UNIVERZITA PALACKÉHO V OLOMOUCI
PEDAGOGICKÁ FAKULTA
Katedra technické a informační výchovy

Bakalářská práce

Michaela Studená

Matematika se zaměřením na vzdělávání a základy technických věd
a informačních technologií pro vzdělávání

Problematika chápání pojmu malware u vysokoškolských studentů

Olomouc 2015

Vedoucí práce: doc. PhDr. Miroslav Chráska, Ph.D.

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma „Problematika chápání pojmu malware u vysokoškolských studentů“ vypracovala samostatně pouze s použitím uvedených zdrojů a podkladových materiálů.

V Olomouci dne 13. 4. 2015

……...

Michaela Studená

Poděkování

Děkuji doc. PhDr. Miroslavu Chráskovi, Ph.D., za odborné vedení bakalářské práce, poskytování rad a materiálových podkladů k práci.

Obsah

Úvod

Žijeme v době, kdy jsou počítače, chytré telefony a tablety nedílnou součástí našeho každodenního života. Bez těchto zařízení bychom se již jen asi těžko obešli, neslouží nám totiž jen k práci, ale také k zábavě. S každodenním používáním však také roste riziko, že svoje zařízení infikujeme některým druhem škodlivého kódu, tzv. malwarem, nejsme-li dostatečně chráněni. Malware může způsobit ztrátu důležitých dat, nebo jejich únik jinému člověku, který s nimi pak může nakládat dle vlastní fantazie.

Spousta lidí v mém okolí ani netuší, jaké škody může malware způsobit, dokonce někteří ani neví, co si pod pojmem „malware“ představit a pro jakýkoliv problém, který se jim na zařízení vyskytne, použijí jednotný název „počítačový vir“. To je ovšem správně pouze v případě, že uživateli opravdu infikoval počítač vir, ale v mnoha případech se jedná o jiný druh malwaru a označení „počítačový vir“ tedy není správné.

To je hlavní důvod, proč jsem si zvolila toto téma, a protože se s touto chybou nesetkávám jen u běžných uživatelů, ale také v médiích a u odborníků v počítačových servisech, myslím si, že by bylo dobré tuto problematiku dále rozvinout.

Doufám, že mé poznatky, které uvedu v této bakalářské práci, pomohou zvýšit povědomí o malwaru, alespoň u části české společnosti, která toto téma již delší dobu značně zanedbává. Pedagogičtí pracovníci by měli také začít vést své žáky k tomu, aby svá digitální zařízení používali bezpečně a bez znalosti problematiky malwaru nemůže být výuka efektivní. Lidé, kteří si myslí, že je zbytečné se problematikou malwaru zabývat, by se měli zamyslet nad tím, že se najde nespočet životních situací, na které může mít nefunkční počítač, či jiné digitální zařízení dopad. Již v minulosti malware způsobil mnoho problémů dokonce i u tak velkých firem jako je Microsoft a Google, dokonce se tvůrcům malwaru podařilo vyřadit z provozu i tísňovou linku 911 a zde již nejde „pouze“ o ztrátu dat, ale i o ohrožení lidských životů.

V této práci se také pokusím o vytvoření nové moderní definice pojmu malware, ukážeme si, jak můžeme malware rozdělit a další fakta, týkající se právní problematiky, motivaci k tvorbě malwaru, nejslavnější jména malwaru, která se zapsala do dějin a také poukážeme, že malware se netýká jen počítačů.

1 Cíle práce

Hlavním cílem teoretické části bakalářské práce je definovat pojem malware a popsat jeho jednotlivé druhy. Dalším cílem je seznámit čtenáře se skutečností, že malware se vyskytuje i na jiných digitálních zařízeních. Také v této práci představíme nejznámější exempláře malwaru, které dokázaly ovlivnit přístup společnosti k zabezpečení, ale také inspirovaly další tvůrce malwaru a uvedeme i právní problematiku, motivaci pro tvorbu malwaru a způsoby, jimiž se můžeme proti malwaru bránit.

Cílem praktické části této bakalářské práce je zjistit představu vysokoškolských studentů o pojmu malware a jeho druzích, zjistit možné závislosti odpovědí studentů na jejich pohlaví, a také zjistit jejich názory na vzdělání v oblasti zabezpečení vzhledem k tomu, za jaký typ člověka se považují. Vlastní výzkumné šetření bude realizováno ve dvou etapách. Na základě teoretických poznatků v této bakalářské práci bude v předvýzkumu vytvořena zkušební verze dotazníku, kterou si ověříme, zdali je dotazník správně sestaven a jeho otázky jsou dostatečně srozumitelné. Také tím získáme možné odpovědi do hlavního výzkumného šetření. Dále se pokusíme navrhnout vhodné řešení, které by mohlo pomoci ke zvýšení povědomí o problematice malwaru již u žáků základních a středních škol.

2 Teoretická část

2.1 Definice pojmu malware

Pojem malware vznikl složením dvou anglických slov malicious (česky zákeřný) a software. Houser (2012) označuje pojmem malware jakýkoliv škodlivý kód, který při svém vniknutí zahájí činnosti ke škodě systému, ve kterém se nachází.

Jirovský (2009) dodává, že takovýto škodlivý kód může být naprogramován, aby se jeho projevy spustily buďto při nějaké akci (např. při spuštění nějakého programu, otevření e-mailu, apod.) nebo může být načasován a projevit se až za určitou dobu.

Z mého pohledu by se dal pojem malware chápat z aktuálnějšího hlediska jako jakýkoliv druh infiltrace, který slouží nejen ke škodě systému, do kterého vnikne, ale i ke škodě samotného uživatele (např. krádež osobních údajů).

2.2 Rozdělení malwaru

Ačkoliv se většina autorů na vymezení pojmu malware shodne, při jeho rozdělení již najdeme značné rozdíly. Je to zejména kvůli skutečnosti, že každý druh malwaru se může jinak šířit, projevovat, a také jejich nebezpečnost se liší, samozřejmě existují i speciální případy a kombinace, které postupem času přibývají.

Například Jalůvka (2000) řadí mezi malware viry, trojské koně, červy, logické bomby a jako samostatnou kategorii (na rozdíl od ostatních autorů) uvádí i makroviry.

Aycock (2006) doplňuje k tomuto rozdělení ještě zadní vrátka (backdoor), spyware, adware, zombie a hybridy. Makroviry pak řadí jako podskupinu virů, stejně jako Hák (2005), který k těmto ještě přidává dialer, phishing a hoax.

Oproti tomu Petrowski (2014) ještě přidává exploit, scareware a ransomware.

V této práci se budeme držet následujícího dělení malwaru, které postihuje zejména počítače: viry, trojský kůň, zadní vrátka, červ, spyware, dialer, adware, rootkit, logická bomba, scareware, zombie, ransomware a jako speciální případy uvedeme i hoax a phishing.

2.2.1 Viry

Počítačový virus je velikostně malý program, který může infikovat jiný program v počítači tím, že do něj zkopíruje své tělo a tak se infikovaný program stane prostředkem pro další šíření viru. Mluvíme o tom, že virus je schopen sebereplikace (Jalůvka, 2000).

Virus se dokáže šířit nejen v rámci jednoho počítače, ale také z jednoho počítače na druhý za pomoci přenosných médií, jako je disketa, CD, DVD nebo USB flash disk a samozřejmě v dnešní době již velmi rozšířeným Internetem, např. jako příloha e-mailu (Aycock, 2006).

Kdyby si tuto práci četl biolog, určitě by potvrdil, že i biologický virus potřebuje svého hostitele, aby se mohl dále šířit, proto se tedy počítačový virus od svého biologického protějšku o moc neliší a v nedávné historii si je laická veřejnost pletla, čímž vznikala někdy i velká nedorozumění, která ještě více podporovala média a mezi veřejností docházelo mnohdy až ke zbytečné panice (Jalůvka, 2000).

Proč bychom se tedy měli počítačových virů bát? Kromě záměny s biologickým virem a následným zmatkům, které se šířily veřejností, mohl uživatel pocítit značné zpomalení počítače a dokonce mohl přijít o svá data.

Počítačový virus můžeme označit za první škodlivý software, který kdy vznikl a v 80. a 90. letech dominoval nad ostatními druhy malwaru, dnes se jedná spíše o vzácnost.

Počítačové viry můžeme dělit různými způsoby, např. podle umístění v paměti, podle koncepce návrhu a projevů chování, atd. Pro tuto práci a pro čtenářovu představu použijeme dělení podle cíle infekce, které popisuje Jalůvka (2000). Tímto rozdělením se specifikuje, co je terčem virového útoku.

