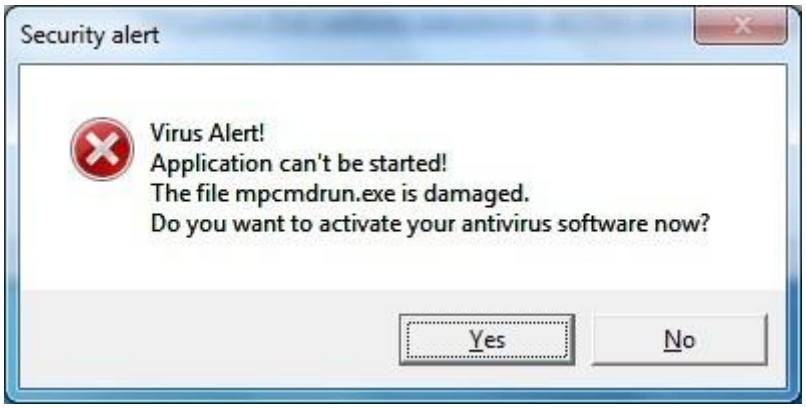
3. červi;
4. spyware;
5. adware;
6. boty;
7. časované bomby;
8. phishing a pharming.

Zcela zásadní roli hraje uživatel počítače. Vždy totiž musí být škodlivý program spuštěn nebo aktivován uživatelem, samovolně se oproti mylným tvrzením nikdy neaktivuje.

1. Počítačový virus

Počítačový virus je *„taková forma počítačové infiltrace, která má schopnost vlastního množení a infikování dalších systémů bez vědomí uživatele a může sloužit k destrukčnímu účelu.“*[13] *„Virus je typ programu, který se dokáže sám šířit tím, že vytváří (někdy upravené) kopie sebe sama.“*[14]

Obrázek č. 3: Virus



Zdroj: Tee Support. *Remove shoprdig.com Virus* [online]. 2011-02-15 [cit. 2015-01-10]. Dostupné na www: <http://blog.teesupport.com/remove-shoprdig-com-virus-shoprdig-com-manual-removal-instructions/>.

[13] KRÁL, M., *Bezpečnost domácího počítače*, s. 24
[14] Wikipedia. *Počítačový virus* [online]. 2014-12-15 [cit. 2015-01-10]. Dostupné na www: <http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus/>.

Základní charakteristiky počítačového viru jsou:

- destrukční účel – cíl viru je smazat či poškodit data;
- připojení k ostatním programům – viry jsou připojeny k běžným programům, nejsou to samostatné programy či soubory;
- schopnost množení – viry se množí a připojují k dalším programům, při množení se mohou modifikovat;
- čekání na spuštění destrukce – spouštěč může být určitá uživatelská akce, datum, čas apod.

Samotné napadení počítačovým virem se obvykle projevuje některým z následujících příznaků:

- úplné zhroucení systému – vir může poškodit soubory životně důležité pro spuštění nebo běh operačního systému, případně smazat či přepsat FAT tabulku pevného disku nebo samotný BIOS. Takovým virem byl například vir zvaný „Černobyl“ (Win32/CIH), který vždy v den výročí výbuchu jaderné elektrárny v Černobylu přepsal tabulku FAT u disku C a ten se stal nečitelným. Zkušení uživatelé a administrátoři dokázali původní FAT tabulku obnovit, avšak takových nebylo mnoho a došlo tak k trvalé ztrátě všech dat. Celkově bylo postiženo tímto virem a jeho modifikacemi na 60 milionů počítačů a ztráty dosáhly jen v komerční sféře nejméně jedné miliardy dolarů. Viry, pracující na tomto principu jsou nejhorší, protože záchrana ztracených dat je obtížná a často nemožná;
- snížení výkonu počítače – viry mohou snížit využitelné místo operační paměti RAM, snížit volné místo na pevném disku, zatížit procesor při běhu infikovaných programů, zpomalit zavádění infikovaných nebo všech programů do paměti, měnit velikosti souborů apod. Všechny tyto akce snižují rychlost zavedení operačního systému a následně odezvu při používání počítače, které vede až k nepoužitelnosti celého PC a je nutno všechny programy včetně operačního systému přeinstalovat;
- špatná funkce programů – viry mohou modifikovat nebo poškodit programy tak, že vůbec nejdou spustit, při jejich spuštění se objevují hlášky o nedostatku paměti nebo jiná neobvyklá hlášení, dochází k neočekávaným pádům programů apod. Některé viry mohou jen vyvolávat chybová nebo vyhrožující hlášení bez dalších projevů a jejich cílem je jen vystrašit uživatele počítače.

Ačkoliv je podle Krále[15] rozdělení virů obtížné a může být nepřesné, můžeme je rozdělit podle toho, jak se chovají, množí, ukládají a jaké mají vlastnosti na viry podle:

- **nebezpečnosti**:
  - destruktivní – napadají počítač a poškozují nebo mažou soubory a data. Likvidace dat může být záměrná u virů, které to mají jako svůj hlavní cíl, nebo nezáměrná u virů, které to mají jako svůj vedlejší cíl například z důvodu zahlazení stop po svojí činnosti;
  - nedestruktivní – po napadení počítače soubory a data neničí, často jde o žerty nebo upozornění bez dalších akcí;
- **projevů**:
  - bez projevů – k infiltraci virem dochází bez jakéhokoliv projevu, cílem je vůbec neupozorňovat na svoji přítomnost. Důvodem je to, že při prozrazení se obvykle uživatel počítače snaží viru zbavit a tím eliminovat jeho záměr (například likvidaci dat apod.);
  - s grafickými projevy – může jít o výzvu k určité uživatelské akci, jako například výzva k instalaci aktualizace, stažení nějakého programu či ovladače apod. Tím obvykle útočník maskuje samotnou instalaci viru. Také může jít o různé grafické vzkazy nebo výzvy nějakého ochranářského hnutí apod.;
  - se speciálními projevy – infiltraci obvykle doprovází nějaký „vtipný“ projev, jako například zrcadlově se pohybující kurzor myši, zpětný chod hodin počítače apod. Tyto projevy mohou působit i humorně, ale to jen do té doby, než uživatel zjistí podstatu této „vtipné“ události;
- **času projevu**:
  - okamžitě se aktivující – viry s touto vlastností se aktivují okamžitě po infiltraci počítače. Důvod je ten, že na takový vir nestihnou zareagovat ani uživatelé, ani výrobci antivirových programů. Stihnou tedy napáchat škody i v současné době, kdy se díky připojení k internetu aktualizují antivirové programy prakticky neustále;
  - aktivující se k určitému datu – dnes již výjimečně používaný druh viru. V dřívějších dobách, kdy nebyl internet rozšířen tak masivně jako dnes, byl

[15] KRÁL, M., *Bezpečnost domácího počítače*, s. 26

tento druh viru velmi oblíbený a rozšířený (viz např. vir WIN32/CIH popsaný výše);

- aktivující se při určitém úkonu – vir se spustí například po několikerém spuštění nebo restartování počítače, stisknutím určité kombinace kláves apod.;

- **oblastí, které jsou napadeny**:
  - boot viry – napadají spustitelné oblasti pevného disku (dříve i disket). Je to jedna z nejstarších technik používaných u virů, kdy dojde k přepsání informací klíčových pro spuštění operačního systému. V dnešní době jsou takové viry okamžitě zjistitelné všemi antivirovými programy, které vždy hlídají zápis do těchto oblastí;
  - souborové viry – napadají všechny spustitelné soubory, které mají koncovku .exe, .com, .sys, .bin. Tyto viry mohou buď jen parazitovat na hostitelském programu a spouštět se nebo šířit s jeho spuštěním, nebo mohou hostitelský program přepsat a spustit se místo něj - dojde ovšem k prozrazení, protože původní program nelze spustit a uživatel se začne zajímat proč;
  - makroviry – jsou infiltrovány do dokumentů kancelářských balíčků, zejména od firmy Microsoft. Tento typ virů se začal objevovat ve druhé polovině devadesátých let minulého století. V poslední době jsou ale kancelářské balíčky proti této skupině poměrně dobře zabezpečeny a raketový růst jejich popularity vystřídal stejně rychlý pád, nicméně se stále ještě vyskytují;
- **chování**:
  - stealth a substealth – viry neviditelné, tajné nebo skryté. Snaží se před uživatelem počítače skrýt všechny stopy vedoucí k odhalení svojí přítomnosti tak, že maskují všechny změny v souborech, které provedly. Předpokladem k neviditelnosti je zavedení viru do operační paměti bez odhalení antivirovým programem. To je v současné době velmi obtížné, protože jsou na tuto hrozbu antivirové programy dobře připraveny. Pokud ale dojde k dočasnému vypnutí antivirové ochrany, nebo k instalaci či spuštění antivirového programu až po napadení virem, může tento vir skrývat svoji přítomnost bez povšimnutí;
  - polymorfní – tyto viry se snaží před uživateli a antivirovými programy maskovat tím, že dokáží změnit strukturu svého těla, které zašifrují. Tím jsou velmi obtížně zjistitelné, pro jejich odhalení bylo nutno zakomponovat do

vyhledávacích algoritmů antivirových programů stroje zaměřené na polymorfní viry a došlo tak k jejich prodražení;

- retroviry - viry tohoto typu fungují na principu zaútočení na antivirový program dříve, než jej odhalí a vyeliminuje. Někdy se tyto viry označují také jako odvetné viry, protože útočníci takové viry často vytvářejí jako odvetu za to, že byl jejich dřívější vir odhalen;
- tunelující – viry, které se snaží obejít či ukrýt před antivirovým programem technikou tunelování. Stejnou techniku používají antivirové programy pro obcházení nalezeného viru, protože předpokládají, že mohl být virus zaveden ještě před spuštěním antivirového programu a díky tomu nemusel být zjištěn;
- armored – viry, které jsou obrněné programovými kódy, které mají za úkol ztížit práci antivirovým programům při jejich detekci. Mohou se krýt za pomoci zaváděcího kódu, který navede antivirový program na jiné místo, než je samotný virus uložen, nebo pomocí obalového kódu, který odvrací pozornost antivirového programu od samotného kódu viru;

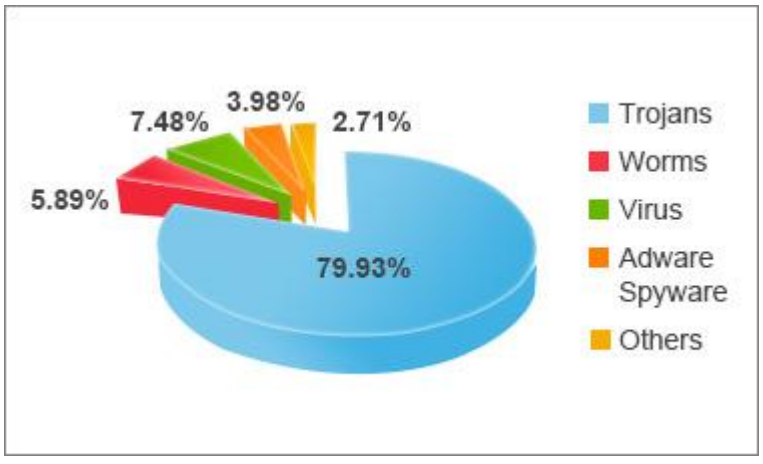
- **umístění v paměti**:
  - rezidentní – virus, který se nelegálně uloží do operační paměti počítače a stane se tam rezidentem. Odtud pak nepozorován provádí svoji činnost. Podkategorií rezidentních virů jsou TSR viry, které se (relativně legálně) nahrály do operační paměti pomocí programů pro MS-DOS. V současné době již nejsou rezidentní viry tak rozšířené, a to díky 32 a 64 bitovým operačním systémům, díky nimž musejí být viry v operační paměti sofistikovanější a tím snáze odhalitelné;
  - nerezidentní – pro svoji škodlivou činnost a šíření nevyužívají operační paměť počítače a nemusejí být ani trvale umístěné v napadeném počítači. Z tohoto důvodu bývají označovány jako viry přímé akce;
- **rychlosti šíření**:
  - rychlé – viry napadající soubory při jejich spuštění i soubory, které jsou otevírány při přesouvání nebo kopírování;
  - pomalé – viry napadající jen soubory, které jsou upravovány nebo kopírovány operačním systémem, např. při manipulaci samotným uživatelem. Z tohoto důvodu je obtížná jejich detekce;

- sparse – viry napadající počítač jen příležitostně, případně při splnění konkrétních podmínek s nízkou pravděpodobností jejich výskytu. Cílem takového chování je minimalizace rizika odhalení uživatelem nebo antivirovým programem;
- ZOO – viry, které nejsou schopné života, a běžný uživatel se s nimi nesetká. Vytvářejí se za účelem nějakého experimentu, případně dosažení určitého prvenství (např. první virus roku apod.).

2. Trojský kůň

Trojský kůň je program, který utajeně provádí škodlivé operace, přičemž ale vypadá jako obyčejný a legální program. Obvykle se trojský kůň vyskytuje ve spustitelném souboru (s koncovkou .exe nebo .com), například jako instalační program, dokonce i jako spouštěcí soubor instalace antivirového programu. Rozdíly mezi trojskými koni a počítačovými viry jsou zásadní – **trojský kůň není schopen množení a nepřipojuje se k jinému souboru,** resp. hostiteli. Přesto je tento typ infiltrace jednoznačně neoblíbenější, jak ukazuje následující graf s rozdělením počítačových infiltrací podle typu.

Graf č. 1: rozdělení infiltrací podle typu v roce 2013



Zdroj: MediaCenter Panda Security. *PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections, Set New Record* [online]. 2013-05-03 [cit. 2015-01-10]. Dostupné na www: <http://www.pandasecurity.com/mediacenter/press-releases/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/>.

Často jsou trojské koně využívány jako **zadní vrátka**. Je to kategorie trojských koní, která se vždy snaží být uživateli počítače skryta. Podstatou funkce zadních vrátek je

otevření komunikační cesty mezi napadeným počítačem a útočníkem. Na napadeném počítači je spuštěna serverová část zadních vrátek a na počítači útočníka pak běží část klientská. Díky tomu může útočník převzít kontrolu nad počítačem, resp. operačním systémem a kopírovat data či s nimi jakkoliv manipulovat.

V současné době jsou trojské koně považovány za dost nedokonalou formu počítačové infiltrace, ačkoliv tomu podíl na celkových infiltracích vůbec neodpovídá. Proto je třeba mít se před nimi na pozoru i vzhledem k tomu, jaké škody mohou být s jejich pomocí napáchány.

3. Červ

„*Červi jsou takovým typem infiltrace, která se do počítače dostává převážně elektronickou poštou*“[16]. V dnešní době, kdy je elektronická pošta využívána téměř každým uživatelem počítače, je tento druh infiltrace velmi rozšířený.

Do počítače infiltrace probíhá tak, že je pomocí elektronické pošty poslán soubor, který se tváří jako např. fotografie, má zajímavý název (jméno známého herce, herečky či modelky apod.) a je spustitelný při otevření – mívá i dvojitou koncovku. V případě, že je útok dobře promyšlen a je pro červa vymyšlen takový název, který přiměje uživatele přílohu otevřít, začíná pro červa život, který lze obvykle rozdělit do dvou fází:

- v první fázi se z adresáře napadeného počítače rozešle na ostatní emailové adresy. Pokud se červ tváří velmi atraktivně a uživatelé ho bez hlubšího zamyšlení otevírají, šíří se geometrickou řadou. Nejvýkonnější červi v historii byli schopni se rozšířit na desítky milionů počítačů po celém světě během několika hodin;
- ve druhé fázi přichází na řadu splnění úkolu, ke kterému byl červ vytvořen – obvykle k útoku typu DDoS, při kterém zneužije napadené počítače.

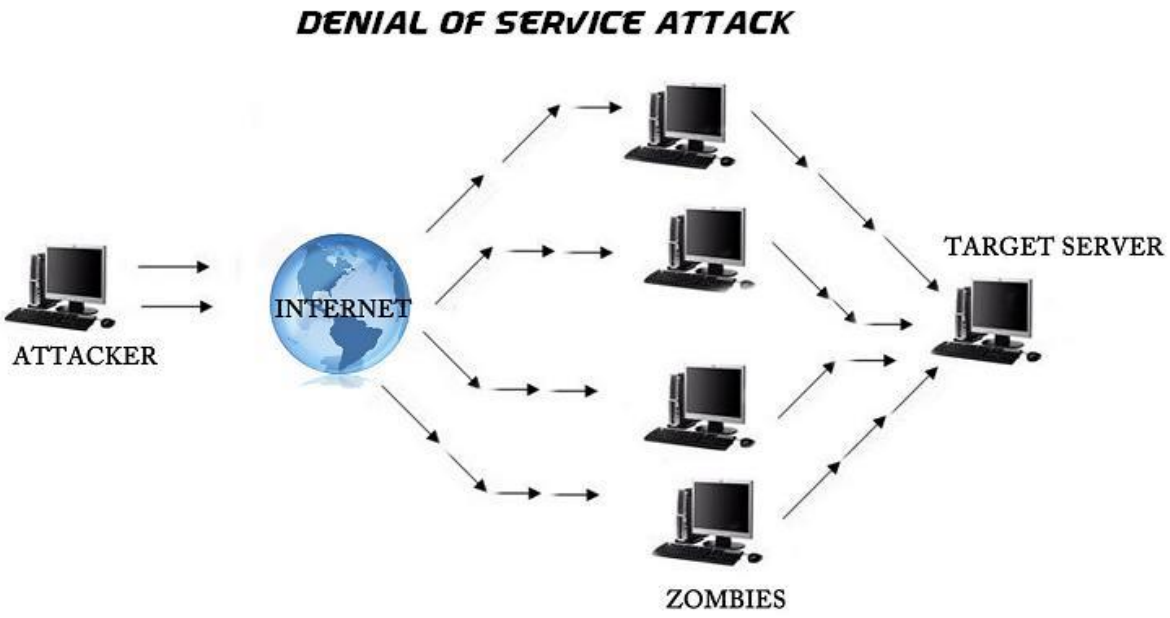
DDoS (Distributed Denial of Service)[17] je takový typ útoku, během kterého je obvykle napaden významný server způsobem, který zcela znemožní komunikaci s ním a jeho služby jsou tak vyřazeny z provozu. Samotné napadení serveru probíhá tak, že pomocí tisíců až milionů napadených počítačů (tzv. zombies) jsou zasílány na cílový server

[16] KRÁL, M., *Bezpečnost domácího počítače*, s. 22

[17] DDoS je rozšířenou variantou DoS útoku, při kterém je server dotazován na dostupnost jedním počítačem nebo serverem. Proti tomuto útoku jsou v současné době servery chráněny.

obyčejné dotazy na dostupnost, kterých je ale takové množství, že je server zcela zahlcen a dojde k jeho vyřazení. Útočníci tímto způsobem dokáží vyřadit z provozu prakticky jakýkoliv server s jakýmkoliv zabezpečením proti napadení. Mezi nejvýznamnější útoky patří vyřazení z provozu serverů americké vlády, celou síť KLDR nebo zpomalení celého Evropského internetu[18]. V České republice byly tyto útoky nejvýznamnější na začátku března 2013, kdy byly ochromeny služby řady institucí - např. Aukro.cz, Seznam.cz, mobilní operátoři či banky.[19] Velmi často se také tento typ útoku používá v kybernetické válce nebo jako odveta (např. radikálů za útoky na jejich pozice, hackerů za přijetí zákona potírajícího kybernetickou kriminalitu apod.).