2.2.1.1 Bootovací viry

První bootovací vir a zároveň úplně první malware vůbec, byl virus Brain. Jak uvádí Hák (2005, s. 18):

„Napsali ho dva bratři Basit a Amjads Farooq Alvi z Pakistánu – Lahore. Údajně ho dávali jako bonus cizincům, kteří si u nich v obchodě kupovali nelegální software. Nutno podotknout, že šlo o velice kvalitní zpracování viru, které způsobilo řadu lokálních epidemií.“

Uvedené viry se chovají tak, že obvykle přepíší svým vlastním kódem boot sektor diskety nebo Master Boot Record pevného disku, a původní přepsanou část boot sektoru uschovají na jiné místo disku. Taková virová infekce se potom šíří na jiné počítače pomocí boot sektorů disket, které přišly do styku s nakaženým systémem.

Jestliže virus zapíše původní boot sektor do kritické oblasti disku či diskety, jako je např. sektor obsahující část tabulky FAT, nebo hlavní diskový adresář, může dojít k tomu, že data na disku jsou navždy ztracena (Hák, 2005).

Obecně, infikovat bootovací sektor bylo strategicky výhodné. Virus sice mohl být na známém místě, ale dokázal se rozmístit dříve, než se spustil antivirový program, nebo jakékoliv jiné zabezpečení operačního systému (Aycock, 2006).

Ve své době byl tento typ viru velmi rozšířený a stal se základním stavebním kamenem pro tvorbu dalšího malwaru, v dnešní době se s ním již prakticky nesetkáme, hlavně kvůli tomu, že se téměř nepoužívají hlavní nositelky tohoto viru - diskety.

2.2.1.2 Souborové viry

Souborové viry infikují soubory, které jsou spustitelné. Na rozdíl od bootovacích virů je několik možností, kam mohou své tělo vložit.

Virus může být vložen na začátek velmi jednoduchého spustitelného souboru, např. *.COM, a systém bude považovat celý soubor jako kombinaci kódu a dat. Při spouštění bude celý soubor i s virem načten do paměti a kód se začne provádět skokem na začátek načteného souboru. V tomto případě virus, který se sám vložil na začátek souboru, dostává kontrolu nad celým infikovaným souborem.

Další možností je, že se virus vloží na konec spustitelného souboru. Ve srovnání s předchozí možností, je tato metoda vkládání jednodušší (Aycock, 2006).

Tyto dvě metody se dají odhalit tím, že se prodlouží délka infikovaného souboru, právě o tělo viru.

Třetí možností je přepisovací vir, jak název napovídá, svým kódem přímo přepíše hostitelský program, a tím jej znehodnotí (TrustPort, 2010). Proto se dá velmi snadno odhalit.

2.2.1.3 Makroviry

Když se začaly viry rozšiřovat, vznikla otázka, zda se dají přenášet i za pomoci textových souborů? V zásadě nedají. Jalůvka (2000, s. 41) uvádí, že:

„Základní podmínkou pro šíření viru je nutnost, aby infikovaný soubor byl spustitelný. Textové soubory nejsou v žádném případě spustitelné, a tudíž se nemohou jejich prostřednictvím šířit.“

Vzhledem k tomu, že textové soubory se sdílí mnohem častěji než spustitelné programy, našli tvůrci malwaru přece jen svou příležitost.

Některé aplikace, jako např. textové editory, mají možnost vkládat makra. Když aplikace načte dokument obsahující makro, může být způsobeno jeho automatické spuštění, což předává kontrolu makroviru. Některé aplikace varují uživatele o přítomnosti maker v dokumentu, ale varování mohou být uživatelem jednoduše ignorována (Aycock, 2006).

Šíření tohoto typu virů ještě podporuje skutečnost, že v minulosti, ale i současnosti nejpoužívanější textový editor z balíku Microsoft Office ukládá makra do stejného dokumentu s vlastním obsahem (Jalůvka, 2000).

2.2.2 Trojský kůň

Trojský kůň posloužil Řekům jako lest, aby mohli dobýt bájné město Trója. V podstatě i takto funguje stejnojmenný malware, až na to, že dobytým místem není Trója, ale uživatelovo zařízení.

Jedná se o volně stažitelné programy, které se tváří užitečně, např. hry, spořiče obrazovky, utility, ale také to mohou být antiviry (Jirovský, 2007). Uživatel si tedy ve víře, že si stáhnul úžasný program zdarma, stáhne kromě toho do svého počítače trojského koně, nebo může stáhnout pouze trojského koně, který pak v jeho zařízení, samozřejmě bez jeho vědomí provádí škodlivou činnost, ve většině případů se jedná o činnost destruktivního charakteru (Jalůvka, 2000; Petrowski, 2014).

Na rozdíl od virů není trojský kůň schopen sebereplikace (Aycock, 2006), šíření tohoto malwaru napomáhá samotný uživatel, který si ho stáhne do svého počítače. To však neznamená, že si trojského koně nemůže s sebou nést nějaký jiný druh malwaru a takto ho dál šířit.

Trojské koně mohou vykonávat různé činnosti, jak jsme již zmínili, většina z nich je destruktivního charakteru, takže od nich můžeme očekávat, že likvidují soubory na disku počítače, většinou se jedná o trojské koně s příponou *.BAT.

Existují trojské koně vytvořené primárně pro získávání přihlašovacích údajů, tím, že tento malware sleduje, které klávesy uživatel stiskl, vyfiltruje možné loginy a hesla, a následně je odesílá tvůrci malwaru.

Dále jsou trojské koně, tzv. droppery. Tváří se jako běžný spustitelný *.EXE soubor, ale po spuštění vypustí další malware do systému, který si s sebou nese. Odnožemi tohoto trojského koně jsou downloadery, ty si s sebou další malware nenesou, ale stahují ho přímo z Internetu.

Některé trojské koně dokonce zneužívají napadený počítač pro odesílání nevyžádaných zpráv, tzv. spamu (Hák, 2005).

2.2.3 Zadní vrátka

Za zadní vrátka (anglicky backdoor) považujeme jakýkoliv mechanismus, který se snaží obejít normální bezpečnostní kontrolu. Zadní vrátka mohou být vloženy buďto do již existujícího programového kódu, nebo se může jednat o samostatný program (Aycock, 2006).

Po tom, co tento malware infikuje cílový počítač, umožní hackerovi jeho vzdálené řízení.

Tento typ malwaru se hodně podobá komerčním produktům, které si uživatelé kupují, popř. jsou součástí operačního systému, pro vzdálený přístup ke svému počítači, jenže tento přístup k zařízení je samozřejmě nevyžádaný a uživatel o jeho přítomnosti neví. Zadní vrátka jsou také těžko zjistitelná, bezpečnostní prvky systému mohou snadno obejít, např. tím, že se vydávají za webový prohlížeč (Jirovský, 2007).

Zadní vrátka musí být připravena na podmínky cílového zařízení, je tím myšleno to, že mohou být vyžadována k přístupu hesla, mohou se v něm vyskytovat zašifrované soubory, apod.

2.2.4 Červ

Příchod prvního červa (anglicky worm) značně změnil u veřejnosti přístup k bezpečnosti počítačů. Červi infikují počítače tím způsobem, že se sebereplikují pomocí počítačové sítě, případně využitím síťových služeb. Na rozdíl od virů červi nepotřebují žádného hostitele. Sebereplikují se obecně ve formě síťových paketů, které se od úspěšně infikovaného systému směrují na další systémy v síti Internet. Šíření může být náhodné nebo dle určitého klíče. Pokud infikovaný paket dorazí do systému se specifickou bezpečnostní dírou a červu se podaří infikovat systém, poslouží toto infikované zařízení k dalšímu šíření infikovaných paketů (Hák, 2005).

Ačkoliv je hlavním úkolem červa jeho vlastní šíření, obvykle tento program může vykonávat i nějakou další činnost, jako např. vyřazení provozu počítače, nebo nějaké jeho součásti, odstraňování souborů, pomáhat šíření jiného malwaru (např. zadní vrátka). Dále červi dokáží na infikovaném zařízení najít taková osobní data, která mohou přinést autorovi červa nějaký zisk. Samozřejmě červ si s sebou nemusí nést žádnou další činnost, ale i tak se může jeho samotným šířením vyskytnout nějaký vedlejší efekt, např. snížení rychlosti Internetu.