Obrázek č. 4: DDoS útok



Zdroj: GloboTech Blog. *Category Archives: Cloud Computing* [online]. 2014-10-22 [cit. 2015-01-10]. Dostupné na www: <http://www.gtcomm.net/blog/category/cloud-computing/>.

Nejsofistikovanější útoky typu DDoS, kromě vyřazení serveru, dokáží pomoci odcizit citlivá data, která se na napadeném serveru nacházejí. Důkazem může být např. útok

[18] Technet.cz. *Skončil obří útok na evropský internet. Hrozba i pro internet věcí* [online]. 2014-02-12 [cit. 2015-01-10]. Dostupné na www: <http://technet.idnes.cz/utok-ntp-evropa-nejmasivnejsi-internetovy-utok-ukazuje-narust-riziko-139-/sw_internet.aspx?c=A140212_161619_sw_internet_vse/>.
[19] Viry.cz. *Rozsáhlé DDoS útoky ochromily služby řady institucí* [online]. 2013-03-07 [cit. 2015-01-10]. Dostupné na www: <http://www.viry.cz/rozsahle-ddos-utoky-ochromily-sluzby-rady-instituci/>.

z konce roku 2014, vedený ze strany KLDR proti serverům filmové společnosti Sony Pictures, při kterém byly odcizeny a následně zneužity citlivé údaje a soubory zaměstnanců této společnosti.

4. Spyware

Pojmem spyware označujeme špionážní programy. „*Jsou to programy, které sbírají a odesílají informace o vašem počítači.*“[20] Zejména se jedná o informace o používaných heslech, přístupech na webové stránky či údaje o používaných programech. Některé z těchto programů dokáží snímat stisknutí kláves a následně je odeslat útočníkovi, který tak může zjistit přihlašovací jména a hesla do různých, např. bankovních, aplikací.

Špionážní programy se do počítače mohou dostat jako součást programů, které uživatel instaluje a nezřídka bývá jejich instalace povolena v licenčním ujednání. Také se mohou do počítače dostat nelegálně - pomocí viru.

Obrázek č. 5: Maskování spywaru za anti-spyware

Zdroj: HowStuffWorks. *How Spyware Works* [online]. 2005-02-16 [cit. 2015-01-10]. Dostupné na www: <http://computer.howstuffworks.com/spyware1.htm>.

Kromě toho, že špionážní programy sbírají a odesílají data, často zpomalí chod operačního systému, programů a internetového počítače. Také dokáží do počítače stáhnout a nainstalovat další špionážní programy a ve výsledku se hlídat před jejich odinstalováním. V důsledku těchto činností dochází k takovému zpomalení počítače, že je nutná jeho reinstalace, pokud se spyware nepodaří zcela odstranit, což je velmi obtížné.

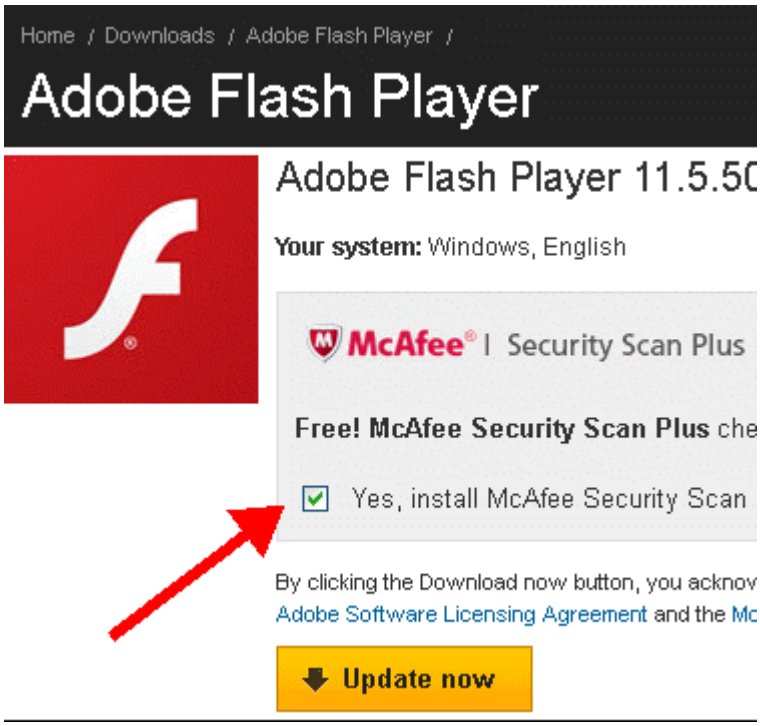
[20] KRÁL, M., *Bezpečnost domácího počítače*, s. 207

Oblíbenou lokalitou spywaru jsou internetové stránky s erotickou tématikou, stránky s nelegálním softwarem, různé stránky s ovladači, které již původní výrobci nevydávají apod.

5. Adware

Adware je, stejně jako spyware, do počítače instalován s nějakým programem, obvykle volně šiřitelným (freewarem). Uživatel počítače vždy musí s jeho instalací souhlasit formou potvrzení licenčních ujednání.

Obrázek č. 6: Adware



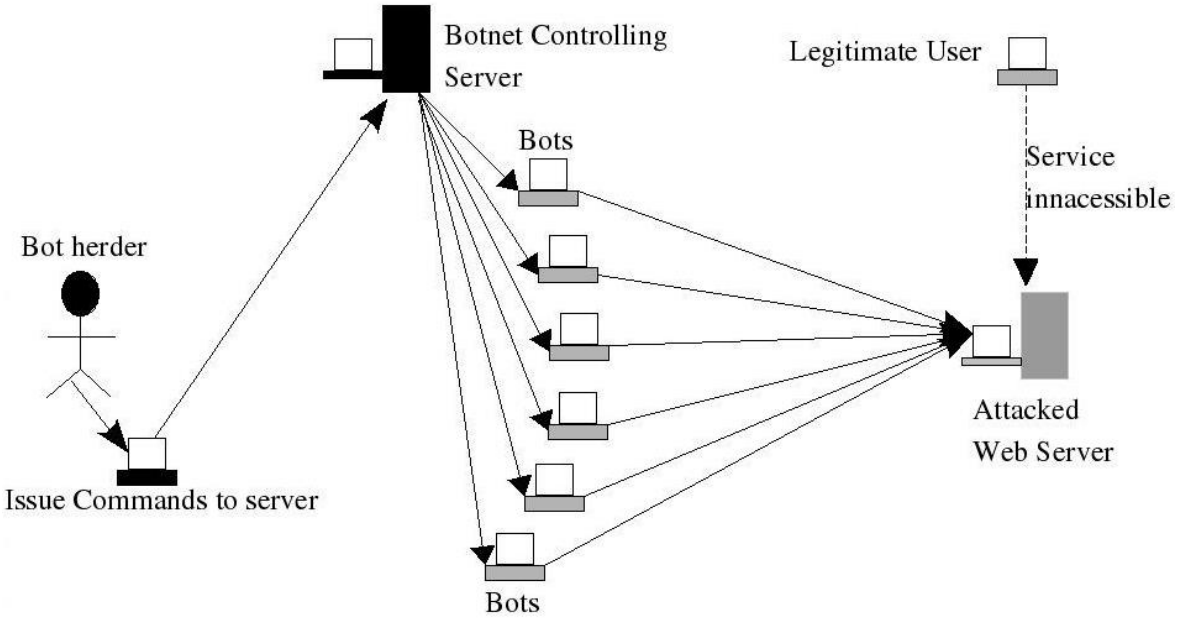
Zdroj: PC Magazine Encyclopedia. *Definition of: adware* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.pcmag.com/encyclopedia/term/37577/adware>.

Podstatou funkce adwaru je stahování reklamních materiálů a jejich následné nabízení uživateli ve formě vyskakujících oken nebo přesměrováváním na určité internetové stránky, což může být pro uživatele obtěžující. Tímto způsobem si výrobce programu, ke kterému je adware přibalen, zajišťuje příjmy z reklam. Adware je v podstatě cenou za to, že je možno freewarový program používat.

6. Bot

Bot je program, který ovládne napadený počítač a vytvoří z něj tzv. „zombie“. Pomocí takto vytvořeného vzdáleného přístupu může útočník vykonávat jakékoliv operace na napadeném počítači a nainstalovat do něj jak další škodlivé programy, tak například tímto způsobem oblíbené rozesílání nevyžádané pošty. Také může útočník vytvořit celou síť zombií, tzv. **botnet**.

Obrázek č. 7: Botnet



Zdroj: TopTenREVIEWS. *Botnet Zombie Apocalypse: How to Protect Your Computer* [online]. [cit. 2015-01-10]. Dostupné na www: <http://mac-internet-security-software-review.toptenreviews.com/how-do-i-know-if-my-computer-is-a-botnet-zombie-.html>.

7. Časovaná bomba

Časovaná bomba je škodlivý program, který je obvykle nainstalován nějakým uživatelem nebo správcem sítě do systému. Dále pak tento program čeká na určitý spouštěcí signál, kterým může být např. přihlášení do systému, určitá hodina nebo datum apod. Poté spustí škodlivou činnost, ke které byl naprogramován – obvykle destrukční.

Časované bomby bývají často instalovány ve firemních počítačích jako odvetná akce za rozpory se zaměstnavatelem, které skončily ukončením pracovního poměru zaměstnance.

Škody bývají o to horší, že takovýto útok není očekáván a navíc je útočník osoba znalá systému a dokáže zacílit na slabá místa.

Časovaná bomba se však může dostat i do domácího počítače, ať už propašována s nějakým virem, nebo „kamarádem“. V těchto případech bývají následky fatální, vzhledem k úrovni znalostí, schopností a možností se se škodami vypořádat.

8. Phishing a Pharming

Phishing a pharming patří do kategorie tzv. sociálního inženýrství, které využívá slabin uživatele nebo jeho dobrosrdečné povahy. Obě metody mají za cíl získat citlivá data uživatele, jako je např. přístupové jméno a heslo do internetového bankovnictví či jiných platebních brán.

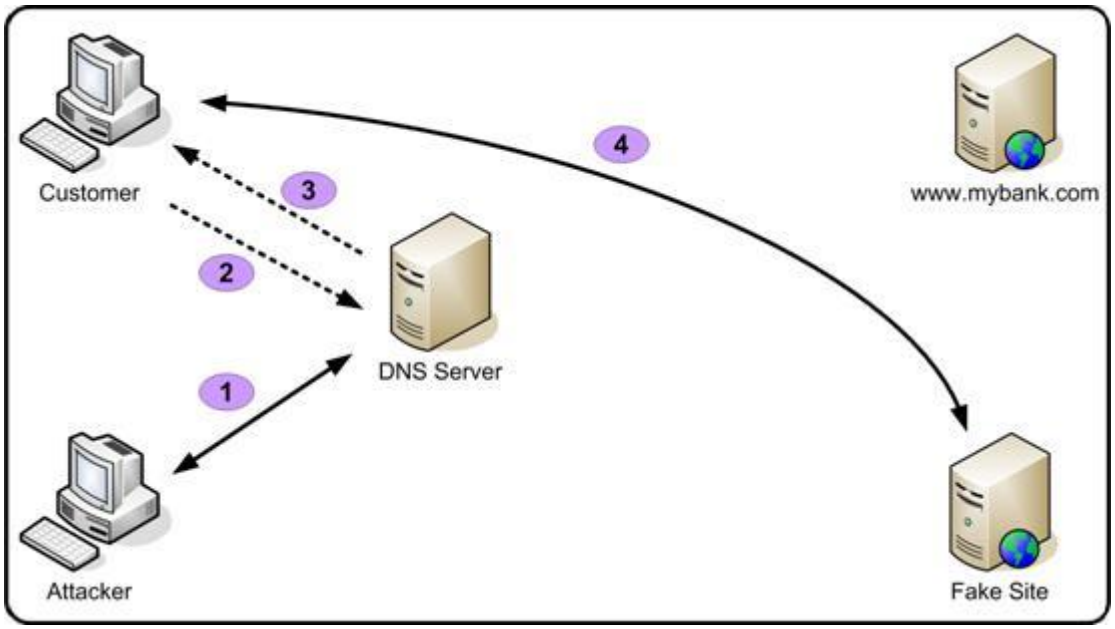
Phishing k tomu používá obvykle emailovou zprávu, ve které přiměje uživatele, aby se přihlásil do internetového bankovnictví nebo do platební brány přes přiložený odkaz ve zprávě. Tento odkaz ale nevede skutečně na internetové bankovnictví nebo platební bránu, ale na stránku útočníka, která je imitací původně odkazované stránky. Uživatel tak nic nepozná a zadá svoje přístupové jméno a heslo, čímž je sdělí útočníkovi. Do svého účtu se však nedostane, naopak toho rychle využije útočník a přes získané údaje se přihlásí do skutečného internetového bankovnictví či platební brány.

Obrázek č. 8: Phishing

Zdroj: DataProtectionCenter.com. *Phishing – going the extra mile (with virtual keyboard)* [online]. 2011-05-19 [cit. 2015-01-10]. Dostupné na www: >http://dataprotectioncenter.com/security/phishing-going-the-extra-mile-with-virtual-keyboard/>.

Pharming je sofistikovanější variantou phishingu. K získání přihlašovacích údajů uživatele také přesměrovává na vlastní upravenou stránku - kombinací podvržení falešné stránky a zároveň přepsání falešné adresy v prohlížeči. Toho dosáhne pomocí útoku na DNS server. Tato metoda je velmi nebezpečná, protože uživatel nemá možnost nijak poznat, že byl přesměrován.

Obrázek č. 9: Pharming



Zdroj: Technical Info. *The Pharming Guide* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.technicalinfo.net/papers/Pharming2.html>.

3.4. Ochrana před hrozbami

Ochranu před hrozbami, vnitřními i vnějšími, je možno rozdělit na ochranu **pasivní** a **aktivní**. Pasivní ochrana působí preventivně a jejím úkolem je předcházet vzniku rizik. Aktivní ochrana má naopak za úkol „zachraňovat“ situaci např. při útoku.

3.4.1. Ochrana před vnitřními hrozbami

3.4.1.1. Zálohování

Základní a také nejdůležitější ochranou před hrozbami technické, softwarové i uživatelské povahy, je **zálohování**.

Zálohováním rozumíme vytvoření kopie důležitých, případně všech dat a jejich uložení na bezpečné místo.

Takové místo je obvykle mimo počítač, ze kterého data zálohujeme. Jedná se především o:

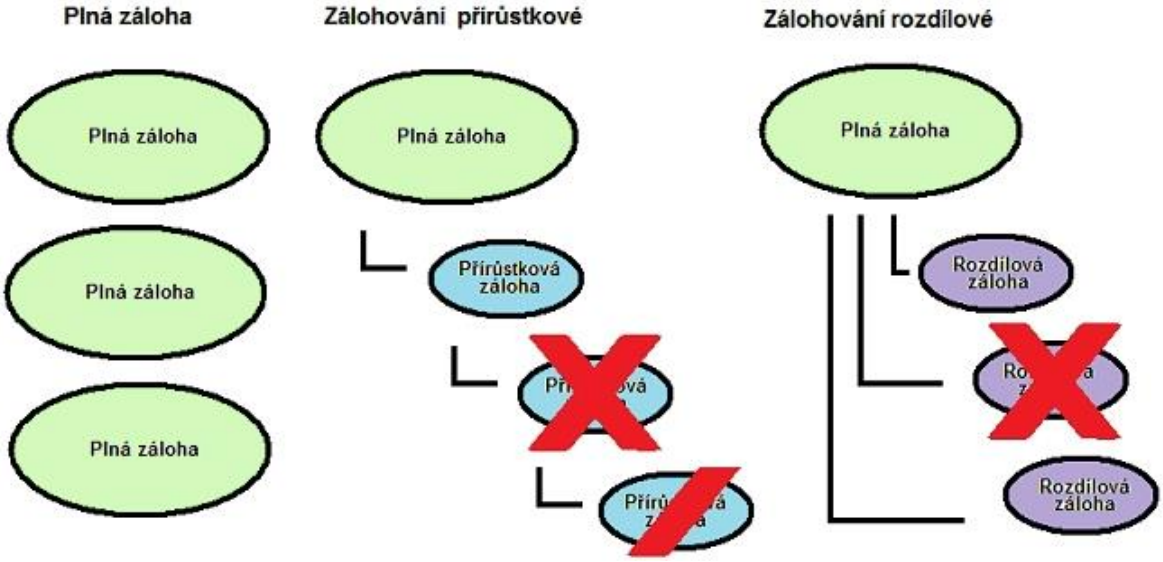
- **optické zapisovací disky** - v současnosti nejlevnější a nejbezpečnější zálohovací médium představují (jednou) zapisovatelné optické disky DVD. Důvodem je dostupnost zapisovacích mechanik – dodávají se prakticky do každého stolního počítače i notebooku. Také cena samotných prázdných DVD médií je velmi příznivá. Kapacita je pro zálohu důležitých dat také stále dostatečná, stejně jako životnost médií. V poslední době dochází k rozšíření Blu-Ray zapisovacích mechanik a zálohování na optická média se tak dostává na vyšší úroveň, protože kapacita dosahuje 25-50GB, což umožňuje zálohování poměrně velkého množství dat na jeden Blu-Ray disk. Nevýhodou je ale jejich cena, která je oproti diskům DVD několikanásobná. Naopak nejlevnější varianta zálohování na optické disky je u CD disků, která je však vykoupena nízkou kapacitou a postačuje prakticky jen na zálohování dokumentů;
- **externí pevné disky** – pro domácí použití jsou oblíbené disky připojitelné přes rozhraní USB, kterým je vybaven každý počítač. Výhodou je snadné používání a velká kapacita. Mezi výhody také bývá uváděna dobrá přenositelnost, ovšem to může být také nevýhoda – při přenášení a připojování do jiných systémů může dojít ke ztrátě dat nebo k infiltraci;
- **externí zálohovací systémy** – v domácnostech stále oblíbenější systémy, které se nazývají „NAS“ nebo „domácí cloudové úložiště“. Jde v podstatě o malý počítač připojený do domácí sítě, který slouží k zálohování, ukládání a sdílení dat mezi všemi zařízeními v síti včetně domácího kina či TV, přičemž je k němu často možný i přístup přes síť internet. Samotné zálohování může být prováděno ručně, nebo díky přiloženému softwaru automaticky. Systém také umožňuje takové nastavení, při němž se stejná data ukládají na dva disky a tím je významně zvýšená bezpečnost dat v případě havárie disku. Nevýhodou je pořizovací cena takového systému, která je násobkem ceny externího disku.