Červi se dají dělit podle způsobu jejich šíření. Máme červy e-mailové, kteří začnou odesílat infikované zprávy na e-mailové adresy, které najdou v cílovém zařízení. Často se tyto zprávy odesílají z e-mailu uživatele napadeného zařízení, tudíž korespondence je věrohodná a nic nebrání tomu, aby byla infikovaná zpráva otevřena.

Internetoví červi zase využívají všechny síťové prostředky, aby našli v síti zranitelný počítač a mohli ho pak napadnout.

IM[1] a IRC[2] červi využívají pro šíření komunikaci v reálném čase, kdy se v případě IM odesílá odkaz na infikované stránky, a v případě IRC se odesílá infikovaný soubor, všechno se opět děje pod účtem uživatele infikovaného zařízení.

Červi využívající sdíleného prostoru kopírují svůj škodlivý kód do sdílených úložišť, kde má uživatel k dispozici soubor ke stažení, který nevzbuzuje podezření, typickým příkladem jsou weby typu Ulož.to, kde se sdílí i nelegální obsah a pokud se soubor jeví jako např. film, stáhne si uživatel do počítače červa, který po spuštění infikuje zařízení (Počítačový červ, 2014).

[1] Zkratka pro Instant messaging, internetová služba sloužící pro chatování v reálném čase (např. ICQ)
[2] Zkratka pro Internet relay chat, internetová služba sloužící pro chatování v reálném čase přes tzv. kanály

Králík

Termínem králík (někdy též bakterie) lze označit speciální druh červa, který se velmi rychle dokáže replikovat.

Jedná se o samostatný program, který se šíří stejným způsobem jako červ, s tím rozdílem, že se po infekci cílového zařízení z toho původního sám odstraní. Jinými slovy existuje pouze jedna kopie králíka v celé síti, dá se říct, že skáče z jednoho zařízení na druhé, čímž připomíná právě svůj zvířecí protějšek.

Ve skutečnosti je tento typ malwaru vzácný, ale o to víc zajímavý (Aycock, 2006).

2.2.5 Spyware

Spyware je druh malwaru, který shromažďuje informace z infikovaného zařízení a vysílá je někomu jinému. Informace, které spyware bez vědomí uživatele sbírá, se liší podle toho, jaký je autorův záměr. Hodnotu mají hlavně jména a hesla, e-mailové adresy, které může později hacker využít pro spam, dále bankovní účty, čísla kreditních karet a v neposlední řadě licenční klíče softwaru, což napomáhá softwarovému pirátství (Aycock, 2006). Někdy se však autoři tohoto druhu malwaru hájí tím, že jejich zájmem je sbírat pouze informace o navštívených stránkách a nainstalovaných programech pro potřeby cílené reklamy (Hák, 2005).

Spyware není schopen sebereplikace, na cílové zařízení se může dostat různými způsoby. Jedním z častých způsobů je šíření jako doplněk programů, přičemž uživatel souhlasí s nainstalováním hlavního programu, tento program mu posléze vnutí instalaci nějakého doplňku, a neznalému uživateli, který tuto instalaci potvrdí, se do zařízení pod touto záminkou nainstaluje spyware, o jehož přítomnosti se však nedozví (Zachar, 2009).

2.2.6 Dialer

Za dialer označujeme speciální případ malwaru, který se týká zejména uživatelů Internetu připojujících se přes modem. Dokáže přesměrovat vytáčení čísla pro internetové připojení na linky s vysokými sazbami, např. 60 Kč za minutu, uživatel nemá o dialeru ani ponětí, dokud mu nepřijde účet za telefon. Mohlo by se říct, že tento typ malwaru je již na ústupu, jelikož se využívá hlavně ADSL a Wi-Fi připojení k Internetu, jenže opak je pravdou (Hák, 2005).

2.2.7 Adware

Adware je druh malwaru, který znepříjemňuje práci na zařízení reklamou. Nejčastěji se s ním setkáváme v aplikacích, které bývají zdarma. Při instalaci takových aplikací dáváme souhlas s licenčním ujednáním, čímž dáváme i souhlas k instalaci adwaru do našeho zařízení. Tento druh adwaru je neškodný, i když může být pro mnohé uživatele „otravný“, ale ve své podstatě nám autor tohoto programu dal něco zdarma a chce po nás, abychom si alespoň prohlédli reklamu, která ho vlastně finančně podporuje (Hák, 2005; Rouse, 2012).

Dalším případem výskytu adwaru jsou vyskakovací okna (tzv. pop-up), která se objevují při surfování na Internetu, nejčastěji na nějakých nedůvěryhodných stránkách.

Tato vyskakovací okna nás lákají na různé soutěže, nebo nám dokonce oznamují, že jsme již vyhráli, nabízí nám i výhodnou koupi zboží a spoustu dalšího. Tím, že na tyto reklamy klikneme, riskujeme nainstalování dalšího malwaru do našeho zařízení.

Spyware a adware spolu také mohou spolupracovat, spyware monitoruje činnost na cílovém zařízení, zajímají ho např. stránky, které vyhledáváme nejčastěji na Internetu, výsledky pak předá adwaru, který nám pak posílá cílené reklamy (Zachar, 2009).

Dá se říct, že tohoto procesu využívá i např. Facebook nebo Google, sbírají data o uživatelově osobě a pak mu nabízí cílenou reklamu (Kasík, 2014).

2.2.8 Rootkit

Rootkit je jedna z nejhorších forem malwaru, i když sám o sobě nepředstavuje žádné nebezpečí. Slouží k tomu, aby maskoval činnost jiného malwaru a tím znemožňuje např. antivirovým programům jeho nalezení.

Za nejznámějším rootkitem stojí společnost Sony, tento rootkit se tajně instaloval, když bylo hudební CD od této společnosti vloženo do počítače. Tento rootkit měl zabránit uživateli kopírovat CD, jenže kromě toho byly společnosti Sony odesílány i údaje o uživatelově aktivitě, samozřejmě všechno se dělo bez vědomí uživatele a antivirů. V tomto případě byla nositelem rootkitu komerční aplikace, ale ve většině případů bývá nositelem rootkitu trojský kůň (Hosch, 2013).

Rootkity se dají jen stěží odstranit, protože bývají zakotveny v operačním systému a nelze tedy zaručit, že by se odstranily všechny škodlivé kódy (Nykodýmová, 2006).

Jedinou jistotou bývá naformátování disku a reinstalace systému.

2.2.9 Logická bomba

Za logickou bombu označujeme buďto samostatný program, nebo část kódu vloženou do jiného programu. Programový kód si s sebou nese náklad, neboli to, jakou činnost má v systému vykonat a dále si s sebou nese nějakou logickou podmínku, za jaké se tento kód vykoná, např. v určitý čas, nebo při stisknutí klávesy, apod. (Hák, 2005).

Aby se logická bomba dostala do počítače, musí ji tam umístit někdo, kdo k němu má přístup, např. zaměstnanec na firemní počítač, nebo se může přenášet pomocí jiného druhu malwaru, např. virus, červ (Dunnigan, 2004).

2.2.10 Scareware

Scareware je škodlivý program, který se obvykle tváří jako antivirus, antispyware, popř. komerční firewall nebo čistič registrů. Tento program posléze najde na počítači problémy, pro jejichž odstranění musí uživatel zaplatit.

Samozřejmě problémy jsou vymyšlené, a pokud uživatel zaplatí, je zaručeno, že o své peníze přišel zbytečně a v horším případě si do počítače stáhne ještě nějaký jiný druh malwaru.

Za scareware také označujeme software, který je určen spíše k postrašení hororovými obrázky, které se objevují na monitoru, případně se může jednat o strašidelné zvuky a videa (Rouse, 2010).

2.2.11 Zombie/Bot

Pod pojmem zombie nebo bot rozumíme malware, který útočníkovi umožňuje ovládat uživatelův počítač a organizovat, za pomoci tohoto zařízení útoky na další počítače v síti Internet, takové zařízení pak také nazýváme jako zombie nebo bot. Útočníci někdy využívají několik počítačů, aby vytvořili tzv. zombie armádu, popřípadě botnetovou síť.

Uživatel takto napadeného počítače obvykle o ničem neví, protože i nadále svůj počítač dokáže ovládat, podezření u zkušenějších uživatelů může vyvolat skutečnost, že je zařízení pomalejší než obvykle (Criddle, 2010).

2.2.12 Ransomware

Ransomware je škodlivý kód šířící se pomocí e-mailových příloh, nebo jako součást programů a nedůvěryhodných stránek.

Způsobuje nedostupnost souborů tím, že tyto položky zašifruje a od uživatele vyžaduje zaplacení určité částky, po které by se mu měly tyto soubory zpřístupnit, bohužel zaplacení částky ve většině případů nepomůže.

Existuje i ransomware, který sice soubory nezašifruje, ale zamezí přístup do systému, buďto tím, že obviní uživatele ze stahování nelegálního materiálu z Internetu a hacker požaduje zaplacení pokuty, popřípadě jde o falešnou aktivaci Windows.

Některé ransomwary tajně zašifrují data a uživateli se neobjeví žádná žádost o výkupné, tvůrce tohoto škodlivého kódu totiž počítá s tím, že uživatel po zjištění, že mu někdo zašifroval soubory, bude pátrat na Internetu, jak tato data získat zpátky. V tuto chvíli mu tvůrce malwaru vnutí koupi anti-ransomware softwaru (Rouse, 2014).

Krásným příkladem ransomwaru, o kterém se v poslední době hodně mluvilo i v médiích, je policejní „virus“, popřípadě i FBI „virus“. Čtenář si jistě všimne, že označení „virus“ je naprosto nevhodné, protože po nakažení tímto „virem“ se uživateli napadeného zařízení zablokuje přístup do systému a zobrazí přes celou obrazovku zprávu od Policie České republiky, v níž je uživatel obviněn ze stahování nelegálního softwaru, za což mu hrozí vysoký trest, ale nabízí se mu možnost zaplatit pokutu. Po zaplacení je uživateli přislíbeno, že celá věc bude smetena ze stolu. Jedná se však o podvod a peníze přistanou v kapse podvodníkovi (Padrta et. Nykles, 2013).

2.2.13 Speciální případy malwaru

Následující druhy několik autorů uvádí jako speciální případy malwaru, ačkoliv splňují definici pouze z části.

Například Hák (2005) je řadí hned vedle takových hrozeb, jaké jsou spyware a adware. V dnešní době se jedná o velmi rozšířené hrozby, i když se nejedná přímo o škodlivé kódy, ale nesou s sebou stejné, ne-li horší bezpečnostní rizika jako ostatní druhy malwaru a proto jsou zařazeny i do této práce.

2.2.13.1 Hoax

Slovo hoax v češtině znamená smyšlenku. Nejčastěji byl tento termín spojován s aprílovými žertíky, avšak s příchodem Internetu tyto žertíky nepřipadají pouze na 1. duben, ale dá se říct, že jsou na denním pořádku. Bohužel ne vždy ve světě Internetu existuje slovo „Apríl“, které by napálenému naznačilo, že byl opravdu oklamán a mnohdy ani nejde o tak nevinné lži.

Pomocí Internetu se denně šíří několik desítek poplašných zpráv, které například slibují finanční pomoc nemocnému dítěti, pokud čtenář přepošle zprávu dál. Další zase varují před novou nemocí a tím vyvolávají mezi čtenáři paniku. Fantazii se zde meze nekladou.

Jak se tedy může stát hoax speciálním případem malwaru? V podstatě tehdy, když nějaký škodolibec vydá do oběhu poplašnou zprávu o nebezpečném malwaru s tím, že vyléčit počítač může uživatel např. smazáním nějakého souboru. Samozřejmě ve skutečnosti žádný takový malware existovat vůbec nemusí a tím, že uživatel smaže nějaký soubor důležitý pro běh systému, může zapříčinit i jeho celkový kolaps.

Co víc, může hoax být i prostředkem ke sběru kontaktních informací, konkrétně e-mailových adres, které pak může kdokoliv využít třeba i k šíření dalšího malwaru a jako bonus může při masovém šíření hoaxu dojít i k přetížení serverů.

Zkušený uživatel může hoax poznat během pár vteřin, zejména kvůli žádosti o přeposlání dalším lidem a mnohdy nereálnými účinky smyšlené hrozby (HOAX, 2015).

2.2.13.2 Phishing

Pojem phishing vychází ze složení dvou anglických slov „phreaking“, což můžeme volně přeložit jako „nabourání“ a „fishing“, česky „rybaření“. Při slově rybaření si může leckdo představit zábavu, ale bohužel v této „hře“ se stává lovenou rybou nepoučený uživatel.

V současnosti se jedná o velmi rozšířenou hrozbu, která často bývá středem pozornosti v médiích, nejlépe o ní pojednává text od Petrowského (2014).

Nejčastěji se zprávy týkají takového phishingu, při kterém je nainstalována na bankomat buďto falešná čtečka karet nebo falešná klávesnice, s jejíž pomocí pak může pachatel odhalit číslo karty a PIN kód bez vědomí vlastníka. V poslední době se častěji pro tento druh phishingu používá název skimming (česky „odčerpání“).

Dalším typem phishingu, se kterým se setkáváme možná ještě častěji než se skimmingem, je tzv. e-mailový spoofing. V tomto případě dochází k rozesílání podvodných e-mailů s požadavkem o sdělení citlivých údajů.

Například se může jednat o e-mail, který na první pohled vypadá, že přichází z banky a žádá ověření uživatelova účtu, tím, že sám uživatel zpátky odešle své přihlašovací údaje do internetového bankovnictví. V takovém případě, pokud uživatel tyto údaje poskytne, může s nimi tvůrce phishingového útoku naložit jak se mu zlíbí a uživateli, který pak najde svůj účet prázdný, zůstanou jen oči pro pláč.

Propracovanější phishingové útoky posílají v e-mailu i odkaz na duplikáty webových stránek, tyto webové stránky nelze na první pohled rozlišit od originálů a samozřejmě na uživatele působí věrohodněji než pouhý e-mail.

Podvodné e-maily mohou také jako bonus obsahovat přílohu, která může vypadat např. jako výpis z účtu, ve skutečnosti se však jedná o malware a zde záleží jen na fantazii útočníka, k jakému účelu malware použije.

Dalším druhem phishingu je pharming (česky farmaření), při kterém je uživatel přesměrován na falešnou stránku v momentu, kdy se nachází na originální stránce. Typicky se tak stává na sociálních sítích jako je Facebook, například při hraní her je uživatel přesměrován na falešnou Facebookovou stránku, kde se musí opět přihlásit. Pokud poskytne své údaje, dostanou se do rukou útočníkovi a ten si pak jeho účet může používat k dalším účelům, například pro další phishingové útoky. Pokud uživatel nijak nepátrá po tom, kam své údaje zadává, nic nepozná, protože po zadání údajů je opět přesměrován na originální stránky Facebooku.

Ve skutečnosti k žádnému odhlášení vůbec nedošlo a i přes to, že by uživatel zadal nesprávné údaje, byl by přesměrován na originální stránky, tak jako při správně zadaných údajích.

2.3 Malware na ostatních digitálních zařízeních

V předchozí kapitole jsme se zaměřili na druhy malwaru, které napadají převážně počítače. Přece jen je již toto téma trochu zažité a této problematice se věnuje celá řada publikací, i když má každá svůj vlastní úhel pohledu.

S příchodem chytrých zařízení se na nich začal malware pomalu, ale jistě objevovat také. Bohužel v tomto případě existuje jen malé procento publikací, které by

se touto problematikou zabývaly, zejména kvůli tomu, že největší rozmach tohoto malwaru přišel teprve před několika lety.

První hrozbou se v roce 2004 stal speciální bluetooth červ jménem Cabir, který využíval bezpečnostních děr v systému Symbian, v podstatě však tento červ nepředstavoval žádné vážné bezpečnostní riziko, pouze se dokázal sám bez vědomí uživatelů šířit pomocí technologie Bluetooth a hodně rychle se kvůli němu vybíjela baterie. Na dnešních mobilních operačních systémech by se však tento červ nemohl tak jednoduše bez pozornosti dále šířit, protože spojení Bluetooth vyžaduje bezpečnostní potvrzení (Kaspersky Lab, 2014; Petrowski, 2014).

V roce 2005 byla objevena vylepšená verze červa Cabir, tento červ nesl název CommWarrior, tento se uměl šířit nejen pomocí Bluetooth, ale také pomocí MMS. To byl větší problém, protože MMS museli uživatelé napadených telefonů zaplatit a navíc některé varianty tohoto červa dokázaly vypínat telefon.

V témže roce byl objeven i první trojský kůň na mobilním zařízení, v podstatě měl stejnou funkci jako ten počítačový. Dostal název Doomboot, protože ho tvůrce vydával za hru Doom, nejen, že nainstaloval do telefonu malware Cabir nebo CommWarrior, ale také zabránil zavedení systému, což znamená, že pokud uživatel po napadení systému Symbian telefon restartoval, s největší pravděpodobností ho znovu nezapnul.