Zálohování v domácnostech je možno provádět nepravidelně (nahodile), nebo pravidelně. K pravidelné záloze může posloužit buď samotný operační systém, nebo

specializovaný software dodávaný k externím diskům nebo zálohovacím systémům. V případě pravidelné zálohy je také možné nastavit zálohování na:

- **kompletní zálohu** – zálohuje se vždy celý systém. Největší výhodou je rychlá a kompletní obnova všech dat v případě selhání systému nebo pevného disku. Je však potřeba počítat s tím, že bude během zálohy výrazně zatížen zálohovaný systém a také bude potřeba velká kapacita;
- **přírůstkovou zálohu** – zálohuje se celý systém a následně jen ta data, která byla změněna od předchozí zálohy. Výhodou je to, že přírůstkové zálohy zaberou jen malou kapacitu. Nevýhodou naopak je, že pro obnovení systému jsou potřeba všechny tyto přírůstkové zálohy, což je časově náročnější a navíc je zvýšené riziko, že při množství záložních souborů bude jeden z nich poškozen;
- **rozdílovou zálohu** – zálohuje se nejprve celý systém a poté vždy data, která byla změněna od této plné zálohy. Výhoda je opět v nízké potřebě kapacity pro zálohy, i když ne tolik, jako u přírůstkové zálohy. Při obnově dat je ale potřeba jen původní plná záloha a jedna rozdílová záloha (obvykle ta poslední), protože rozdílové zálohy jsou na sobě zcela nezávislé.

Obrázek č. 10: Typy zálohování



Zdroj: Acronis. *Inkrementální – přírůstková záloha* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.acronis.cz/kb/inkrementalni-zaloha/>.

3.4.1.2. Důslednost a ostražitost

Jakkoliv se to může zdát být samozřejmé, velmi důležitá je důslednost a ostražitost. Důslednost především v pravidelném zálohování, pokud je prováděno ručně, pravidelném aktualizování operačního systému, nastavením hesla do systému apod. Ostražitost je potřeba mít zejména na internetové síti tak, aby nebyl do počítače zavlečen nežádoucí software například z „neznámých" adres. Také je nutno mít se na pozoru před instalováním softwaru z neoriginálních zdrojů, ať už se jedná o přenosná média nebo internet.

3.4.1.3. Fyzická ochrana

Před hrozbami technické povahy je dobré počítač chránit fyzickým zabezpečením. Mezi tato zabezpečení patří:

- **nepřerušitelné zdroje napájení** (UPS) – chrání počítač před výpadkem elektrické energie. Jsou využitelné zejména pro stolní počítače, protože notebooky mají vlastní baterii. Ačkoliv jsou schopné dodávat elektrickou energii řádově jen několik minut, je to dostatečná doba na to, aby byla všechna práce uložena a počítač byl řádně vypnut. Tím se předejde ztrátě neuložených dat a možné havárii některé součásti počítače v důsledku nekorektního vypnutí;
- **přepěťové ochrany –** v dnešní době levná ochrana počítače před přepětím v rozvodné elektrické síti. Standardní přepěťové ochrany jsou schopny ochránit počítač a jeho periferie, které jsou k ochraně připojeny. Lepší ochrany dokáží ochránit před přepětím i síť LAN, telefonní přípojku, anténní přípojku, nebo odpojovat zařízení z důvodu elektrické energie;
    - **umístěním počítače** – vliv na životnost hardwarového vybavení má i to, pokud je počítač umístěn na zemi nebo jiném prašném místě. Stejně tak je vhodné mít počítač umístěný na alespoň trochu vyvýšeném místě z důvodu možného vytopení, které by mělo pro počítač zcela jistě fatální následky. Také by měl být počítač umístěn na místě s dostatečným prouděním vzduchu, aby se zamezilo jeho přehřívání.

3.4.2. Ochrana před vnějšími hrozbami

Jako vnější hrozby byla definována **krádež** počítače či jeho příslušenství a **infiltrace**.

Ochrana před krádeží spočívá v umístění počítače tak, aby bylo co nejobtížnější jeho odcizení. To znamená vyvarovat se jeho umístění tak, aby byl přímo viditelný a dosažitelný např. při otevřeném okně apod. Také je možno samotný počítač zamykat – některé počítačové skříně a monitory jsou pro to vybaveny, stejně jako jsou prakticky všechny notebooky osazeny přípravou pro uzamykací systém „Kensington lock“.

Obrázek č. 11: Uzamykací systém pro notebooky

Zdroj: Travel Stack Exchange. *Traveling with a laptop* [online]. [cit. 2015-01-10]. Dostupné na www: <http://travel.stackexchange.com/questions/10206/travelling-with-a-laptop/>.

Ochrana před infiltrací spočívá jak v používání originálního a pravidelně aktualizovaného operačního systému a ostatního softwaru, tak i v používání různých ochran počítače, jako je **firewall**, **antivirový software** a **antispyware**.

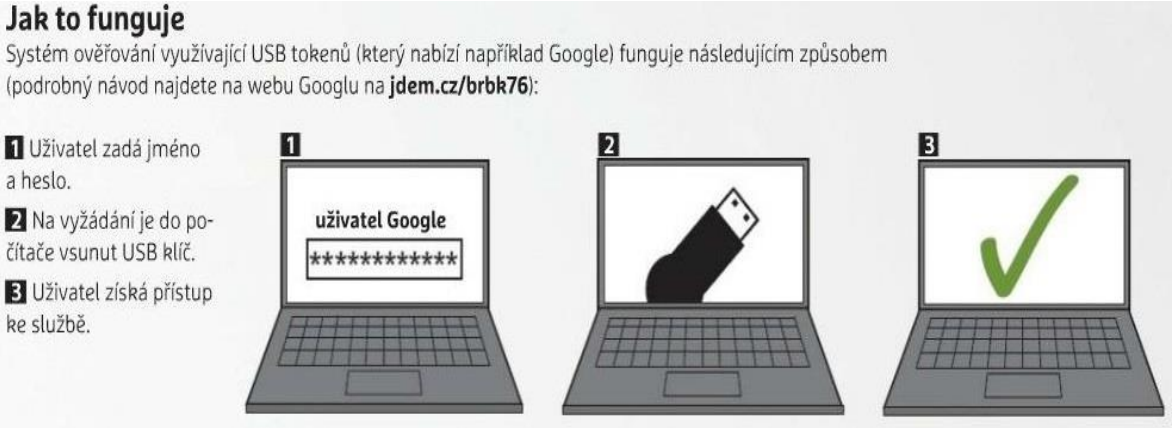
3.4.2.1. Operační systém

Jako první krok v ochraně před počítačovou infiltrací je považováno používání originálního operačního systému. Takový systém nabízí v první řadě záruku „čistoty“ instalovaného operačního systému, dále pak jeho pravidelnou aktualizaci včetně záplatování zjištěných bezpečnostních mezer. Neoriginální operační systém sice lze provozovat i s pravidelnými aktualizacemi, avšak riziko infiltrace nastává už při instalaci

samotného operačního systému a trvá po celou dobu jeho používání, neboť je z důvodu odstranění kontroly originality změněna jeho zdrojová část.

Dále je nutné takové zabezpečení operačního systému, aby se do něj nemohl dostat jakýkoliv uživatel (útočník) a nemohl tak provádět neoprávněnou činnost. Základní ochranou je nastavení hesla (autentizace) pro přihlášení do operačního systému. Další možností je tzv. dvoufaktorová autentizace. „*Dvoufaktorová autentizace (2FAS) zajišťuje, že i pokud vám hacker ukradne heslo, nezpůsobí vám to žádné problémy. V rámci tohoto systému se totiž uživatel vždy musí identifikovat skrz dva nezávislé kanály – kromě hesla to může být např. USB klíč.*“[21] První faktor je tedy něco, „co uživatel ví“ (např. jméno a heslo, tel. číslo apod.) a druhý faktor je něco, „co uživatel má“ (např. USB klíč, otisk prstu, mobilní telefon apod.). Takové zabezpečení je používáno např. v oblasti internetového bankovnictví, je ale možné jej použít i pro přístup k operačnímu systému, přihlášení do sítě apod.

Obrázek č. 12: Funkce dvoufaktorové autentizace



Zdroj: HELD, Njels, KRATOCHVÍL, Petr. Dvojitá je lepší. *CHIP 02/2015*, s. 36.

3.4.2.2. Firewall

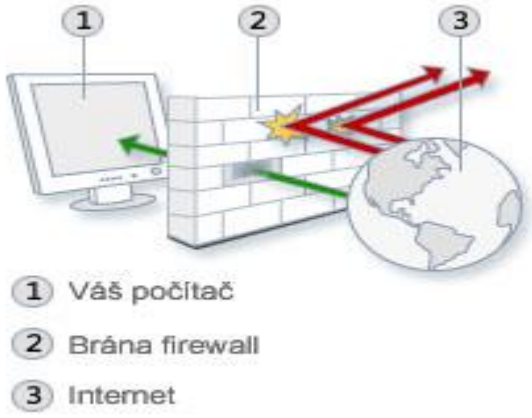
„*Firewall je **nástroj**, jenž **odděluje chráněnou síť od nechráněné** (nebo chráněnou část sítě od nechráněné části) a nabízí základní zabezpečení systému při připojení k internetu.*

[21] HELD, Njels, KRATOCHVÍL, Petr. Dvojitá je lepší. *CHIP 02/2015*, s. 36.

K tomuto účelu může firewall používat ***kombinaci programového i technického vybavení.***“[22]

Brána firewall hlídá veškerou komunikaci z počítače do internetu, případně ze zabezpečené sítě do nezabezpečené, a zároveň veškerou komunikaci opačným směrem. Brána má nastaveno, jaká komunikace je povolena a jakým programem. V případě, že detekuje jakoukoliv jinou komunikaci, tak ji nepovolí a dotáže se uživatele či administrátora, jak s touto komunikací naložit. Obvykle jsou na výběr možnosti **povolit**, **povolit trvale** či **zablokovat**.

Obrázek č. 13: Firewall



Zdroj: Microsoft. *Co je brána firewall?* [online]. [cit. 2015-01-10]. Dostupné na www: <http://windows.microsoft.com/cs-cz/windows/what-is-firewall#1TC=windows-7/>.

Firewall může být buď hardwarový jako samostatné zařízení, nebo softwarový v podobě programu.

Hardwarový firewall je v domácnostech využíván převážně v routerech, ve kterých bývá standardně integrován. Takový firewall však bohužel nenabízí všechny funkce, ale jako základní ochrana je dostatečný, např. jako ochrana proti DoS útokům a proti útočníkům využívajícím standardní protokoly. Firewally, které obsahují lepší výbavu proti schopnějším útočníkům, jsou nepoměrně dražší a zejména složitější na administraci, proto jsou používány v podnicích.

[22] KRÁL, M., *Bezpečnost domácího počítače*, s. 153-154

Softwarový firewall je např. aplikace integrovaná do samotného operačního systému, v případě produktů firmy Microsoft jde o „Bránu firewall systému Windows“. Nabízí základní ochranu počítače a jednoduché nastavení. Výhodou je také to, že je integrovaná do systému Windows (od verze Windows XP) a uživatel nemusí shánět a instalovat žádný další program. Bohužel však nenabízí komplexní ochranu, kterou nabízejí výrobci třetích stran zdarma, nebo za úplatu. Instalaci a nastavení takových firewallů zvládnou i mírně pokročilí uživatelé.

3.4.2.3. Antivirový software

Antivirový software detekuje hrozby ve formě virů. Princip funkce je založen na **monitorování podezřelých činností**, které jsou typicky vyvolávány některým virem, a na **vyhledávání virů** v počítači.

Pro funkci monitorování podezřelých činností je v paměti počítače zaveden program, který jakoukoliv podezřelou činnost, jako je např. nepovolený zápis na disk či formátování disku, zablokuje. Pokud je zjištěno, že takovou činnost provedl již známý vir, obvykle ho smaže nebo uloží do „trezoru“[23], odkud již nemůže páchat škody a oznámí to hlášením uživateli. V případě neznámých podezřelých programů je uživatel vyzván k další akci.

Funkce vyhledávání virů je založena na skenování operační paměti a souborů v počítači, heurestické analýze či kontrole integrity. Nalezené známé viry jsou také buď smazány, nebo uloženy do „trezoru“, neznámé podezřelé soubory jsou dány do karantény a uživatel je vyzván k další akci. Samotné vyhledávání virů může být prováděno ručně uživatelem, nebo může být nastaveno automaticky.

Antivirový program může uživatel získat, stejně jako v případě firewallu, také společně s operačním systémem, nebo jako samostatný komerční program. V případě operačního systému Microsoft Windows je jako součást operačního systému nabízen antivirový program Microsoft Windows Defender, který je ovšem jeden z nejslabších. Mnohem lepší alternativou je použití některého z komerčních antivirových programů, které nabízejí lepší zabezpečení, více funkcí a uživatelskou přívětivost.

[23] Trezor je zabezpečené místo na disku, ze kterého nemůže uložený soubor proniknout zpět do systému

3.4.2.4. AntiSpyware

AntiSpyware je program, který chrání počítač před spywarem a adwarem. Funguje podobně jako antivirový program – trvale monitoruje spyware a adware a také je vyhledává na disku počítače. Detekovanou nežádoucí činnost zablokuje a vyzve uživatele k další akci, případně původce rovnou odstraní.

Stejně jako v případě firewallu a antivirového programu je možné získat antispyware jako součást operačního systému (Microsoft Windows AntiSpyware) zdarma, ovšem stejně jako v případě firewallu a antivirového programu se jedná o jedno z nejslabších řešení. Opět je tak výhodnější sáhnout po komerčním řešení třetích stran.

4. Praktická část

4.1. Průzkum zaměřený na uživatele domácího PC

Cílem průzkumu bylo zjistit, k jakému účelu uživatelé domácí PC používají, jaké mají povědomí o možných hrozbách a jak se proti nim brání.

Otázky, na které by měl průzkum pomoci najít odpovědi, jsou:

- Používají uživatelé domácí počítač k účelům, které obecně zvyšují míru rizika infiltrace?
- Znají uživatelé domácího počítače software, který je může proti riziku infiltrace ochránit?
- Které druhy softwaru pro ochranu před vnějšími hrozbami používají uživatelé domácího počítače?
- Jsou si uživatelé domácího počítače vědomi, že zásadní vliv na bezpečnost počítače má samotný uživatel?
- Jsou si uživatelé domácího počítače vědomi, jaký má vliv na bezpečnost používání originálního softwaru?
- Jsou si uživatelé domácího počítače vědomi, jaké riziko představují různé uživatelské akce spojené s používání počítače?
- Jaké mají uživatelé domácího počítače povědomí o tom, že zálohování ochrání jejich data před ztrátou?
- Zálohují uživatelé domácího počítače důležitá data a jak často?
- Používají uživatelé domácího počítače ochranu před anomáliemi v elektrické síti?

4.1.1. Technika průzkumu

Technika zvolená pro průzkum byl **dotazník**.

Prvním krokem při tvorbě dotazníku bylo stanovení cíle, na který bude průzkum zaměřen. Poté byly položeny otázky, na které má výzkum odpovědět. V následujícím kroku byl sestaven samotný dotazník. Při samotném sestavování dotazníku bylo nutné brát v úvahu faktory, jako je jednoznačnost položených otázek a odpovědí, srozumitelnost otázek a odpovědí, stručnost otázek a také pokládat jen ty otázky, které jsou pro průzkum podstatné.

Dotazník byl sestaven celkem z patnácti otázek, přičemž hned první byla segmentační. Dále byly položeny otázky, na které bylo možné vybrat jednu nebo více odpovědí, a také otázky, které se větvily do dalších podotázek.

Z důvodu objektivity nebyla do dotazníku zahrnuta otázka „používáte nějaký nelegální software?“ Lze se totiž domnívat, že by taková otázka nebyla zodpovězena pravdivě, případně by respondenti ukončili vyplňování dotazníku.

4.1.2. Zkoumaný vzorek respondentů

Pro uvedený průzkum byli vybráni studenti České zemědělské univerzity a Vysoké školy ekonomie a managementu, současní a bývalí zaměstnanci Národní technické knihovny a také členové Calibra clubu Česká republika. Dotazník byl sestaven pomocí internetové služby Vyplňto a respondentům rozeslán elektronickou poštou.

Celkem se průzkumu zúčastnilo 213 respondentů různých věkových kategorií a různých skupin uživatelů, což dává dostatečný reprezentativní vzorek pro zajištění cílů průzkumu.

Dotazník byl zadán a rozeslán respondentům na konci roku 2014, trval celkem 14 dní a poté byl vyhodnocen.

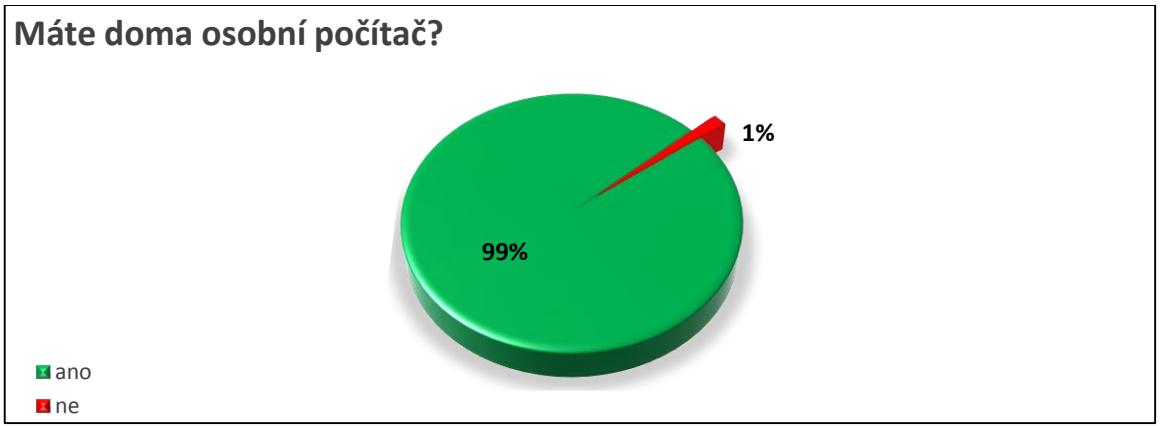
4.2. Vyhodnocení jednotlivých částí dotazníku

Otázka č. 1: Máte doma osobní počítač?

První otázka byla segmentační a respondenti měli na výběr dvě možnosti: ano či ne. V případě záporné odpovědi by dotazník ukončen, protože by respondent nemohl odpovědět na další otázky. V případě kladné odpovědi dotazník pokračoval dále a respondenti již odpovídali na všechny zbývající otázky.