Rok 2006 přinesl dalšího trojského koně, tentokrát se vydával za Java program umožňující stahování dalších užitečných programů zdarma, což znělo velmi lákavě, ovšem program ve skutečnosti odesílal prémiové SMS na číslo do Ruska a to tak lákavé nebylo (Hypponen, 2006).

Ve stejném roce se objevila novinka v podobě spywaru, která posílala neoprávvněným osobám výpisy hovorů a kopie textových zpráv. S příchodem nových mobilních operačních systémů jako je Android, iOS, Windows Phone, atd. se šíří malware stále rychleji a to zejména kvůli tomu, že se mobilní zařízení stala přístupnější pro připojení k Internetu, ale i ke stahování aplikací a dalších dat, čímž si vlastně uživatelé přizpůsobují zařízení k vlastním potřebám.

Vzhledem k tomu, že se mobilní zařízení stále více podobají počítačům, není divu, že i malware je velmi podobný tomu počítačovému. Výhodou pro útočníky oproti počítačům je právě to, že mobilní telefony a některé tablety se používají nejen pro již uvedené činnosti, ale i pro telefonování a posílání SMS a MMS, které jsou přímou bránou k penězům, z čehož si může útočník udělat zlatý důl (Barker, 2014).

Garnaeva a kol. (2014) uveřejnili na webu Securelist.com roční přehled pod záštitou společnosti Kaspersky Lab, přičemž bylo sděleno, že od začátku listopadu 2013 do konce října 2014 bylo zaznamenáno 1 363 549 jedinečných hrozeb na mobilních zařízeních, které používají jako operační systém Android, oproti tomu předchozí rok za stejně dlouhou dobu to bylo „pouze“ 335 000 hrozeb. Z toho 53 % mobilního malwaru je vytvořeno za účelem krádeže peněz.

Ve většině případů se můžeme setkat s trojskými koni, ale hrozbou jsou i zadní vrátka, červi, adware, spyware, dialer a dokonce byl již zaznamenán i případ rootkitu, zombie, scarewaru a ransomwaru. Samozřejmě se nevyhneme i phishingovým útokům a hoaxu.

Výhodou jednodušších typů mobilního malwaru od toho počítačového je možnost odstranění pouhou odinstalací škodlivé aplikace, ale samozřejmě ty složitější se dokáží proti takovým uživatelovým zákrokům dobře bránit (Niemeyer et. Kratochvíl, 2011).

Dokonce jsou již známé i případy, kdy hackeři využili pro rozesílání spamu i jiné zařízení než tablety a mobilní telefony, jednalo se o chytrou chladničku připojenou k Internetu a chytré televize.

2.4 Nejvýznamnější počítačový malware v dosavadní historii

Je to téměř 30 let, co světlo světa spatřil první malware, za tu dobu přibylo několik milionů dalších druhů. I když některé typy malwaru přežily sotva pár minut, některá jména se vryla do paměti společnosti dodnes.

Pro tuto bakalářskou práci využijeme řazení, které zvolil Bell (2014) ve svém článku na serveru Bullguard.com. Jde o malware Storm, Melissa, MyDoom, Sasser, Anna Kournikova, Morrisův červ, I LOVE YOU, SQL Slammer, Nimda a Conficker. Tento malware byl velmi významný, nejen tím, že změnil celkový přístup společnosti k bezpečnosti, ale díky němu byly odhaleny slabiny v počítačových systémech, což vedlo k jejich pozdější nápravě.

V dnešní době se jen zřídkakdy objeví nový typ malwaru, většinou jde však alespoň o inspiraci výše uvedeným. I když se všechen uvedený malware týká operačního systému Windows, neznamená to, že by se na ostatních operačních systémech malware nevyskytoval a taková tvrzení můžeme označit za mýtus, zářným příkladem je např. trojský kůň Flashback, který napadal výhradně počítače s operačním systémem Mac, stejně tak existuje malware i pro Linux.

Jednoduše Windows patří mezi nejrozšířenější počítačové systémy a jeho upravené verze můžeme najít i v takových zařízeních jako jsou jukeboxy nebo bankomaty, proto si i tvůrci malwaru vybírají převážně tento systém.

2.4.1 Storm

Tento trojský kůň Storm (bouře) získal od počítačových uživatelů svoje jméno díky tomu, že byl součástí e-mailu, který měl informovat o ničivé bouři, která zasáhla Evropu začátkem roku 2007.

Později se šířil i jako informační e-mail o dalších událostech nejen o katastrofách, nebo jako falešné oznámení o doručené elektronické pohlednici (Dočekal, 2007).

Jakmile uživatel otevřel e-mail s takovouto přílohou, trojský kůň vypustil svůj náklad, čímž vytvořil z počítače zombie. To umožňovalo útočníkovi použít infikované počítače jako prostředek k dalším útokům.

Za svou kariéru dokázal tento malware vytvořit dosud největší botnetovou síť, protože se mu podařilo nakazit odhadem až 10 milionů počítačů (Bell, 2014; Strickland, 2008).

2.4.2 Melissa

Jedná se o makrovir pojmenovaný po tanečnici z Miami, který upravil a rozeslal do počítačového světa v roce 1999 David L. Smith. Ten si za svoje počínání musel později odpykat 20 měsíců ve vězení, přitom mu hrozilo původně až 10 let.

Tento makrovir se nejdříve objevil na diskuzním fóru jako dokument obsahující hesla na 80 pornostránek. Později k šíření stačily pouze e-maily, které vypadaly jako by přišly od známého člověka, ale obsahovaly jako přílohu infikovaný dokument.

Po otevření dokumentu se počítač infikoval a Melissa si dokázala obstarat své šíření dál tím, že poslala stejný dokument na prvních 50 e-mailových adres, které našla v programu Outlook na napadeném počítači. Melissa dokázala napadnout několik milionů počítačů a přetížit několik desítek serverů (Erben, 2014; Bell, 2014).

2.4.3 MyDoom

Jedná se o červa, který je také znám pod názvem Novarg. I jako předchozí uvedené hrozby se šířil e-mailem, jeho předmět zněl obvykle velmi důležitě, a proto ho uživatelé otevírali. Dále se vyskytl na webech určených pro sdílení dokumentů.

Jakmile je počítač infikován nainstaluje se do napadeného počítače backdoor, což umožňuje útočníkovi připojit se k zařízení bez vědomí uživatele. V dnešní době se s různými variantami MyDoom můžeme stále setkat.

Na vrcholu své slávy tento malware způsobil vypnutí serverů Google skoro na celý den. Nikdy se nevypátralo, kdo stál za vznikem tohoto červa, i když byla vypsána odměna 250 000 € za nalezení tohoto tvůrce (Bell, 2014; Strickland, 2008).

2.4.4 Sasser

Na své 18. narozeniny vypustil do oběhu Němec Sven Jaschan červa Sasser. Napadal počítače připojené k síti Internet tím, že využíval bezpečnostní chybu ve Windows, konkrétně chybu v LSASS (Local Security Authority Subsystem Services), paradoxně má tato služba za úkol spravovat zabezpečení v systému Windows.

Sasser znemožňoval plynulou práci na počítači, ten totiž zamrzal, nešel jednoduše vypnout a docházelo k pádům celého systému.

I když Microsoft vydal na chybu v LSASS záplatu, bylo tímto červem nakaženo několik milionů počítačů a způsobilo to mnoho problémů i některým institucím (Bell, 2014).

2.4.5 Anna Kournikova

Červ pojmenovaný po známé tenistce sliboval uživateli její privátní fotografie. Vzhledem k tomu, že Anna Kournikova je nejen nadaná tenistka, ale i krásná žena, byl o tyto fotografie zájem, a proto odkaz, který přišel e-mailem, uživatelé bezmyšlenkovitě otevírali.

Sám o sobě by tento červ až tak škodlivý nebyl, nebýt toho, že se bez uživatelova vědomí sám odesílal na adresy všech jeho známých, které si červ našel v Outlooku a tím přetěžoval e-mailové servery.

Tohoto červa vytvořil Dán Jan de Vit, zajímavostí je, že na to nepotřeboval žádné zvláštní programátorské znalosti, jednoduše použil generátor malwaru, který jen obalil svou lží, aby přílohu vůbec uživatelé otevřeli (Bell, 2014).

2.4.6 Morrisův červ

Jak název napovídá, jedná se o červa, kterého vytvořil Robert Tappan Morris, tehdy ho vyslal do sítě Arpanet, což byl předchůdce dnešního Internetu. Morris se později obhajoval tím, že chtěl pouze zjistit, kolik počítačů je k Arpanetu připojeno, ale kód infikoval kolem 6 000 počítačů a výrazně zpomalil jejich běh a některé počítače dokázal infikovat i vícekrát. Tímto počinem dokázal Morris změnit pohled společnosti na zabezpečení počítačů (ČT24, 2013).

2.4.7 I LOVE YOU

V roce 2000 byl trojicí studentů Onel de Guzman, Irene de Guzman a Reonel Ramones vytvořen a následně vypuštěn červ I LOVE YOU napsaný v jazyku Visual Basic.

Přes pouhou noc stačil napadnout několik desítek tisíc počítačů, včetně zařízení FBI nebo britského parlamentu.

Tento červ využíval především zvědavosti uživatelů, kteří rozklikli e-mail, aby si přečetli falešný milostný dopis. Místo toho byl jejich počítač infikován červem, který se rozeslal na všechny e-mailové adresy, které našel v Outlooku. Dále dokázal nahrazovat soubory svou kopií, případně přidávat nové soubory, dokázal dokonce s pomocí dalšího malwaru krást hesla.

Odstranit tohoto červa se podařilo thajskému programátorovi jménem Narinnat Suksawat.

Vzhledem k tomu, že filipínské zákony neřešily problematiku malwaru, vyvázla trojice studentů bez trestu. Pro Filipíny to znamenalo zejména to, že později v tomto roce vydaly zákon, který považuje psaní malwaru za nezákonné (Erben, 2014).

2.4.8 SQL Slammer

SQL Slammer je červ, který dokázal v roce 2003 napadnout během pouhých deseti minut více než 75 000 počítačů a každou další minutou se tento počet rapidně zvyšoval, patří tak mezi nejrychleji se šířící malware všech dob. Ironií je to, že mohl být odstraněn jednoduše restartem počítače a nainstalováním příslušné záplaty, aby se malware nemohl objevit na počítači znovu.

Napadal zejména SQL servery firem tím, že se šířil pomocí sítě, některé servery firem vyřadil přetížením z provozu, u dalších zpomalil provoz.

Tento červ napáchal mnoho škod, některé lety musely být zrušeny, nefungovaly bankomaty americké banky a ve městě Seattle dokonce došlo k přetížení tísňové linky 911 (Bell, 2014).

2.4.9 Nimda

Tento malware se během pouhých 25 minut dokázal stát nejrozšířenějším červem své doby.

Měl nejednu zákeřnou vlastnost, dokázal totiž nejen sám sebe posílat pomocí e-mailových příloh, ale také pak použít napadený počítač k prozkoumání webu kvůli zranitelným webovým stránkám. Originální stránky si pak podle sebe upravil, aby nabízely soubory ke stažení, ale ve skutečnosti tyto soubory obsahovaly opět tohoto zákeřného červa.

Třešničkou na dortu je možnost měnit a poškozovat soubory uložené na pevném disku uživatelova počítače (Bell, 2014).

2.4.10 Conficker

Invaze tohoto červa přišla v roce 2008, napadl více než 15 milionů počítačů. Dokázal ve Windows znepřístupnit aplikace, které mají na starosti zabezpečení počítače. Také počítač znepřístupnil všem aktualizacím.

Dále Conficker stahoval do napadeného zařízení další malware, který následně kradl informace a přeposílal je dál.

Firma Microsoft vydala později aktualizaci, která měla ochránit ještě neinfikované počítače před Confickerem, ale později se zjistilo, že Conficker dokázal

využít automatického spouštění tzv. AutoPlay po připojení USB flash disku, tato funkce umožňuje uživateli výběr programu pro otevření souboru uloženém na USB zařízení. Conficker jen přidal duplikát možnosti „Otevřít složku a zobrazit soubory“, pokud uživatel vybral tuto možnost, byl červ vypuštěn do systému.

Mezi počítači, které tento červ napadl, byly i ty patřící francouzskému námořnictvu, Ministerstvu obrany Velké Británie, ale i německým ozbrojeným silám.

Microsoft kvůli tomuto malwaru udělal i zvláštní opatření jen proto, aby zjistil, jak se ho zbavit. Tohoto opatření se účastnily skoro všechny organizace, které chtěly zachovat bezpečný Internet (Bell, 2014).

2.5 Kybernetická kriminalita

Je důležité si uvědomit, že počítače, mobilní telefony a další digitální zařízení nejsou pouze předmětem trestného činu, ale také mohou být nástrojem k páchání takovýchto činů, toto pojetí označujeme pojmem kybernetická kriminalita (Jirovský, 2007).

Když se podíváme do trestního zákoníku, konkrétně Zákon č. 40/2009 Sb., nenalezneme zde přímo žádný oddíl, který by se této problematice věnoval, je to zejména z toho důvodu, že mnoho zákonů se dá aplikovat do různých situací, kde nemusí být prostředkem, popř. předmětem trestného činu digitální zařízení a samozřejmě je zbytečné vytvářet novou kategorii, která by pouze vytvářela duplicity (Macháček, 2013).

Mezi zákony, které se konkrétně týkají přímo digitálních zařízení, patří § 230 Neoprávněný přístup k počítačovému systému a nosiči informací viz Příloha 1 a § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat viz Příloha 2. Dále § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti viz Příloha 3. Tyto zákony spadají pod oddíl Trestné činy proti majetku (Matejka, 2001).

Co je tedy nejdůležitější vědět je, že samotná tvorba malwaru v našem státě není trestná, trestné je pokud se prokáže, že se autor malwaru pokusil jeho pomocí napáchat škodu, zneužít informace, atd. nebo se mu to skutečně povedlo. Samozřejmě záleží na konkrétním soudu, jak danou situaci vyhodnotí a jestli se vůbec najde skutečný tvůrce malwaru.

2.6 Důvody tvorby malwaru

V této kapitole si uvedeme nejčastější důvody, proč vůbec malware vzniká, ale je důležité si uvědomit, že je to velice individuální věc.

Často ve společnosti slyšíme o hackerech v negativním slova smyslu. Původně se však pojmem hacker označoval specialista ve svém oboru, někdo kdo zná dokonale systém, na kterém pracuje. Hackerům jde především o to, dostat se v systému tam, kam se ještě nikdo nedostal, tedy překonat hranice, ale nijak neškodit. V současné době je to ovšem tak, že když už se hacker někam dostane, využije toho ke svému prospěchu (Jalůvka, 2000).

Tvůrci malwaru však ani nemusí být odborníky, jak jsme již zmínili v této bakalářské práci, červ Anna Kournikova byl vytvořen generátorem malwaru a nebylo zde třeba mít nějaké speciální programátorské schopnosti. Na druhou stranu se spíše setkáváme s malwarem vytvořeným programátory, než obyčejnými lidmi se základními znalostmi digitálních zařízení.

Jalůvka (2000) jako motivaci pro tvorbu malwaru uvádí touhu po slávě, dále prostředek seberealizace, čímž si autor malwaru dokazuje své schopnosti. Dále zmiňuje lidskou zvědavost, kdy se programátoři snaží si osvojit principy toho, jak malware funguje. Následuje i snaha škodit, ničit a ubližovat, ať už z pomsty nebo opět kvůli tomu si něco dokázat, případně tvůrce malwaru toto nedělá kvůli sobě, ale třeba se tímto způsobem snaží pomoct svému blízkému nebo firmě, která si ho najala. S tímto úzce souvisí i ekonomický zisk, často se říká, že některé druhy malwaru vymýšlejí lidé z firem, které se zabývají tvorbou programů na ochranu digitálních zařízení, ale tato skutečnost ještě nebyla u žádné firmy dokázána. Existují i názory, že si tvůrce malwaru najímají firmy také proto, aby ověřili své zabezpečení. Také se v médiích občas mluví o kybernetické válce. Pokud by došlo k nějakému mezinárodnímu konfliktu a vypukla by válka, předpokládá se, že zbraněmi v této válce by byly počítače. Mezi ekonomický zisk by pak patřila i krádež údajů k bankovním účtům za pomoci malwaru a následné zneužití.

2.7 Ochrana před malwarem

Pokud bychom se vrátili v tomto textu o několik kapitol zpět, zjistili bychom, že možnosti šíření malwaru jsou rozmanité, proto je důležité vědět, jak se proti němu co

nejúčinněji bránit. Jistě se shodneme, že nejlepší situace je, když zařízení není napadeno vůbec, v tomto případě je tedy důležitá prevence.