Z odpovědí na tuto otázku bylo kladných celkem 210 odpovědí, zatímco záporné byly pouze 3 odpovědi. Cílem této otázky bylo zejména odfiltrovat ty uživatele počítače, kteří nemají osobní počítač přímo doma. Jak ale vyplývá z grafu č. 2, takových uživatelů je naprosté minimum.

Graf č. 2: podíl respondentů vlastnících domácí počítač



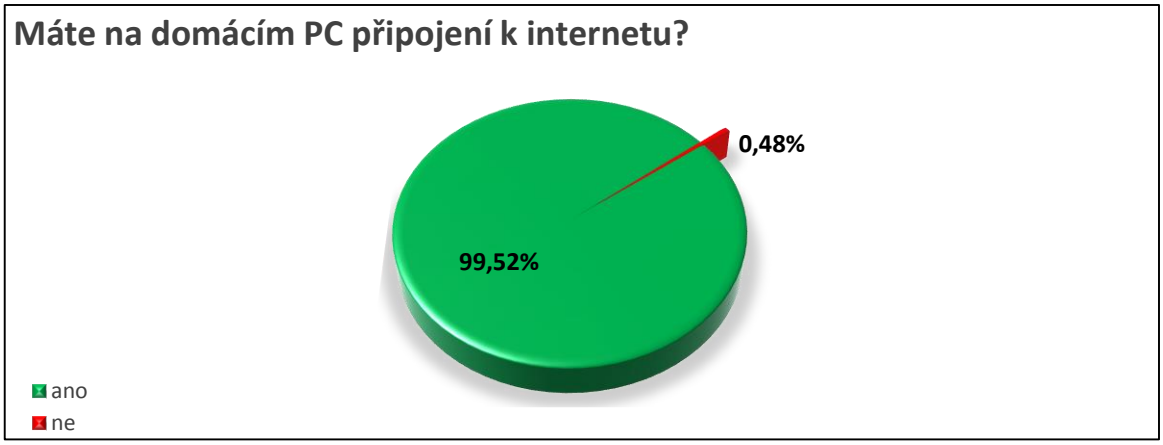
Zdroj: vlastní zpracování na základě výsledků dotazníku

Otázka č. 2: Máte na domácím PC připojení k internetu?

Druhé otázky se vzhledem k odpovědím na otázku předchozí zúčastnilo celkem 210 respondentů. Možné odpovědi byly opět pouze ano či ne, protože samotný typ internetového připojení nemá pro účely tohoto průzkumu prakticky žádný vliv. Cílem této otázky bylo zjistit, zda jsou uživatelé domácího počítače připojeni k internetu a zda jsou tedy vystaveni významně vyššímu riziku infiltrace oproti uživatelům bez internetového připojení.

Z odpovědí vyplynulo, že připojení má doma prakticky každý uživatel domácího počítače. Je tedy potřeba počítat s tím, že jsou téměř všichni uživatelé vystaveni hrozbám ve vysoké míře.

Graf č. 3: podíl respondentů s internetovým připojením



Zdroj: vlastní zpracování na základě výsledků dotazníku

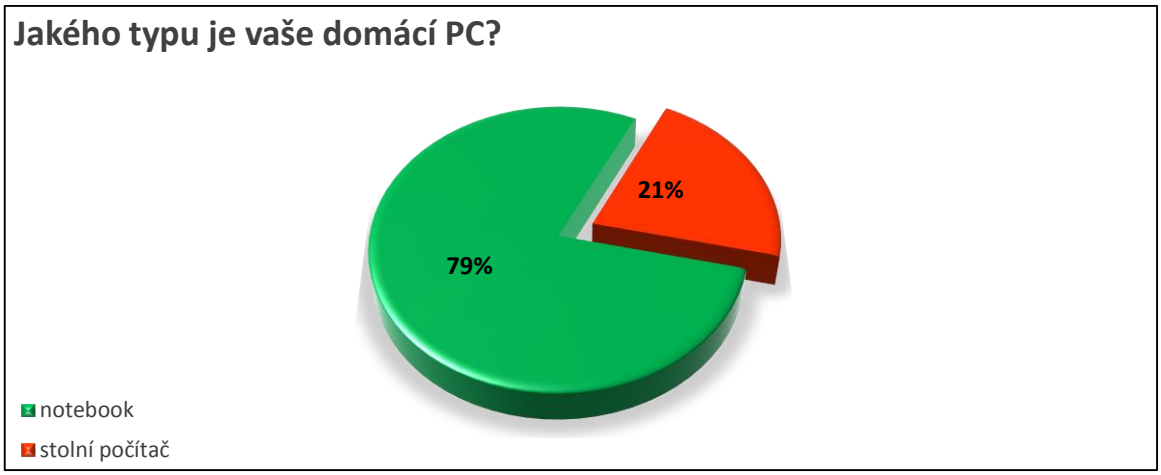
Otázka č. 3: Jakého typu je Vaše domácí PC?

Třetí otázka nabízela dvě možné odpovědi: stolní počítač nebo notebook. Cílem otázky bylo rozdělení respondentů na uživatele, kteří mohou být vystaveni riziku v ještě ve větší míře v případě vlastnictví notebooků. U přenosného počítače lze totiž očekávat, že bude používán mimo domov, a to i s připojením k internetu přes neznámou či nezabezpečenou síť. Také je u těchto uživatelů větší riziko ztráty či poškození počítače. Na druhou stranu jsou uživatelé vlastnící notebook jako domácí počítač lépe chráněni před anomáliemi v elektrické síti, protože mají jak nezávislý zdroj odolný proti přepětí, tak i záložní baterii více než nahrazující celou UPS.

Jak vyplynulo z odpovědí respondentů, stolní počítač dnes používá jen cca každý pátý uživatel domácího počítače. Je to jednak dáno poklesem ceny notebooků, ale také samotnými potřebami uživatelů.

V poznámce u otázky bylo uvedeno, že pokud vlastní respondent stolní počítač i notebook, bude do dotazníku zahrnut stolní počítač. Důvodem bylo to, že stolní počítače mají delší životnost oproti notebookům a nelze je (jednoduše) přenášet např. do práce a využívat i jinak, než jako domácí PC.

Graf č. 4: Rozdělení domácích počítačů podle typu



Zdroj: vlastní zpracování na základě výsledků dotazníku

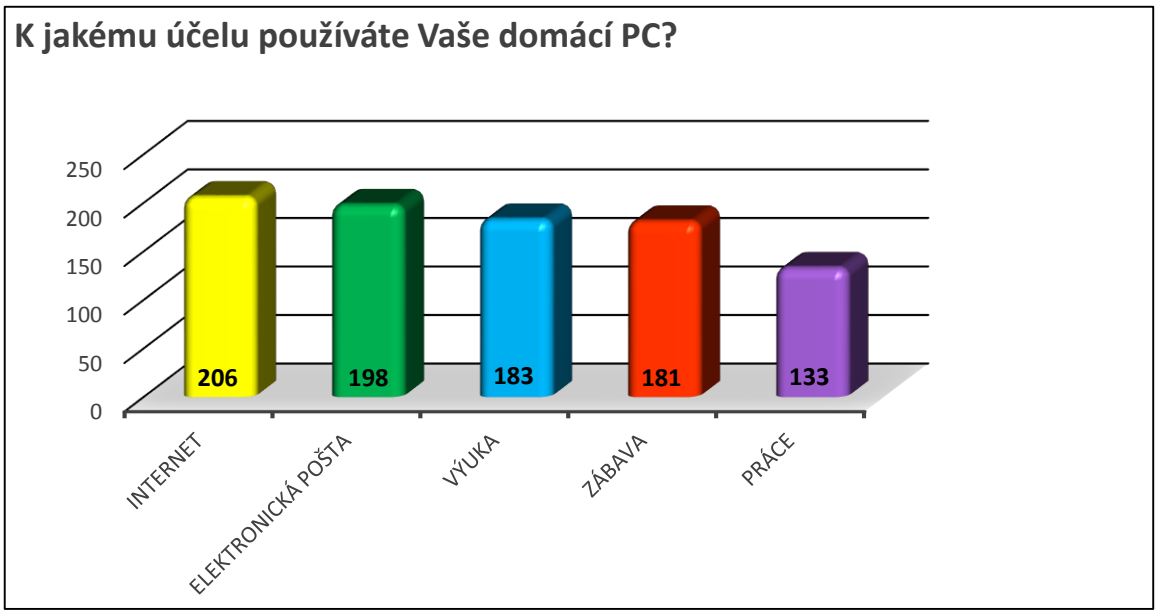
Otázka č. 4: K jakému účelu používáte Vaše domácí PC?

Na tuto otázku již bylo nabídnuto pět odpovědí: internet, elektronická pošta, výuka, zábava a práce. Respondenti mohli odpovědět na více otázek, nejméně však na jednu.

Cílem otázky bylo zjistit, k jakému konkrétnímu účelu je domácí počítač využíván a tím dojít k odpovědi, v jaké míře jsou vystaveni riziku infiltrace.

Výsledky odpovědí na tuto otázku vypovídají o tom, že téměř všichni uživatelé používají svůj počítač k procházení internetu a k elektronické poště, významné procento také k výuce a zábavě. Téměř dvě třetiny domácích počítačů jsou používány k pracovním účelům. Je tudíž patrné, že čelit hrozbám musí všichni uživatelé.

Graf č. 5: Účel použití domácího PC



Zdroj: vlastní zpracování na základě výsledků dotazníku

Otázka č. 5: Jaký typ softwaru na svém počítači používáte?

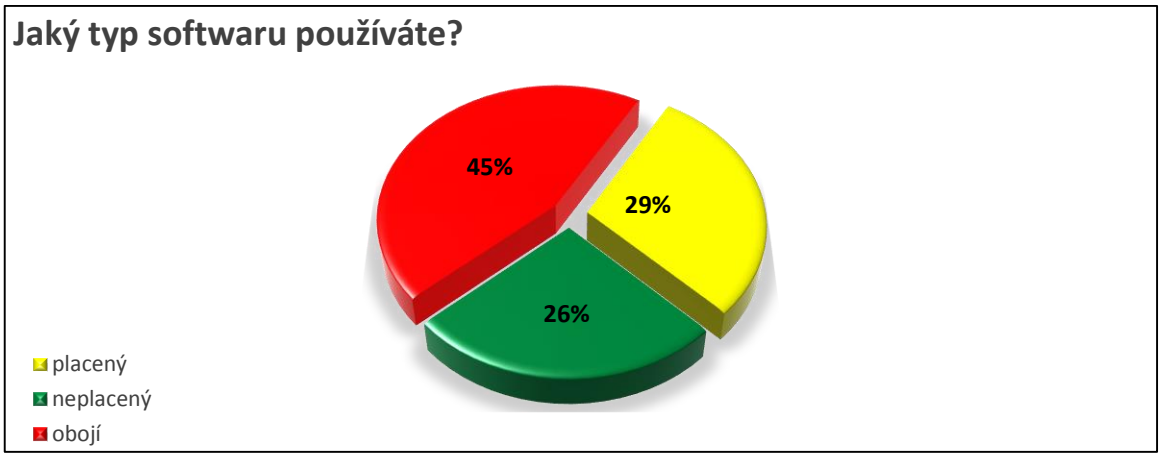
U páté otázky byla na výběr jedna ze tří odpovědí: placený, neplacený či obojí. Cílem této otázky bylo zjistit, v jaké míře je používán neplacený software, u kterého je vyšší riziko infiltrace.

Neplacený, neboli volně šiřitelný software (freeware), totiž často obsahuje spyware nebo adware a uživatel je tak ohrožen výrazně více, než uživatel používající placený software. U něj sice také nelze vyloučit nějakou formu malwaru, je to však výjimkou.

Také samotné získávání neplaceného softwaru může být nebezpečné, neboť ten se nachází často na stránkách, které mohou počítač infiltrovat.

Z odpovědí na tuto otázku vyplývá, že zhruba polovina respondentů používá neplacený software a je tak vystavena zvýšenému riziku infiltrace oproti druhé polovině, která takový software nepoužívá.

Graf č. 6: Používání softwaru podle typu licence



Zdroj: vlastní zpracování na základě výsledků dotazníku

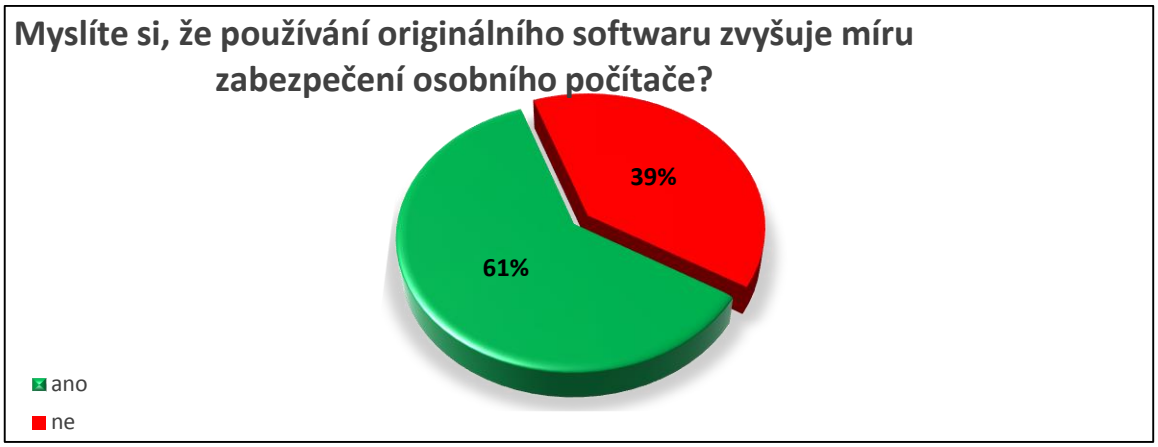
Otázka č. 6: Myslíte si, že používání originálního softwaru zvyšuje míru zabezpečení osobního počítače?

Na šestou otázku bylo možno odpovědět pouze **ano** či **ne**. Cílem otázky bylo zjistit, nakolik jsou si uživatelé počítače vědomi, že u neoriginální softwaru je vysoká míra rizika infiltrace.

Zvýšené riziko začíná již u neoriginálního operačního systému, kdy při jeho získání či instalaci může být počítač ohrožen, a pokračuje to uživatelským softwarem. Záruka toho, že při získání a používání softwaru nedojde k infiltraci, může být nabídnuta pouze u originálního softwaru.

Z odpovědí na tuto otázku si však poměrně překvapivě dvě pětiny respondentů nemyslí, že tomu tak je. Důvodem k tomuto přesvědčení může být například neznalost, nebo právě používání nelegálního softwaru.

Graf č. 7: Povědomí o bezpečnosti a používání originálního softwaru



Zdroj: vlastní zpracování na základě výsledků dotazníku

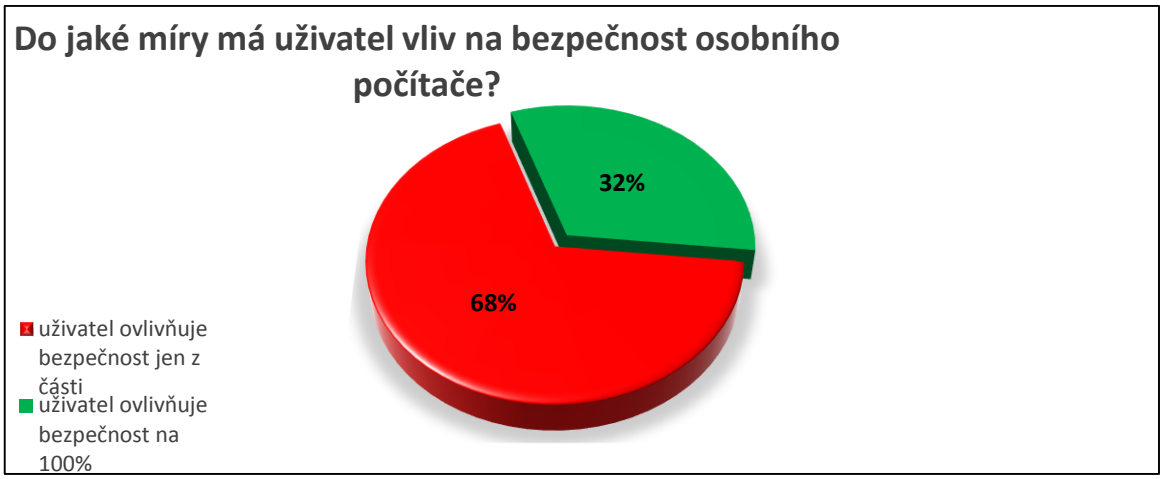
Otázka č. 7: Do jaké míry má uživatel vliv na bezpečnost osobního počítače?

U této otázky byly na výběr dvě odpovědi: uživatel ovlivňuje bezpečnost počítače jen z části, nebo na 100%. Cílem bylo zjistit, jaké povědomí mají uživatelé počítače o tom, jak hrozby fungují.

Infiltrace totiž může být v počítači pouze tehdy, když ji uživatel spustí nebo povolí. To se může stát i nevědomě nebo kvůli neznalosti, v každém případě je to ale „vina“ uživatele. Stejně tak uživatel ovlivní používání softwaru, který počítač chrání proti infiltraci a je to zase jen na něm. Podobná situace je u ochrany počítače před vnitřními hrozbami, kdy je opět jen na uživateli, zda a případně jaké opatření přijme.

Z odpovědí na tuto otázku vyplývá, že většina uživatelů si myslí, že má uživatel vliv na bezpečnost jen částečný.

Graf č. 8: Názor na vliv uživatele v oblasti bezpečnosti počítače



Zdroj: vlastní zpracování na základě výsledků dotazníku

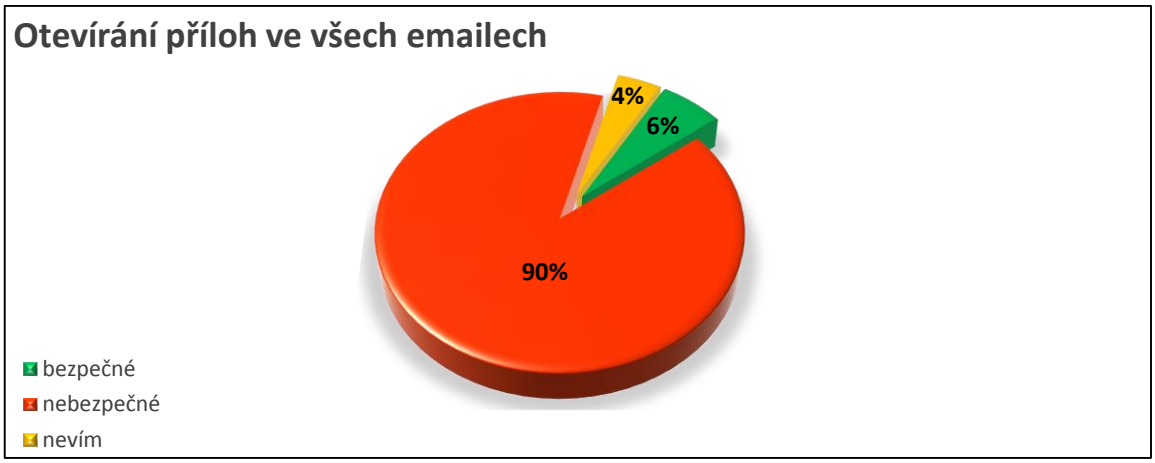
Otázka č. 8: u následujících otázek určete, která uživatelská akce je bezpečná či nikoliv:

1. otevírání příloh ve všech emailech;
2. okamžité potvrzení různých upozorňujících hlášení bez jejich přečtení nebo pochopení;
3. používání mnoha oken či programů najednou;
4. hraní počítačových her;
5. návštěvy zahraničních internetových stránek s erotickou tématikou;
6. přihlášení do internetového bankovnictví přes odkaz z emailu;
7. kopírování nebo instalace softwaru z neznámých médií (CD, DVD, USB);
8. zapnutí automatických aktualizací operačního systému;
9. dočasné vypnutí antiviru nebo firewallu.

U každé podotázky bylo možné zvolit jedu z odpovědí: **bezpečné**, **nebezpečné** či **nevím**. Cílem této otázky bylo zjistit, zda jsou si uživatelé počítače vědomi rizik spojených s určitou činností.

U první podotázky byla velká většina (89,5%) odpovědí „nebezpečné“. To se může zdát jako velké procento uživatelů, ovšem to, že 4,2% respondentů neví a 6,2% respondentů to dokonce pokládá za bezpečné, je dobrou zprávou pro útočníky, protože se stále najde dostatečný počet uživatelů, ke kterým se mohou infiltrovat.

Graf č. 9: Otevírání příloh ve všech emailech



Zdroj: vlastní zpracování na základě výsledků dotazníku

Druhá podotázka dopadla velmi podobně jako první, pouze se prohodil poměr mezi těmi, kteří nevědí (6,7%) a těmi, kteří to považují za bezpečné (4,3%). Výsledek je také relativně dobrý, stále se ale najde dostatečné množství uživatelů, kteří klidně odkliknou spuštění malwaru.

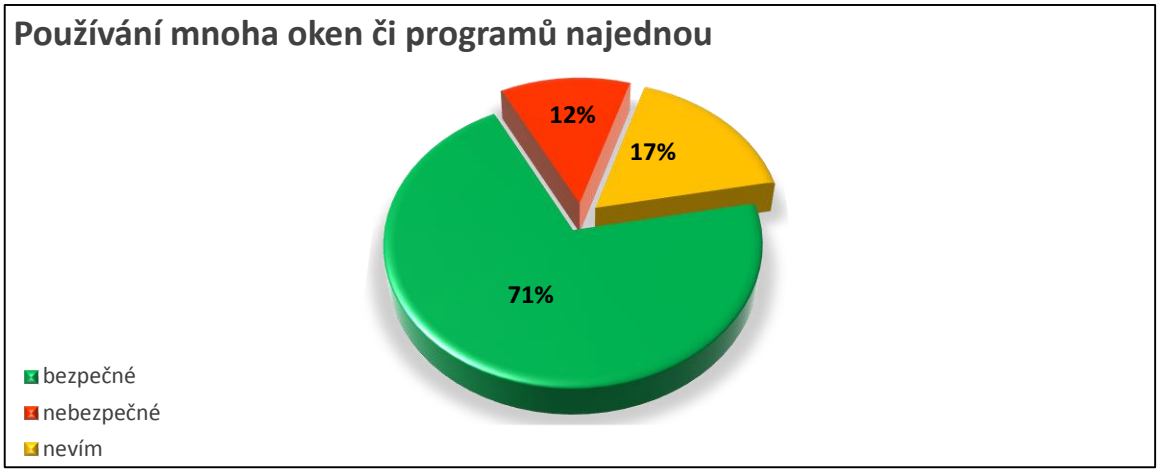
Graf č. 10: Okamžité potvrzení různých upozorňujících hlášení

Zdroj: vlastní zpracování na základě výsledků dotazníku

Třetí podotázka byla zodpovězena většinou (70,5%) jako „bezpečná“. Jako nebezpečnou činnost to považovalo 12,4% respondentů a 17,1% respondentů uvedlo, že neví. Při chodu mnoha programů a otevřených oknech se může stát, že uživatel v této záplavě přehlédne infiltraci či potvrdí její spuštění. Také je možné, že nějaký spuštěný

program koná nekalou činnost a proto je doporučeno zavřít především komunikační programy, např. Skype apod. Z odpovědí vyplývá, že většina uživatelů dává přednost opatrnosti, případně dostatečné rychlosti odezvy počítače.

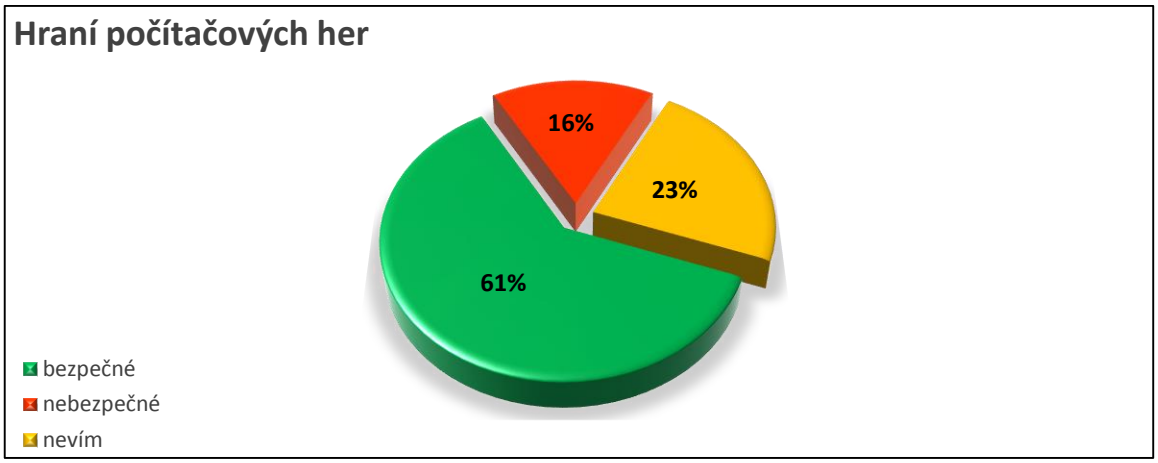
Graf č. 11: Používání mnoha oken či programů najednou



Zdroj: vlastní zpracování na základě výsledků dotazníku

Čtvrtou podotázku zodpovědělo 61% respondentů jako „bezpečnou“, 15,7% respondentů jako nebezpečnou a 23,3% respondentů odpovědělo, že neví. Obecně lze říci, že hraní počítačových her nemá vliv na bezpečnost počítače. Podmínkou je ale použití originálních her. V poslední době se rozšiřují také hry hrané ve webovém prohlížeči či hry „zdarma“, ke kterým je možno následně přikupovat bonusy za peníze. Takové hry mohou být pro počítač hrozbou, neboť jejich získávání může být rizikové, podobně jako u jiného neplaceného softwaru. Z odpovědí tak vyplývá, že poměrně velká část (39%) respondentů o hraní počítačových her nemá dostatek informací.

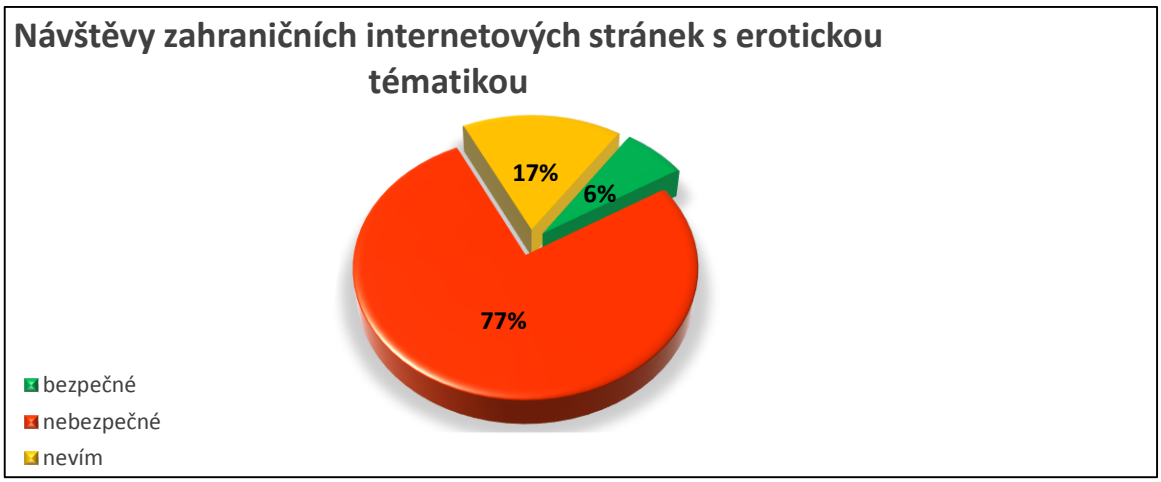
Graf č. 12: Hraní počítačových her



Zdroj: vlastní zpracování na základě výsledků dotazníku

Pátá podotázka byla lehce choulostivější, nicméně vzhledem k zaměření častého cíle útočníků zcela relevantní. Vzhledem k tématice na uvedených stránkách je často nutno mít snížené zabezpečení internetového prohlížeče a riziko infiltrace je tak výrazně větší. Toho využívají právě útočníci a často takové stránky využívají k útokům. Jedná se zejména o spyware a malware, ale ani počítačové viry rozhodně nejsou výjimkou. Jak ovšem vyplývá z odpovědí na tuto otázku, za nebezpečné to považuje jen 76,7% respondentů a 6,7% respondentů to přímo považuje za bezpečné.

Graf č. 13: Návštěvy zahraničních stránek s erotickou tématikou



Zdroj: vlastní zpracování na základě výsledků dotazníku

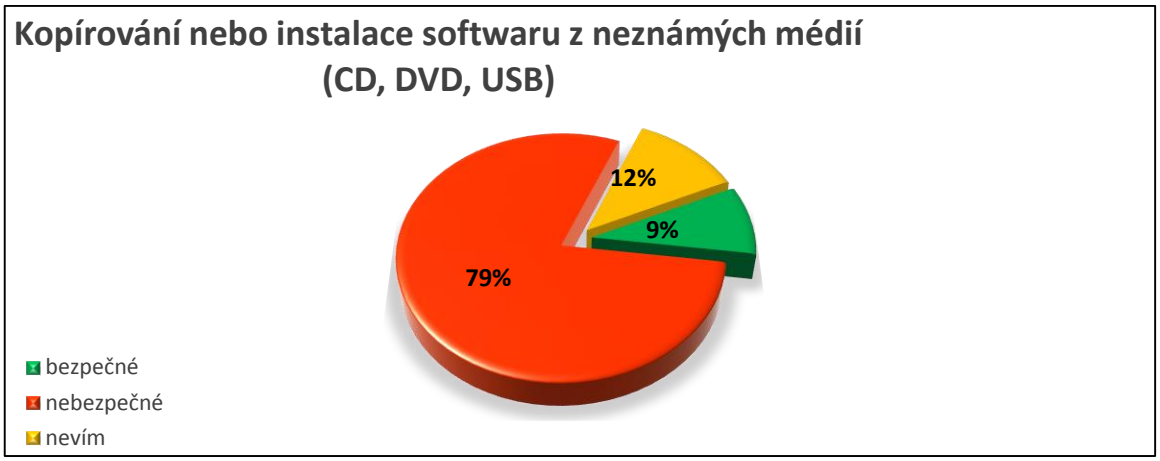
Šestá podotázka byla zaměřena na přihlašování do internetového bankovnictví přes odkaz v emailu. Z tohoto pohledu „pouhých“ 84,8% respondentů odpovědělo, že je takové přihlášení nebezpečné, naopak jako bezpečné odpovědělo 5,7% respondentů. Z odpovědí vyplývá, že z celkového vzorku respondentů by 12 z nich bylo vystaveno přímé hrozbě vytunelování jejich bankovního účtu, což není moc optimistický výsledek. Dalších 20 respondentů, kteří odpověděli, že neví, by (snad) u své banky zjišťovalo více informací.

Graf č. 14: Přihlášení do internetového bankovnictví

Zdroj: vlastní zpracování na základě výsledků dotazníku

Sedmá podotázka směřovala k tomu, zda jsou si uživatelé vědomi hrozby při používání neznámých médií. Na takových médiích, jako je CD, DVD nebo USB, může být skryta hrozba např. ve formě počítačového viru nebo spywaru. Za nebezpečné to označilo 79% respondentů, za bezpečné pak 9% respondentů. Zbytek odpověděl, že neví.

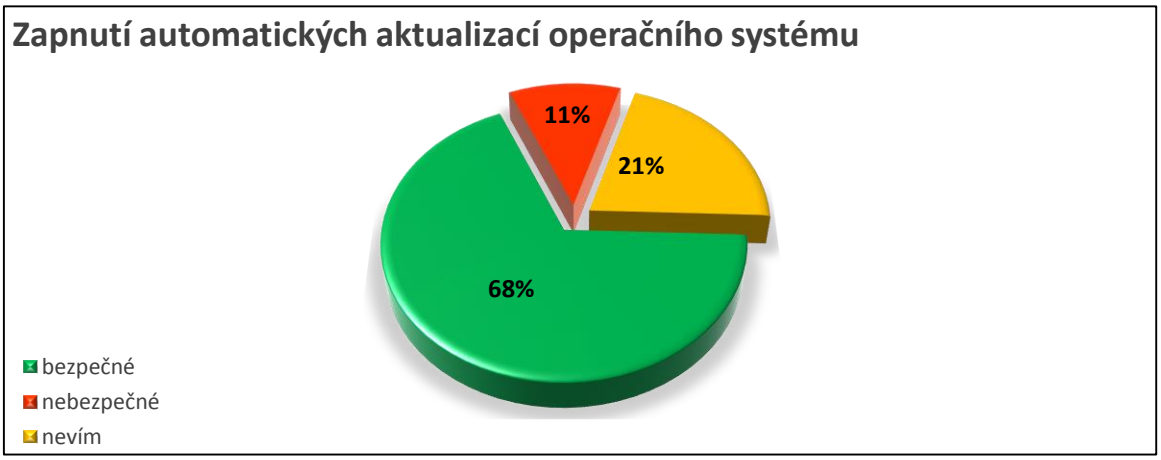
Graf č. 15: Kopírování nebo instalace softwaru z neznámých médií



Zdroj: vlastní zpracování na základě výsledků dotazníku

Osmou podotázku zodpovědělo jako bezpečnou jen 68,1% respondentů, což není příliš velké procento vzhledem k tomu, jak je tato činnost pro bezpečnost operačního systému důležitá. Dokonce jako nebezpečné to označilo 11% respondentů, zbytek označil odpověď „nevím“.

Graf č. 16: Zapnutí automatických aktualizací operačního systému

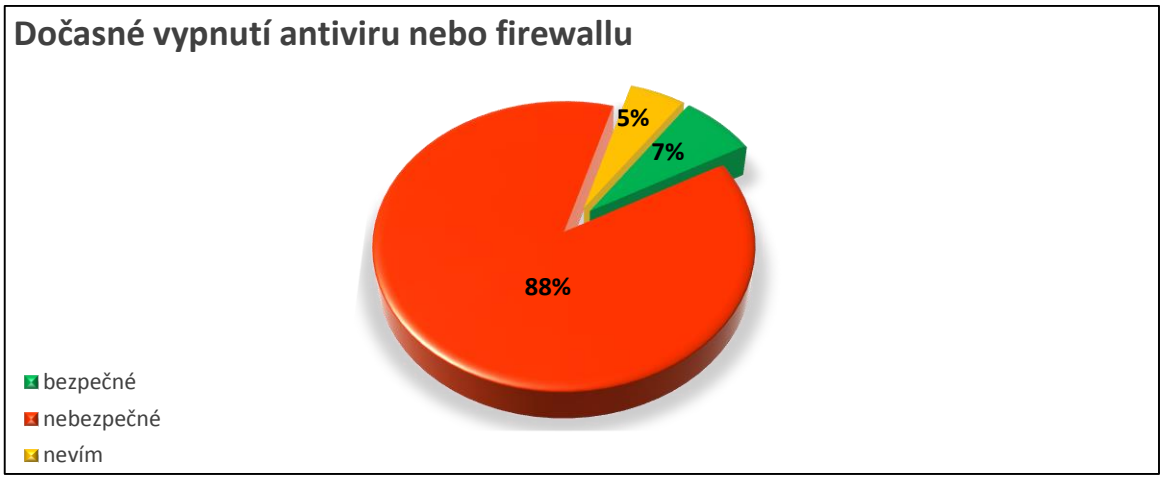


Zdroj: vlastní zpracování na základě výsledků dotazníku

Devátou podotázku, která se ptala na dočasné vyřazení firewallu nebo antiviru z provozu, zodpovědělo celkem 87,6% respondentů jako nebezpečnou, naopak 7,1% respondentů si myslí, že je taková činnost bezpečná. Z odpovědí tedy vyplývá, že výrazná

většina respondentů má povědomí o tom, jaké hrozby může přinést vyřazení zabezpečení. Bohužel 15 respondentů by bez tohoto povědomí bylo vystaveno hrozbě infiltrace.

Graf č. 17: Dočasné vypnutí antiviru nebo firewallu

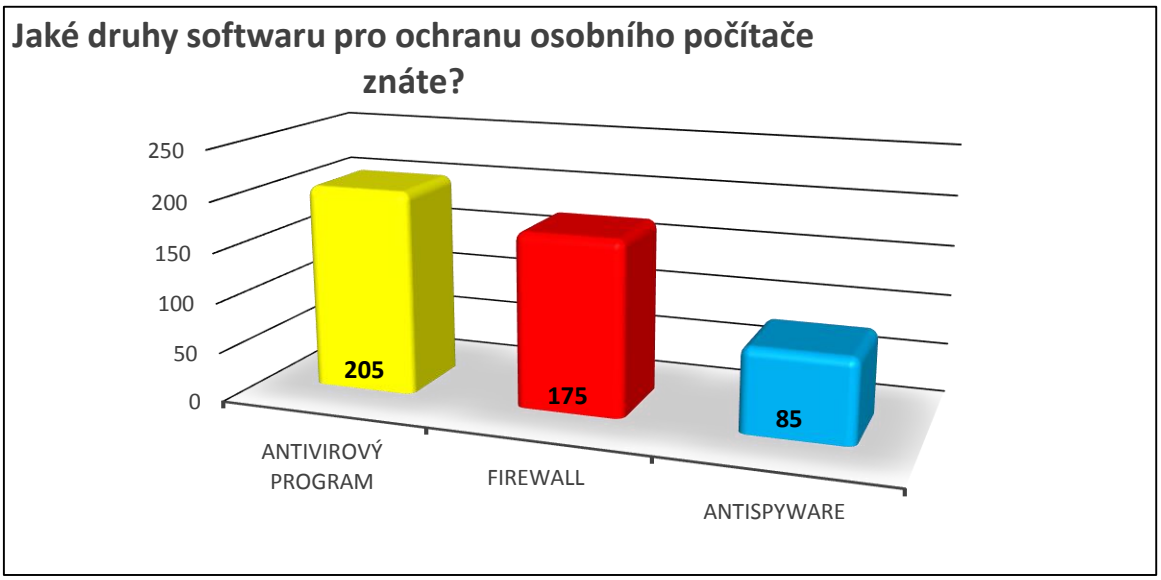


Zdroj: vlastní zpracování na základě výsledků dotazníku

Otázka č. 9: Jaké druhy softwaru pro ochranu osobního počítače znáte?