Prevencí budeme rozumět všechny postupy uživatele digitálního zařízení, díky kterým se vyhýbá napadení malwarem.

Základem prevence je mít své zařízení aktualizované, neboť aktualizace systému a jeho aplikací by měla zajišťovat záplatu bezpečnostních děr, které byly v průběhu používání odhaleny. Zde mohou samozřejmě narazit na problém lidé, kteří využívají nelegálním způsobem získaný operační systém či další programy a mají zakázané aktualizace, takovýto neaktualizovaný software je přímo rájem pro výskyt malwaru.

Dále je důležitá rozvaha samotného uživatele, měl by být schopen vyhodnotit situaci, vyhnout se návštěvě podezřelých stránek, stahování z neznámých zdrojů, otevírání e-mailových příloh přicházejících od neznámých uživatelů a klikání na vyskakující reklamy, v neposlední řadě by si měl volit bezpečná hesla a tato dále nikomu nesdělovat.

Použití softwarové ochrany je taktéž při prevenci žádoucí, neboť dokáže nezvané návštěvníky v našem systému včas zachytit a případně po napadení počítače izolovat nebo i zneškodnit. Na našem digitálním zařízení by neměl chybět antivirový program, čtenář by jistě mohl namítnout, že jsme v předchozích kapitolách uvedli, že se s viry již moc často nesetkáváme a tedy není potřebné mít nainstalovaný program konkrétně proti virům. Není to však pravda, antivirový program nás nechrání jen před viry, totiž v době, kdy byly pouze viry, dostal tento program takovýto název a ten se používá dodnes, i přes skutečnost, že si poradí i s dalšími druhy malwaru (Hák, 2012).

Jednotlivé antivirové programy mohou pracovat na základě různých technik. Jalůvka (2000) uvádí mezi tyto techniky skener, který analyzuje řetězce potenciálně škodlivého kódu a porovnává je s již známými řetězci odhalených škodlivých kódů. Zde vzniká riziko falešných poplachů.

Dále uvádí heuristickou analýzu, ta byla zřízena z toho důvodu, že některé druhy malwaru umí škodlivé řetězce skrýt a tím obejít antivirovou ochranu používající ke kontrole skener. Heuristická analýza kontroluje jednotlivé příkazy zadané v podezřelém programu na základě pravidel, která určují, jak se malware chová v určitých případech. Pokud by některý z příkazů odpovídal chování malwaru, upozorní na to uživatele, který pak posoudí, jestli se nejedná o falešný poplach. Samozřejmě i tuto techniku dokáží tvůrci malwaru obejít.

Clean je jednou z dalších technik, má za úkol odstranit malware, který lze bez poškození dalších programů, případně celkově systému smazat. Efektivně dokáže odstranit prodlužovací viry, které své tělo vkopírují do kódu nějakého programu, clean kontroluje změny softwaru a pokud přijde na to, že byl kód programu prodloužen, tento vir odstraní. Bohužel ne všechen malware lze takto jednoduše odstranit.

Další technikou je rezidentní štít, ten funguje v reálném čase a nepřetržitě na pozadí systému kontroluje soubory, se kterými uživatel právě pracuje. Soubory kontroluje na základě databáze virových pravidel, v případě napadení zařízení malwarem, rezidentní štít rychle zareaguje a nakažený soubor odstraní, případně izoluje nebo vyléčí.

Monitor diskových změn pracuje v podstatě jako clean, zaznamenává si všechny atributy souborů jako je délka, datum změny, apod. Rozdíl je v tom, že monitor diskových změn samovolně nemaže části souborů.

Jalůvka (2000) ještě rozděluje softwarovou ochranu počítače na jednoúčelové programy, které jsou opravdu vytvořeny pouze pro odstranění jednoho konkrétního škodlivého kódu a dále na programové balíky, které obsahují jednotlivé programy, které pracují na výše zmiňovaných technikách, a tedy uživateli pro řešení problému nabízí individuální řešení.

Některé programové balíky disponují i firewallem, který však můžeme získat i jako samostatný program. Firewall kontroluje síťovou komunikaci a zabraňuje přímému napadení počítače přes síť (Kuchař, 2005).

Také je velmi populární antispywarové zabezpečení, první programy tohoto druhu se specializovaly pouze na hledání a odstranění spywaru, ale v současnosti je k dispozici celá řada kombinací, takže např. programový balík s antispywarem a antivirem a nebo antispyware společně i s programy pro čištění digitálních zařízení.

Tvůrci malwaru jsou vždy o krok napřed před tvůrci programů pro ochranu, takže je důležité vědět, jak postupovat v případě, kdy je zařízení napadeno tak, že ani tato softwarová ochrana není účinná. Velkou váhu má zálohování dat, což znamená vytvoření jejich kopií a uložení na bezpečné místo, v případě že pak malware jakkoliv poškodí, či úplně smaže tato data, můžeme je po odstranění malwaru obnovit z této zálohy.

Pokud vlivem malwaru dojde k znepřístupnění operačního systému u počítačů, je výhodné použít záchranná média. Pokud i přes to nedojde uživatel k pozitivnímu výsledku, může pomoci naformátování disku a reinstalace systému (Geier et. Bednařík, 2011).

3 Praktická část – realizace výzkumu

3.1 Cíl výzkumu

V této praktické části se budeme snažit zjistit, jestli vysokoškolští studenti správně chápou pojem malware vzhledem k textu v teoretické části a zda se s tímto pojmem vůbec setkali. Dále jestli znají jeho druhy a jestli o nich také něco vědí. Budeme také zjišťovat, zda chápání pojmů závisí na pohlaví studentů. Dále chceme zjistit, jaký pohled mají VŠ studenti na vzdělání v oblasti zabezpečení, a co by se v ní dalo zlepšit, aby vzdělání dosáhlo vyšší úrovně. Na základě toho se pak pokusíme doporučit řešení, které by mohlo být prospěšné ke zvýšení povědomí studentů o problematice malwaru. Budeme se snažit zjistit, zda pro vzdělávání v oblasti malwaru studenti využívají Internet a zda jejich odpovědi závisí na tom, za jaký typ člověka se oni sami považují.

V neposlední řadě se budeme snažit vypozorovat i zajímavé závislosti mezi některými výsledky.

3.2 Výzkumné problémy

Budeme zjišťovat, zda studenti budou mít problémy s chápáním pojmu malware, vzhledem k tomu, že v médiích se často mluví o virech jako o souhrnném názvu pro všechny hrozby, čímž může být ovlivněno i chápání studentů, jako příklad můžeme uvést nedávno vydaný článek s názvem *„Nový podvodný e-mail obsahuje nebezpečný vir. Přílohu nespouštějte“* (Všetečka, 2014), který pochází z webových stránek, které se prezentují jako názory odborníků v oblasti technologií a očekávali bychom v tomto směru použití správných termínů. Dále se setkáme s problémy i v literatuře, konkrétně v učebnicích *„S počítačem na základní škole“* (Navrátil, 2010) a *„S počítačem nejen k maturitě“* (Navrátil, 2006), které se používají pro výuku informatiky a informačních a komunikačních technologií na některých základních a středních školách. Zde jsou virům připisovány takové projevy, kterými se viry nevyznačují, ale pokud se s takovouto literaturou na školách pracuje, může to vyvolat u mladších žáků zmatek, který si s sebou nesou i do budoucna.

Dále budeme zjišťovat, zda se vůbec studenti setkali i s dalšími druhy malwaru a jestli se v těchto pojmech orientují, což by mohlo být úzce spjato s výše uvedenými poznatky.

V bakalářské práci byly formulovány následující čtyři základní okruhy problémů.

P_1: Mají studenti problémy s chápáním pojmu malware?

P_2: Orientují se studenti v dalších pojmech týkajících se malwaru?

P_3: Souvisí chápání pojmů spojených s malwarem s pohlavím studentů?

P_4: Zálohují data častěji studenti, kteří se již stali obětí malwaru?

3.3 Formulace hypotéz a výzkumných předpokladů

Na základě studia literatury (Navrátil, 2006; Jalůvka, 2000) ale i vlastních zkušeností jsme se rozhodli pro stanovení následujících hypotéz (H) a výzkumných předpokladů (VP).

H_1: Ženy se stávají obětmi malwaru častěji než muži.

H_2: Muži dokáží častěji správně definovat pojem malware než ženy.