Na tuto otázku bylo možné odpovědět: antivirový program, firewall či antispyware. Bylo možno vybrat všechny odpovědi, nejméně však jednu. Cílem této otázky bylo zjistit, jaké mají uživatelé povědomí o softwaru, kterým se mohou chránit proti infiltraci. Z odpovědí vyplynulo, že téměř každý uživatel zná antivirový program (97,6% respondentů), s firewallem je to již trochu slabší – kladně odpovědělo 83,3% respondentů. Poměrně špatné povědomí je u antispywaru, který zná jen 40,4% respondentů.

Graf č. 18: Používání ochranného softwaru

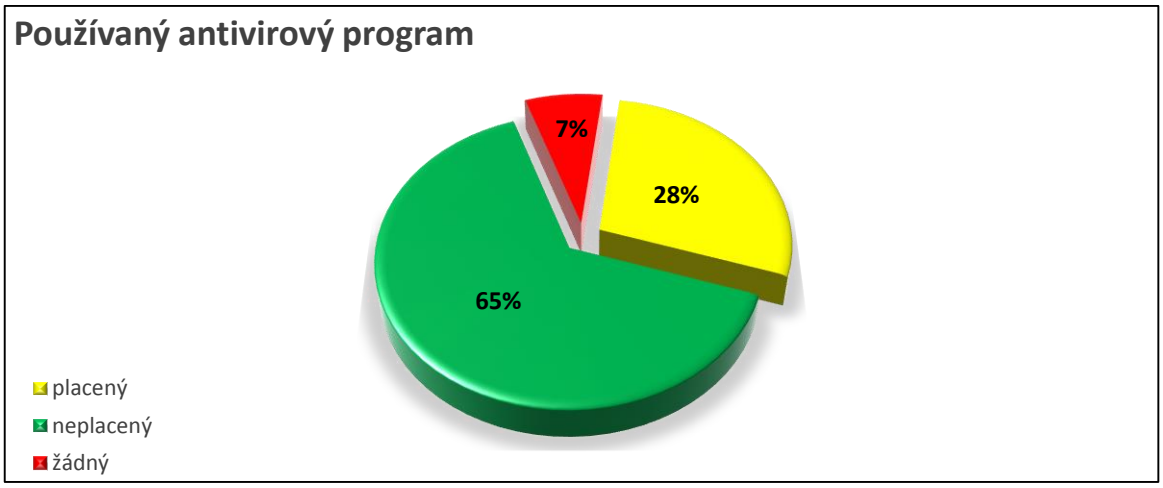


Zdroj: vlastní zpracování na základě výsledků dotazníku

Otázka č. 10: Na svém počítači používáte: antivirový program, firewall, antispyware.

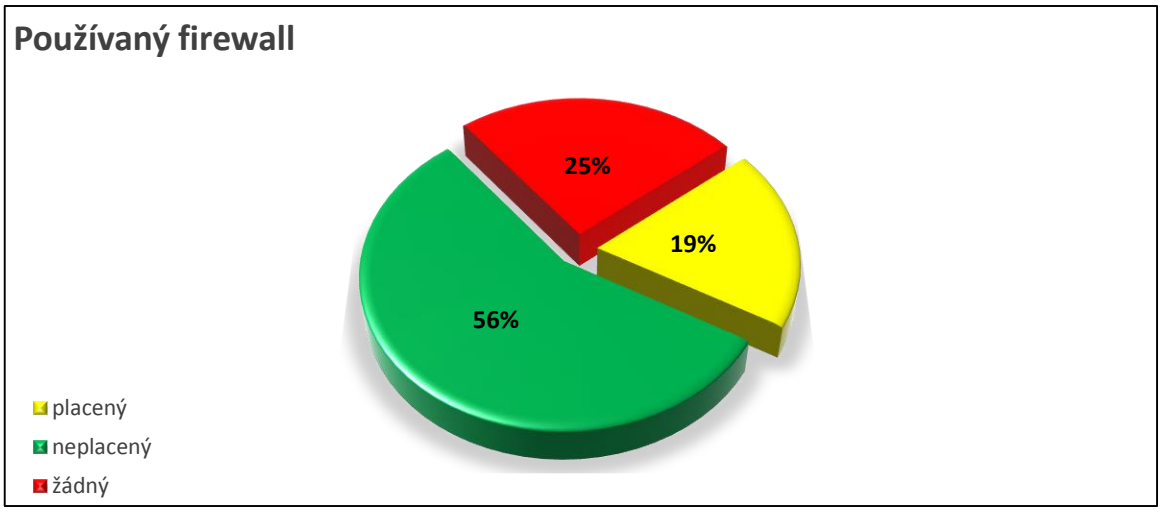
Desátá otázka navazovala na předchozí, kdy měli respondenti vybrat software, který skutečně na svém počítači používají a pokud ano, zda je placený či zdarma. Z odpovědí je možné zjistit, že ačkoliv uživatelé znají do určité míry software na ochranu počítače, stejně ho část nepoužívá. Antivirový program nepoužívá 7,1% respondentů, ačkoliv ho nezná jen 2,4% respondentů. Antispyware nepoužívá 65,2% respondentů, přičemž ho nezná 59,6% respondentů. Nehorší situace je v případě firewallu, který sice zná 83,3% respondentů, ovšem nepoužívá ho 24,8% respondentů.

Graf č. 19: Použití antivirového programu



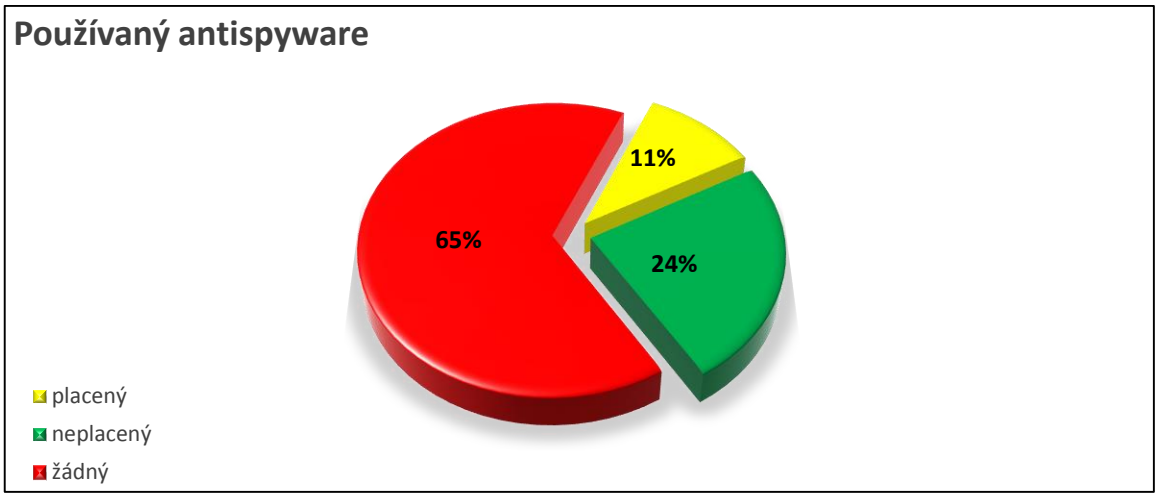
Zdroj: vlastní zpracování na základě výsledků dotazníku

Graf č. 20: Použití firewallu



Zdroj: vlastní zpracování na základě výsledků dotazníku

Graf č. 21: Použití antispywaru



Zdroj: vlastní zpracování na základě výsledků dotazníku

Zajímavý je také poměr placených a neplacených programů. Z uživatelů, kteří používají firewall, ho používá v placené verzi 25% uživatelů. Antivirový program v placené verzi používá dokonce 30% uživatelů, stejný poměr je i u antispywaru. Je tedy vidět, že z respondentů, kteří nějaký software používají, jsou ochotni za něj zaplatit.

Otázka č. 11: Víte o tom, že svoje data můžete ochránit pravidelným zálohováním?

Na jedenáctou otázku byla možná odpověď pouze **ano** či **ne**. Cílem bylo zjistit, zda uživatelé počítače mají povědomí o možnosti ochrany dat pomocí zálohování. Výsledek je dost optimistický, neboť 97,6% respondentů odpovědělo „**ano**“.

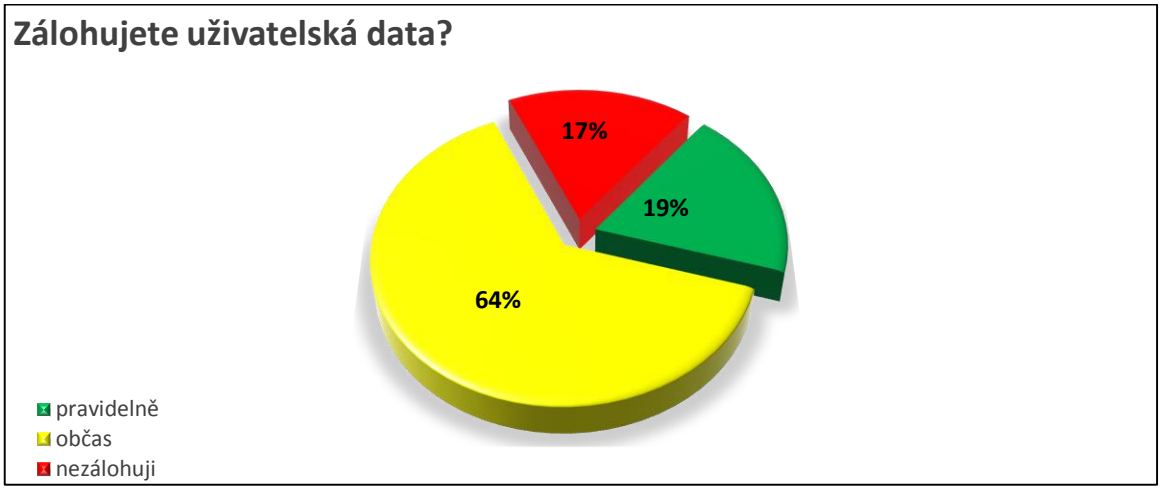
Graf č. 22: Povědomí uživatelů o možnosti zálohování

Zdroj: vlastní zpracování na základě výsledků dotazníku

Otázka č. 12: Zálohujete uživatelská data?

Tato otázka navazovala na předchozí, kdy respondenti mohli vybrat mezi třemi možnostmi: **pravidelně**, **občas** a **nezálohuji**. Bohužel se opět ukázalo, že ačkoliv uživatelé možnost ochrany dat proti ztrátě znají, nevyužívají ji zdaleka všichni. Vůbec totiž data nezálohuje 17,1% respondentů. Z těch, kteří data zálohují, je ale jen 23% takových, kteří data zálohují pravidelně.

Graf č. 23: Používání zálohování dat

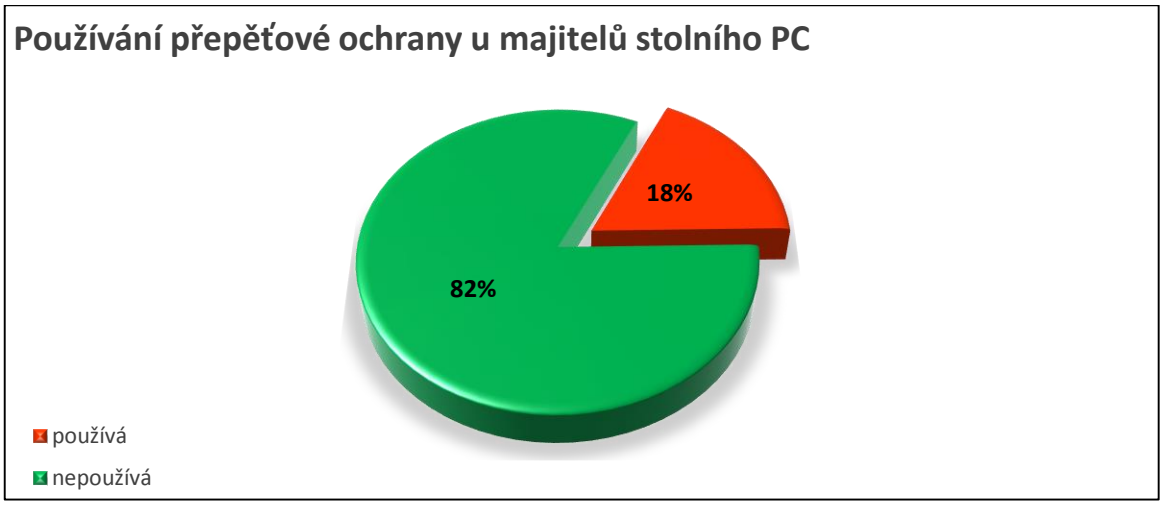


Zdroj: vlastní zpracování na základě výsledků dotazníku

Otázka č. 13: Používáte ochranu počítače před přepětím nebo výpadkem elektrické energie?

Třináctá otázka měla za cíl zjistit, zda si domácí počítač uživatelé chrání proti anomáliím v elektrické síti. Na výběr byly opět tři možnosti: **ano - UPS**, **ano - přepěťovou ochranu** a **ne**. Z odpovědí vyplynulo, že žádnou ochranu nepoužívají majitelé notebooku, což není překvapivé, protože přínos takové ochrany u přenosného počítače není prakticky žádný. U stolních počítačů jsou využívány jen ochrany proti přepětí – konkrétně 18% z respondentů vlastnících stolní počítač odpovědělo kladně. Nepřerušitelné zdroje napájení UPS nejsou používány vůbec. Je tedy vidět, že z výpadku elektrické energie nebo přepětí v síti uživatelé velký strach nemají.

Graf č. 24: Používání přepěťové ochrany u stolního PC

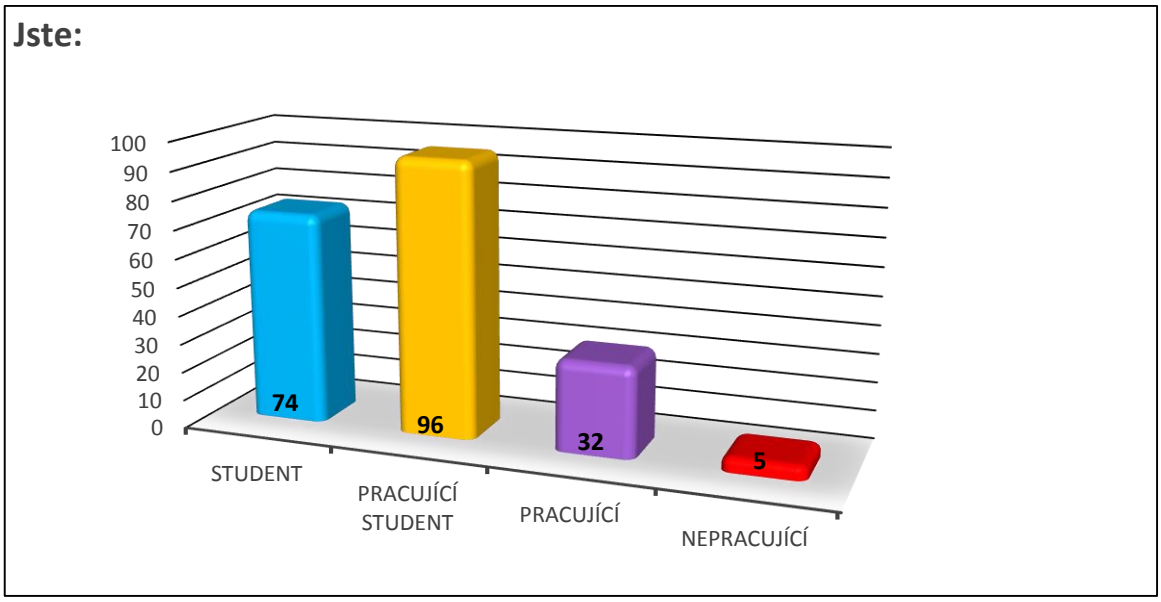


Zdroj: vlastní zpracování na základě výsledků dotazníku

Otázka č. 14: Jste: student, pracující student, pracující nebo nepracující?

Čtrnáctá otázka měla čtyři možnosti odpovědi podle toho, jaký je statut respondenta. Cílem bylo zjistit, jaký mají podíl na vědomostech studenti či „nestudenti“.

Graf č. 25: Rozdělení respondentů

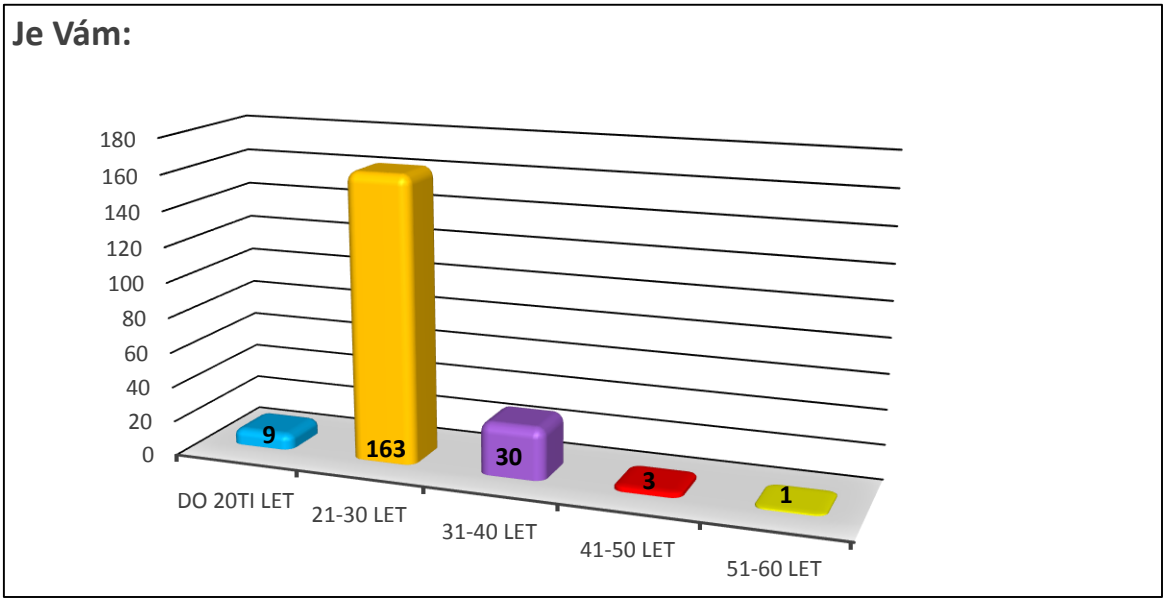


Zdroj: vlastní zpracování na základě výsledků dotazníku

Otázka č. 15: Je Vám: do 20ti let, 21 - 30 let, 31 – 40 let, 41 – 50 let, 51 – 60 let?

Patnáctá a poslední otázka měla za cíl zjistit, jaké mají povědomí o bezpečnosti domácího počítače různé věkové skupiny.

Graf č. 26: Rozdělení respondentů podle věku



Zdroj: vlastní zpracování na základě výsledků dotazníku

5. Celkové vyhodnocení výsledků a doporučení

5.1. Vyhodnocení výsledků

Z průzkumu vyplynulo, že prakticky všichni uživatelé domácího počítače na něm mají připojení k internetu. Není tedy překvapením, že hlavním účelem použití je procházení internetu a používání elektronické pošty, což jsou dva hlavní „kanály“, přes které hrozí riziko infiltrace. Tyto oblasti používali uživatelé bez rozdílu věku či statusu studenta nebo „nestudenta“.

Dále bylo zjištěno, že uživatelé mají velmi dobré povědomí o tom, že je možné se chránit před infiltrací pomocí antivirového programu, případně firewallu. Bohužel moc neznají antispyware, který je důležitou ochranou před špionáží počítače, případně před otravným nabízením různých reklam. V této oblasti by si uživatelé měli doplnit vědomosti o antispywaru a jeho přínosu.

V dalším kroku by měli všichni uživatelé takový software používat, neboť podle výsledků to část uživatelů nedělá. Antivirový program nepoužívají výhradně studenti a pracující studenti převážně ve věku 21 – 30 let. Přitom právě studenti vysoké školy by měli mít povědomí o možnosti infiltrace na nejvyšší úrovni. Ochranu ve formě firewallu a antispywaru nepoužívají uživatelé všech věkových kategorií, studenti i „nestudenti“. V oblasti samotného používání softwaru na ochranu počítače je tedy potřeba dost zapracovat, protože pokud je výrazná část uživatelů bez ochrany, může to přinést problémy všem.

S výše uvedeným zjištěním souvisí i fakt, že poměrně velká část uživatelů neví o tom, kdo hraje zásadní roli v oblasti bezpečnosti počítače. Pokud by si byli vědomi toho, že to jsou oni sami, pravděpodobně by svoje chování změnili a software pro ochranu počítače by používali ve všech oblastech.

Na to navazuje také zjištění, že podle názoru dvou pětin uživatelů nemá vliv na bezpečnost počítače používání originálního softwaru. To je dost významná část uživatelů. Jistě by bylo zajímavé zjistit, kolik z těchto uživatelů skutečně používá nelegální software a je tak vystaveno mnohem vyšší míře rizika infiltrace, než ostatní uživatelé. Ze zřejmých důvodů ale toto výzkum neřešil.

Uživatelé mají ovšem velmi dobré povědomí o tom, jak je určitá uživatelská akce bezpečná či nikoliv. V oblasti používání elektronické pošty ale ani velmi dobré povědomí nestačí, tam by mělo být stoprocentní. Část uživatelů totiž neví, jak může být nebezpečná příloha nebo odkaz v emailu a v případě útoku by u nich pravděpodobně došlo k infiltraci počítače nebo proniknutí do jejich bankovního účtu. Přitom se každá banka snaží šířit mezi svými klienty osvětu v oblasti používání internetového bankovnictví, ještě stále je ale co zlepšovat. Jedná se sice o nízké procento uživatelů, díky nim jsou ale útočníci stále „udržováni při životě“.

Navíc většina uživatelů svoje data zálohuje jen občas, ačkoliv téměř všichni vědí, že by jim tato činnost data ochránila, resp. zachránila. A to i při havárii pevného disku v důsledku výpadku elektrické energie, nebo jiné anomálii v síti - zejména v případech, kdy se proti těmto hrozbám uživatelé chrání jen minimálně.

5.2. Doporučení

1. Uživatelé by si nejprve měli doplnit znalosti zejména v kritických oblastech, jako je používání elektronické pošty a internetového bankovnictví;
2. měli by zlepšit své znalosti v možnostech ochrany počítače, především u spywaru a originality softwaru;
3. měli by používat software na ochranu před infiltrací, protože povědomí o něm mají a navíc je možno používat i velmi kvalitní software zdarma;
4. v každém případě by měli uživatelé zálohovat svoje uživatelská data, v optimálním případě pravidelně;
5. nakonec by uživatelé měli také používat alespoň základní ochranu proti přepětí v rozvodné síti, pokud vlastní stolní počítač.

Komerční software

Komerční software, který nabízí ochranu proti různým formám počítačové infiltrace, je dodáván buď jako samostatný nástroj (firewall, antivirus nebo antispyware), nebo jako balíček obsahující komplexní ochranu proti všem hrozbám.

Na základě nejaktuálnějšího testu bezpečnostních balíčků[24] lze usoudit, že takové balíčky jsou pro ochranu domácího počítače optimální variantou. Lze vybírat mezi placenými i neplacenými variantami a také mezi doplňkovými funkcemi, jako je např. zabezpečení hesel či bezpečné mazání dat apod.

Z neplacených variant je nejrozšířenější program Avast Free Antivirus, který však skončil až na desátém místě mezi čtrnácti testovanými produkty. Podobně dopadl i AVG Free Antivirus, který je co se týče rozšířenosti a oblíbenosti hned za programem Avast. Za ním skončili už jen Comodo Internet Security Premium a Microsoft Windows Defender – jeho výkon byl dokonce hodnocen jako „ubohý".

Z placených variant bezpečnostních balíčků dopadl nejlépe BitDefender Internet Security 2015. Kromě výborné antivirové kontroly při své práci zatěžuje jen minimálně celý systém a nabízí celou řadu doplňkových služeb. Bohužel cena je výrazně vyšší, než u ostatních placených programů, které se umístily v první polovině.

Také je nutno počítat se softwarem pro automatické zálohování.

Doporučený neplacený software

Pro **ochranu proti malwaru** lze doporučit produkt Panda Free Antivirus, který nabízí antivirovou ochranu hodnocenou téměř na 100% a i v dalších oblastech si vedl výborně. V hodnocení byl nejlepší mezi bezplatnými produkty a celkově skončil na pátém místě. Balíček lze zdarma stáhnout ze stránek výrobce (http://www.cloudantivirus.com/cz/), ze serverů nabízející stahování programů (www.slunecnice.cz apod.), nebo z optických médií přiložených k odborným časopisům (např. CHIP, Computer apod.).

Jako **zálohovací software** je možno nouzově využít v případě operačního systému Windows integrovanou utilitu pro zálohování, zvanou Windows Zálohování. Jedná se o

[24] HARTIMALER, Benjamin, KRATOCHVÍL, Petr. Nejlepší antivirová ochrana. *CHIP 03/2015*, s. 82-87

jednoduchý program, který však nabízí jen základní funkci zálohy celého disku a není tudíž ideální.

Pro dlouhodobé zálohování je možno doporučit např. program FBackup. Jde o jednoduchý a přehledný nástroj, který umožňuje pokročilé zálohování, včetně automatického. Poslední verze však není česky lokalizovaná, což je častý problém u programů s licencí freeware. Program lze získat na českých úložištích s programy, jako je např. Slunečnice.cz, Instaluj.cz nebo Stahuj.cz, případně přímo na stránkách výrobce www.fbackum.com.

Jako alternativu lze také využít softwaru, který bývá přiložen k vypalovacím mechanikám CD/DVD/BluRay, externím pevným diskům nebo diskovým úložištím.

Doporučený placený software

Pro **ochranu proti malwaru** u domácího použití lze jednoznačně doporučit Symantec Norton Security, který se v posledním testu[25] bezpečnostních balíčků umístil na druhém místě. Antivirová ochrana je hodnocena na plných 100%, čehož žádný jiný nedosáhl. Zátěž systému je nízká a v nabídce je řada doplňkových funkcí. Cena pro jeden počítač na rok je velmi příznivá a při zakoupení licencí pro více počítačů je jedna z nejnižších v testu.

[25] HARTIMALER, Benjamin, KRATOCHVÍL, Petr. Nejlepší antivirová ochrana. *CHIP 03/2015*, s. 82-87

Obrázek č. 14: Norton Security

Zdroj: Techsupportall.com. *Download Norton 2015* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.techsupportall.com/download-norton-2015-norton-security-review-coupon-codes/>.

Balíček je nabízen jako komplexní ochrana osobního počítače pro systémy Windows i MAC a také pro mobilní zařízení se systémy Android i iOS. Cena[26] aktuální v únoru 2015 byla 1099,-Kč pro jedno zařízení na rok, 1699,-Kč pro pět zařízení na rok. Nejdražší varianta je pro 10 zařízení a stojí 1899,-Kč na rok. Ve variantách s více licencemi je tak možné zabezpečit všechna zařízení v domácnosti. K dispozici je také varianta s funkcí zálohování dat na internetové úložiště o kapacitě 25GB, která je však téměř o polovinu dražší a nebudeme jí dále věnovat pozornost.

[26] Symantec. *Norton Security* [online], [cit. 2015-01-10]. Dostupné na www: <http://norton.symantec.com/norton/ps/bb/3up_ns1_ns_nsbu_cz_cs_largo_notw_brnf.html?om_sem_cid=hho_sem_ic:cz:ggl:CS:e|kw0000006084|55408476562|c&country=CZ>.

Uvedený balíček nabízí tyto funkce:

- firewall;
- antivirová ochrana;
- antispyware;
- ochrana před krádeží identity;
- antispamový filtr – blokování nevyžádané pošty;
- ochrana uložených uživatelských jmen a hesel;
- ochrana mobilních zařízení se systémy Android a iOS;
- ochrana soukromí na mobilních zařízení;
- ochrana proti enormnímu vybíjení baterií mobilního zařízení;
- ochrana proti enormnímu využívání datových přenosů u mobilních zařízení;
- určení polohy odcizeného nebo ztraceného mobilního zařízení.

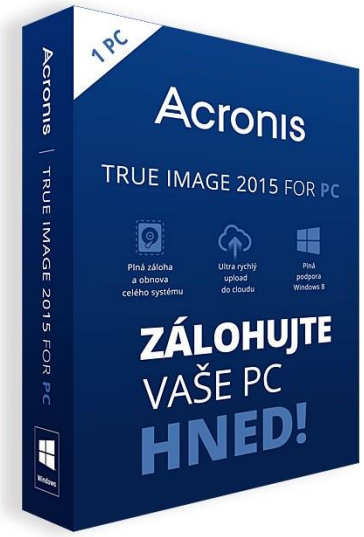
Tento balíček, stejně jako další software společnosti Norton, lze získat:

- online bezhotovostní platbou a následným stažením balíčku na stránkách cz.norton.com;
- v prodejně s výpočetní technikou jako standardní krabicovou verzi produktu.

Samotnou instalaci produktu zvládne každý uživatel.

Zálohovací software v placené licenci lze doporučit Acronis True Image for PC. Jde o pokročilý software, který nabízí všechny druhy zálohy na širokou škálu možných zálohovacích zařízení. Software je i v českém jazyce a jeho instalaci a obsluhu zvládne každý běžný uživatel.

Obrázek č. 15: Acronis True Image for PC



Zdroj: Acronis. *Acronis True Image 2015 for PC 1 Computer CZ* [online]. [cit. 2015-01-10]. Dostupné na www: <http://shop.backup-store.cz/true-image-2015-PC-cz.html/>.

Software nabízí tyto funkce:

- zálohování metodou tvorby obrazu disku;
- zálohování zvolených souborů a adresářů;
- plné, přírůstkové a rozdílové zálohy;
- komprese a šifrování dat 256bit;
- možnost vyloučení nepotřebných dat ze zálohování;
- online i offline zálohování;
- nastavení maximálního vytížení sítě během zálohování;
- obnova celého PC, nebo jen potřebných dat;
- obnova zálohy na nový PC bez nutnosti instalace operačního systému a to i na rozdílný hardware;
- zálohování na lokální i síťové úložiště, do zařízení NAS, na CD, DVD, HD-DVD, BluRay;
- podpora rozhraní IDE, SATA, SCSI, iSCSI, Firewire, USB
- možnost ukládání zálohy do skryté části disku, do několika úložišť, postupné přesouvání do jiného úložiště;

- verifikace a konsolidace záloh, jejich postupné odmazávání podle nastaveného plánu, dělení záloh na potřebnou velikost;
- podpora Windows XP – Windows 8.1;
- jazyky CZ, EN, DE, RU včetně kompletní dokumentace.

Cena softwaru Acronis True Image for PC je 1421,- Kč za licenci pro jeden počítač. Software lze získat elektronicky ze stránek výrobce www.acronis.cz nebo e-shopů (např. Alza), případně jako krabicovou verzi ve specializovaných obchodech nebo e-shopech.

Doporučená ochrana proti přepětí a výpadku el. energie

Ochrana proti přepětí v rozvodné síti elektrické energie může být jako samostatné zařízení v ceně od cca 200,- Kč, nebo ve spojení se záložním zdrojem UPS. Jako doporučené je kombinované zařízení APC Back-UPS 400. Pro domácí použití je záložní zdroj dostatečně výkonný a disponuje nejen ochranou proti přepětí v rozvodné síti, ale i ochranou proti přepění na telefonní lince a datové síti.

Obrázek č. 16: Záložní zdroj APC Back-UPS 400

Zdroj: APC. *APC Back-UPS 400* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.apc.com/products/resource/include/techspec_index.cfm?base_sku=BE400-CP&total_watts=200/>.

Záložní zdroj lze zakoupit v prodejnách s elektronikou nebo IT technikou, případně specializovaných e-shopech. Cena zařízení je od 949,- Kč v závislosti na konkrétním prodejci.

Doporučené zálohovací zařízení

Zálohování pro domácí účely lze provádět na různá zařízení, jako jsou média CD/DVD/BluRay, externí pevné disky či diskové úložiště.

Doporučit lze vzhledem k ceně zálohování na DVD média. Vypalovací mechanikou CD/DVD dnes disponuje většina počítačů a cena kvalitních médií začíná na 15,- Kč. Lze ale pořídit i vysoce odolné a trvanlivé médium DVD za 80,- Kč s předpokládanou životností 1000 let. Nízká cena zálohování na média DVD je vykoupena nepraktičností, kdy nelze pořizovat některé typy záloh a hodí se tak především pro zálohování vybraných důležitých souborů a adresářů, případně operačního systému. Zálohování tímto způsobem lze by mělo být prováděno alespoň 1x měsíčně.

Pro plnohodnotné zálohování počítače lze doporučit zálohování na externí pevný disk Verbatim 2.5" Store 'n' Go USB 1TB HDD, který je připojitelný přes rozhraní USB a spolu s ním je dodáván i zálohovací software.

Obrázek č. 17: Verbatim 2.5“ Store 'n' Go USB 3.0 1TB HDD

Zdroj: Verbatim. *Přenosný pevný disk Store 'n' Go USB 3.0 1TB - černá* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.verbatim-europe.cz/cz/prod/store-n-go-usb-3-0-portable-hard-drive-1tb-black-53023/>.

Zařízení lze pořídit opět v prodejnách s IT technikou, případně specializovaných e-shopech. Cena zařízení je od 1740,- Kč v závislosti na konkrétním prodejci.

Další možností, ovšem tou nejdražší, je zálohování na diskové úložiště, tzv. NAS. Tyto úložiště jsou umístěné v síti LAN a lze na nich nastavit zcela automatické zálohování a to i v reálném čase. Díky tomu je k dispozici záloha i posledních dat, pokud dojde k havárii pevného disku v počítači. Spotřeba zařízení je jen několik málo wattů a zůstává v provozu trvale. Cena začíná na cca 3.000,- Kč a končí na více než 30.000,- Kč.

5.3. Náklady na ochranu PC

Náklady na komplexní ochranu domácího PC lze rozdělit do dvou kategorií:

1. náklady na ochranu proti malwaru, tedy proti škodlivému softwaru;
2. náklady na ochranu před ztrátou dat, tedy anomáliím v rozvodné síti el. energie nebo před jejich smazáním či destrukcí.

První kategorie zahrnuje samotný bezpečnostní software. Jak vyplývá z předchozích kapitol, pokud si uživatel dohledá odborné informace, **lze velmi kvalitní bezpečnostní software pořídit zdarma**, byť nemá některé pokročilé funkce placených programů. Uživatel, který využije některé nestandardní funkce, nebo chce mít jistotu v ochraně, může sáhnout po placeném bezpečnostním softwaru, který je v současnosti předplácen na rok dopředu. Taková varianta **pro jeden počítač stojí u doporučeného softwaru 1099,- Kč na rok**, v případě více počítačů se neplatí adekvátní násobky, ale jen část ceny navíc.

Druhou kategorii je možno ještě rozdělit na software a hardware. V případě softwaru jde o software zálohovací, který **je možno pořídit samostatně zdarma**, jako přibalený software k zálohovacímu zařízení zdarma nebo jako samostatný placený program. **Placený doporučený software stojí 1421,- Kč** s trvalou licencí pro jeden počítač. Při využití pro více počítačů se podobně jako u bezpečnostního softwaru připlácí jen část ceny, nikoliv adekvátní násobky. V případě hardwaru jde o jedinou „věc“, kterou nelze získat zdarma. Zálohování nejdůležitějších dat a souborů však může stát jen řádově desítky Kč, pokud je uživatel ochoten „skousnout“ omezení související se zálohováním na optická média DVD. Doporučená varianta je ovšem také cenově příznivá – **stojí 1740,- Kč**, pokud vezmeme v úvahu kapacitu, kompatibilitu i praktičnost. Pokud ale uživatel využije komfort a pokročilé funkce včetně automatického zálohová, cena se může vyšplhat na tisíce Kč. Také

záložní zdroj UPS a přepěťová ochrana není finančně příliš náročná, kvalitní kombinované **doporučené řešení je dokonce nižší než 1.000,- Kč**.

Souhrn nákladů na komplexní ochranu počítače je uveden v tabulce 1.

Tabulka č. 1: Náklady na komplexní ochranu počítače

	bezpečnostní software		zálohovací software		zálohování na DVD	zálohovací zařízení 1TB	UPS včetně přepěťové ochrany
	zdarma	placený	zdarma	placený	1 médium 4,7GB		
1. rok	0,-	1099,-	0,-	1421,-	180,-	1740,-	949,-
každý další rok	0,-	1099,-	0,-	0	180,-	0	0
celkem za dva roky	**0,-**	2198,-	**0,-**	1421,-	**360,-**	**1740,-**	**949,-**

Zdroj: vlastní zpracování

Jak je vidět v tabulce č. 1, počítač lze ochránit za relativně velmi nízké náklady. Lze dokonce říci, že náklady na ochranu mohou být zanedbatelné, v porovnání s náklady na samotný provoz počítače. Do těch je totiž nutno započítat nejen náklady na spotřebovanou el. energii, ale především náklady na připojení k síti internet, které jsou v dnešní době pro domácnosti v řádu stokorun (cca 300,- a více). Pro uživatele, který je ochoten si informace a software vyhledat a nevadí mu některá omezení, tak mohou být náklady na kompletní ochranu domácího PC rovny pouze tříměsíční ceně za připojení k internetu.

V porovnání s tím, jaké škody dokáže malware či havárie pevného disku napáchat, jsou uvedené náklady skutečně velmi nízké a dokáže je unést každý uživatel domácího počítače, který disponuje připojením k internetu.

6. Závěr

Diplomová práce se zabývala komplexním zabezpečením domácího PC. Jsou v ní charakterizovány vnitřní a vnější hrozby, na které by uživatelé měli být připraveni a také metody a programy, které takovým hrozbám umí čelit.

Pro vypracování byly využity dlouholeté znalosti a zkušenosti autora z oblasti osobních počítačů, především pro domácí použití. V praktické části byla použita metoda dotazníkového výzkumu znalostí domácích uživatelů.

Z výzkumu vyplynulo, že v oblasti ochrany proti vnějším hrozbám mají uživatelé velmi dobré povědomí o programech, které je mohou ochránit, ale ne všichni uživatelé takové programy používají. Dále bylo výzkumem zjištěno, že se stále najde určitá část uživatelů, kteří si nejsou vědomi následků svého jednání při používání počítače. V neposlední řadě výzkum ukázal, že zálohování a ochrana proti výpadku el. energie nebo přepětí není na dobré úrovni.

Práce proto uvádí konkrétní doporučení, jak si svůj počítač ochránit proti vnitřním i vnějším hrozbám, včetně rozpočtu jednotlivých druhů ochran.

Na závěr tedy lze konstatovat, že zabezpečení domácích PC je na dobré úrovni, stále je však co zlepšovat, zejména v oblasti osvěty uživatelů.

Diplomová práce by měla být vodítkem a zdrojem informací pro běžné uživatele domácího počítače. Měla by pomoci omezit škody, ke kterým dochází při ztrátě dat, ať už osobního charakteru, nebo souborů uložených v počítači.

7. Seznam použitých zdrojů

BITTO, Ondřej. *Jak zabezpečit domácí a malou síť Windows XP*. Brno: Computer Press, 2006, 216 s., ISBN: 80-251-1098-2.

ENDORF Carl, CHULTZ Eugene, MELLANDER Jim. Detekce a prevence počítačového útoku. Praha: Grada, 2005, 356 s., ISBN 80-247-1035-8.

HALBICH Čestmír, BRECHLEROVÁ Dagmar. *Bezpečnost informačních systémů – vybrané kapitoly*. Praha: Česká zemědělská univerzita v Praze, 2003, 104s., ISBN: 80-213-1090-1.

HANÁČEK Petr, STAUDEK Jan. *Bezpečnost informačních systémů*. Praha: Úřad pro státní informační systém, 2000, 128s., ISBN: 80-238-5400-3

JIROVSKÝ Václav. *Kybernetická kriminalita*. Praha: Grada, 2007, 288 s., ISBN: 978-80-247-1561-2

KRÁL, Mojmír. *Bezpečnost domácího počítače - prakticky a názorně.* Praha: Grada, 2006, 336 s., ISBN: 80-247-1408-6.

CHIP 02/2015: magazín o digitálních technologiích. Praha: Burdainternational, 2015, roč. 25, únor, ISSN: 1210-0684: MK ČR E 5361

CHIP 03/2015: magazín o digitálních technologiích. Praha: Burdainternational, 2015, roč. 25, březen, ISSN: 1210-0684: MK ČR E 5361

Internetové zdroje:

Acronis. *Inkrementální – přírůstková záloha* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.acronis.cz/kb/inkrementalni-zaloha/>

Český statistický úřad. *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci 2014* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.czso.cz/csu/2014edicniplan.nsf/p/062004-14>

CIO Business World.cz. *Drahá e-špionáž* [online]. [cit. 2015-01-10]. Dostupné na www: <http://businessworld.cz/bezpecnost/draha-e-spionaz-11408>

DataProtectionCenter.com. *Phishing – going the extra mile (with virtual keyboard)* [online]. [cit. 2015-01-10]. Dostupné na www:

>http://dataprotectioncenter.com/security/phishing-going-the-extra-mile-with-virtual-keyboard/>

GloboTech Blog. *Category Archives: Cloud Computing* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.gtcomm.net/blog/category/cloud-computing/>

HowStuffWorks. *How Spyware Works* [online]. [cit. 2015-01-10]. Dostupné na www: <http://computer.howstuffworks.com/spyware1.htm>

MediaCenter Panda Security. *PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections, Set New Record* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.pandasecurity.com/mediacenter/press-releases/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/>

Microsoft. *Co je brána firewall?* [online]. [cit. 2015-01-10]. Dostupné na www: <http://windows.microsoft.com/cs-cz/windows/what-is-firewall#1TC=windows-7/>

PC Magazine Encyclopedia. *Definition of: adware* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.pcmag.com/encyclopedia/term/37577/adware>

Svět hardware. *Počítačová havěť – vývoj a rozdělení malware* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.svethardware.cz/pocitacova-havet-vyvoj-a-rozdeleni-malware/25680>

Symantec. *Norton Security* [online], [cit. 2015-01-10]. Dostupné na www: <http://norton.symantec.com/norton/ps/bb/3up_ns1_ns_nsbu_cz_cs_largo_notw_brnf.html ?om_sem_cid=hho_sem_ic:cz:ggl:CS:e|kw0000006084|55408476562|c&country=CZ>

Technical Info. *The Pharming Guide* [online]. [cit. 2015-01-10]. Dostupné na www: <http://www.technicalinfo.net/papers/Pharming2.html>

Technet.cz. *Skončil obří útok na evropský internet. Hrozba i pro internet věcí* [online]. 2014-02-12 [cit. 2015-01-10]. Dostupné na www: <http:// http://technet.idnes.cz/utok-ntp-evropa-nejmasivnejsi-internetovy-utok-ukazuje-narust-riziko-139-/sw_internet.aspx?c=A140212_161619_sw_internet_vse/>

Tee Support. *Remove shoprdig.com Virus* [online]. [cit. 2015-01-10]. Dostupné na www: <http://blog.teesupport.com/remove-shoprdig-com-virus-shoprdig-com-manual-removal-instructions/>

TopTenREVIEWS. *Botnet Zombie Apocalypse: How to Protect Your Computer* [online]. [cit. 2015-01-10]. Dostupné na www: <http://mac-internet-security-software-review.toptenreviews.com/how-do-i-know-if-my-computer-is-a-botnet-zombie-.html>

Travel Stack Exchange. *Traveling with a laptop* [online]. [cit. 2015-01-10]. Dostupné na www: <http://travel.stackexchange.com/questions/10206/travelling-with-a-laptop/>

Viry.cz. *Rozsáhlé DDoS útoky ochromily služby řady institucí* [online]. 2013-03-07 [cit. 2015-01-10]. Dostupné na www: <http:// http://www.viry.cz/rozsahle-ddos-utoky-ochromily-sluzby-rady-instituci/>

Wikipedia. *Počítačový virus* [online]. 2014-12-15 [cit. 2015-01-10]. Dostupné na www: <http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus/>

Seznam grafů

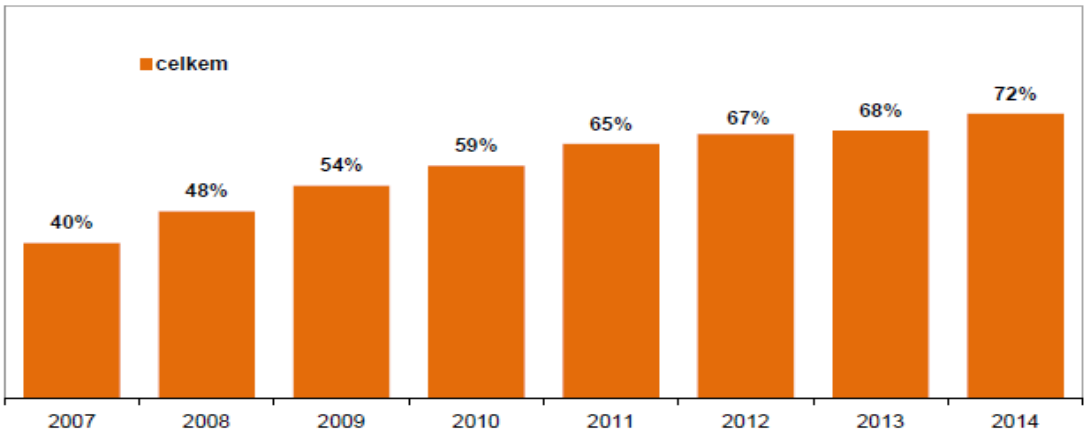
Seznam obrázků

Seznam tabulek

8. Přílohy

Příloha č. 1: Domácnosti s počítačem

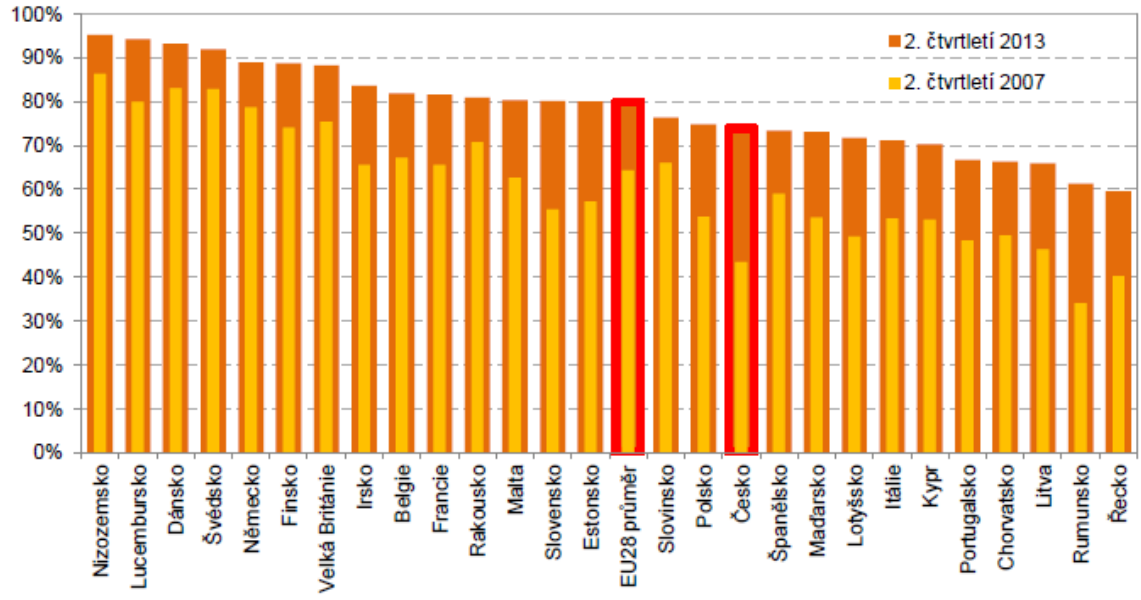
Graf 1: Domácnosti s počítačem *(% domácností)*



Zdroj: Český statistický úřad. *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci 2014* [online]. 2014-12-02 [cit. 2015-01-10]. Dostupné na www: <http://www.czso.cz/csu/2014edicniplan.nsf/p/062004-14>.

Příloha č. 2: Domácnosti s počítačem v EU

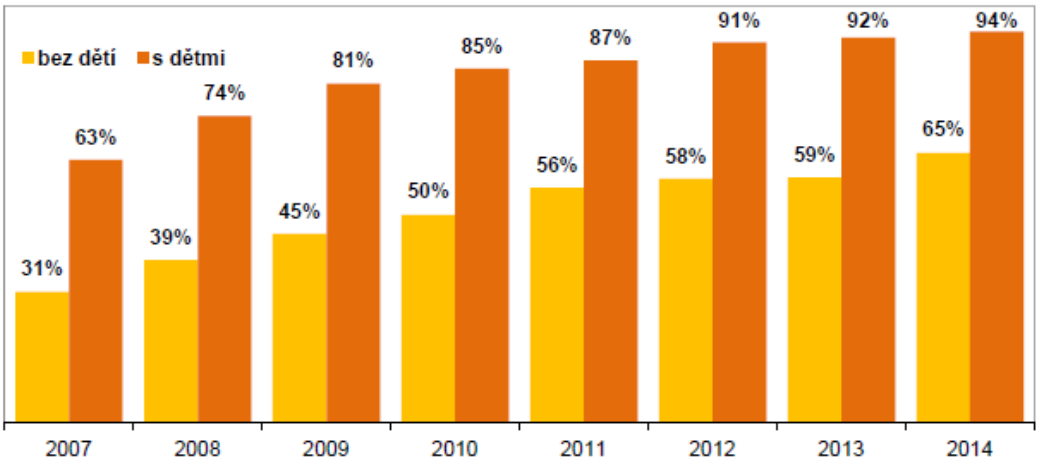
Graf 7: Domácnosti s počítačem v zemích EU *(% domácností)*



Zdroj: Český statistický úřad. *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci 2014* [online]. 2014-12-02 [cit. 2015-01-10]. Dostupné na www: <http://www.czso.cz/csu/2014edicniplan.nsf/p/062004-14>.

Příloha č. 3: Domácnosti s počítačem podle přítomnosti dětí

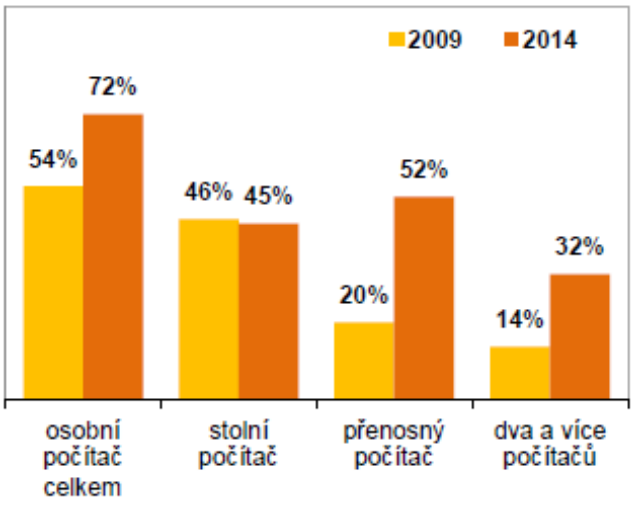
Graf 2: Domácnosti s počítačem podle přítomnosti dětí *(% domácností)*



Zdroj: Český statistický úřad. *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci 2014* [online]. 2014-12-02 [cit. 2015-01-10]. Dostupné na www: <http://www.czso.cz/csu/2014edicniplan.nsf/p/062004-14>.

Příloha č. 4: Domácnosti s počítačem podle typu počítače

Graf 4: Domácnosti s počítačem podle typu počítače *(% domácností)*



Zdroj: Český statistický úřad. *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci 2014* [online]. 2014-12-02 [cit. 2015-01-10]. Dostupné na www: <http://www.czso.cz/csu/2014edicniplan.nsf/p/062004-14>.

Příloha č. 5: Dotazník - otázky kladené na respondenty

1. Máte doma osobní počítač?
    a. ano;
    b. ne.

2. Máte na domácím PC připojení k internetu?
    a. ano;
    b. ne.

3. Jakého typu je Vaše domácí PC?
    a. stolní počítač;
    b. notebook.

4. K jakému účelu používáte domácí PC?
    a. internet;
    b. elektronická pošta;
    c. výuka;
    d. zábava – hraní her, přehrávání filmů či hudby;
    e. práce.

5. Jaký typ softwaru na svém počítači používáte?
    a. placený;
    b. neplacený;
    c. obojí.

6. Myslíte si, že používání originálního softwaru zvyšuje míru zabezpečení osobního počítače?
    a. ano;
    b. ne.

7. Do jaké míry má uživatel vliv na bezpečnost osobního počítače?
    a. uživatel ovlivňuje bezpečnost jen z části;

b. uživatel ovlivňuje bezpečnost na 100%.

8. U následujících otázek určete, která uživatelská akce je bezpečná či nikoliv:
    a. otevírání příloh ve všech emailech:
        i. bezpečné;
        ii. nebezpečné;
        iii. nevím;
    b. okamžité potvrzení různých upozorňujících hlášení bez jejich přečtení nebo pochopení:
        i. bezpečné;
        ii. nebezpečné;
        iii. nevím;
    c. používání mnoha oken či programů najednou:
        i. bezpečné;
        ii. nebezpečné;
        iii. nevím;
    d. hraní počítačových her:
        i. bezpečné;
        ii. nebezpečné;
        iii. nevím;
    e. návštěvy zahraničních internetových stránek s erotickou tématikou:
        i. bezpečné;
        ii. nebezpečné;
        iii. nevím;
    f. přihlášení do internetového bankovnictví přes odkaz z emailu:
        i. bezpečné;
        ii. nebezpečné;
        iii. nevím;
    g. kopírování nebo instalace softwaru z neznámých médií (CD, DVD, USB):
        i. bezpečné;
        ii. nebezpečné;

iii. nevím;

h. zapnutí automatických aktualizací operačního systému:
    i. bezpečné;
    ii. nebezpečné;
    iii. nevím;
i. dočasné vypnutí antiviru nebo firewallu:
    i. bezpečné;
    ii. nebezpečné;
    iii. nevím;

9. Jaké druhy softwaru pro ochranu osobního počítače znáte?
    a. Firewall;
    b. Antivirový program;
    c. Antispyware.
10. Na svém domácím počítači používáte:
    a. Firewall:
        i. komerční – placený;
        ii. zdarma – freeware;
        iii. nepoužívám;
    b. Antivirový program:
        i. komerční – placený;
        ii. zdarma – freeware;
        iii. nepoužívám;
    c. Antispyware:
        i. komerční – placený;
        ii. zdarma – freeware;
        iii. nepoužívám;
    d.
11. Víte o tom, že svoje data můžete ochránit pravidelným zálohováním?
    a. ano;
    b. ne.

12. Zálohujete uživatelská data?

a. pravidelně;
b. občas;
c. nezálohuji.

13. Používáte ochranu počítače před přepětím nebo výpadkem elektrické energie?

a. ano – UPS;
b. ano – přepěťovou ochranu;
c. ne.

14. Jste:

a. student;
b. pracující;
c. pracující student;
d. nepracující.

15. Je Vám:

a. do 20ti let;
b. 21 – 30 let;
c. 31 – 40 let;
d. 41 – 50 let;
e. 51 – 60 let.