H_3: Studenti, kteří měli své zařízení napadené malwarem, zálohují svá data častěji než ti studenti, kteří neměli své zařízení napadené malwarem.

H_4: Studenti, kteří se považují za technický typ člověka, vyhledávají informace z oblasti zabezpečení častěji na Internetu než studenti, kteří se pokládají za netechnický typ.

VP_1: Více než 50 % studentů alespoň 8 z 15 pojmů týkajících se malwaru slyšelo.

VP_2: Více než 50 % studentů, kteří minimálně 8 z 15 pojmů slyšelo, neumí správně definovat 8 a více pojmů.

VP_3: Více než 50 % studentů si myslí, že současná společnost není dobře vzdělaná v oblasti malwaru.

3.4 Použitá výzkumná metoda

Pro předvýzkum a samotný výzkum jsme zvolili jako výzkumnou metodu dotazník (Chráska, 2006). Dotazník pro předvýzkum se skládal celkem z 27 otázek. Z nich bylo 21 otevřených, 3 uzavřené, 2 polouzavřené a 1 výčtová otázka nabízející

i možnost vlastní odpovědi. Poslední otázkou v předvýzkumu jsme žádali respondenty o zpětnou vazbu k dotazníku.

Samotný dotazník pro hlavní výzkumné šetření obsahoval otázky téměř totožné s předvýzkumem, rozdílem bylo, že jsme využili odpovědí respondentů z předvýzkumu, abychom vyplňování dotazníku zjednodušili a tím se otevřené otázky změnily na polouzavřené, případně výčtové. Respondentům byl ponechán prostor pro připsání vlastní odpovědi, pokud by se nespokojili se stávajícími. Přibyly také otázky, kterými jsme se respondentů ptali, zda vůbec daný pojem slyšeli a pokud odpověděli záporně, systém elektronického dotazníku přeskočil otázku, na kterou by respondenti nedokázali odpovědět.

Konkrétně u 2. otázky, pomocí které jsme se snažili zjistit účel využívání digitálních zařízení, byly vytvořeny kategorie *Sociální sítě a komunikace*, *Internetové bankovnictví, Hry a multimédia (např. poslech hudby, sledování filmů, ...), Studium, Práce, Vyhledávání informací a aktuálního zpravodajství, Online nakupování, Stahování dat* a *Správa webových stránek/blogu*, ze kterých si respondenti mohli vybrat několik možností, případně napsat svou vlastní odpověď.

Třetí otázka byla zjednodušena podobným způsobem, a byla tedy vytvořena kategorie *Ztráta dat smazáním nebo zašifrováním, Únik citlivých údajů (např. osobní údaje, údaje k bankovnímu účtu, hesla, ...), Ovládnutí zařízení jinou osobou (hackerem), Ztráta finančního obnosu, Znemožnění přístupu do svého zařízení* a *Nemám obavy.*

Další otázka zůstala v původní podobě, ale studenti, kteří uvedli, že se stali obětí škodlivého softwaru, dostali ještě jednu další otázku, kde měli na výběr z výčtu škodlivých činností, které malware stihl napáchat a to *Ztráta dat smazáním nebo zašifrováním, Ovládnutí zařízení hackerem* a *Znemožnění přístupu do svého zařízení*, případně vlastní odpověď.

Otázka 6. se týkala zálohování, zde byla ještě doplněná odpověď *Nevím, co je to zálohování souborů*.

Následovaly otázky ověřující chápání jednotlivých pojmů, jak již bylo zmíněno, přidali jsme před každý pojem otázku, zda vůbec o pojmu respondenti slyšeli a na základě jejich odpovědi jim byla předložena (či vynechána) otázka, která se týkala jejich představy o konkrétním pojmu. Museli jsme zvolit takový jazyk odpovědí na otázky, aby respondenti nebyli ovlivňováni přesnými definicemi z teoretické části. Při každé otázce týkajících se pojmů mohli studenti zvolit odpověď *Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit*, případně dopsat svou vlastní odpověď.

Při otázce týkající se představy o pojmu malware měli studenti na výběr z možností *Škodlivý kód, který se dokáže kopírovat*, tuto odpověď jsme vybrali záměrně, protože by se zde respondenti dopustili záměny s virem, případně červem. Možnost *Souhrnný název pro všechny druhy škodlivého softwaru*, což by odpovídalo správnému chápání pojmu malware a *Nemoc počítačů, při které dochází k totální destrukci systému,* tato odpověď byla zvolená pro zajímavost a jde již o příliš přehnané chápání tohoto pojmu, je tedy potřeba brát jej s rezervou, hlavně z toho důvodu, že počítač zde vystupuje jako živá bytost, která může onemocnět.

U pojmu počítačový virus si mohli studenti vybírat z odpovědí *Souhrnný název pro všechny druhy škodlivého softwaru*, volbou této odpovědi by se studenti dopustili záměny s pojmem malware, dále *Škodlivý kód, který se dokáže kopírovat*, což je sice velmi stručné, ale správné chápání a *Nemoc počítačů, při které dochází k totálnímu zničení systému*, která byla zařazena ze stejného důvodu jako u předchozí otázky.

Další otázky se týkaly pojmu trojský kůň, i zde měli studenti možnost vybírat si mimo stálé odpovědi i další. *Škodlivý software, který se rozesílá jako skrytá příloha e-mailu, po jehož otevření dojde k úplnému zničení systému* byla opět jedna z odpovědí, která byla velmi nadsazená, odpověď *Software, který vypadá užitečně, ale po vniknutí do systému je škodlivý* měla značit správné chápání tohoto pojmu a dále *Druh počítačového viru, který se dokáže ukrýt v zařízení tak dobře, že ho neodhalí ani zabezpečovací prvky systému*, což opět není zcela správně, jelikož toto pojetí nelze aplikovat na všechny typy trojských koní.

Pojem zadní vrátka přinesl opět rozmanité odpovědi, a tedy do dotazníku byly použity následující možnosti *Jakýkoliv způsob, kterým se obejde zabezpečení systému a tím dává prostor hackerovi ovládnout cílové digitální zařízení*, což by označovalo nejlepší pochopení tohoto pojmu, *Způsob, kterým se maskuje aktivita škodlivého kódu na digitálním zařízení* by spíše náležela pojmu rootkit a *Obnovení systému ze zálohy po napadení digitálního zařízení škodlivým softwarem* značí úplně špatné pojetí.

Dalším pojmem byl následně červ, kde jsme studentům nabídli odpovědi *Škodlivý software šířící se pomocí sítě*, což považujeme za správné chápání, dále *Druh škodlivého softwaru, který se vyznačuje tím, že maže pouze části souborů a tím se zvětšuje on sám*, což by neznačilo správné pojetí a odpověď *Škodlivý software, který se dokáže šířit pouze pomocí USB flash disků* není taktéž vzhledem k teoretickým poznatkům zcela správně.

U pojmu spyware to pak byl výběr odpovědí *Škodlivý software, který shromažďuje informace z infikovaného digitálního zařízení a odesílá je jiné osobě*, což značí správné

pojetí a dále *Software, který má za úkol sledovat, jestli se v systému nenachází škodlivý software nebo jiná hrozba* společně s odpovědí *Škodlivý software, který je jedním z druhů počítačových virů*, které představovaly odpovědi s nesprávným pochopením tohoto pojmu.

Pro pojem adware byli vybrány následující odpovědi, a to *Škodlivý software, který způsobuje zobrazování vyskakovacích reklam*, což by bylo správné pojetí a ostatní dvě by byly ne zcela, nebo vůbec správné, tedy *Škodlivý software, který se dostane do digitálního zařízení kliknutím na reklamu na nedůvěryhodných stránkách* a *Software, ve kterém lze jednoduše vytvořit reklamu, a tu pak můžeme umístit na Internet.*

Další dvojice otázek, se zabývala pojmem dialer, zde respondenti vybírali z jedné správné definice *Škodlivý software, který v případě počítačů mění způsob vytáčení čísla pro internetové připojení a v případě mobilních telefonů posílá prémiové SMS zprávy* a dalších dvou méně vydařených odpovědí, které se v předvýzkumu taktéž vyskytly *Člověk, který napomáhá k šíření škodlivého softwaru* a *Vir na mobilní telefony a tablety*.

U pojmu rootkit to byly tyto odpovědi *Škodlivý software, který maskuje činnost dalších druhů škodlivého softwaru*, *Člověk, který napomáhá k šíření škodlivého softwaru* a *Nástroje sloužící pro opravu digitálního zařízení, které napadl škodlivý software*, samozřejmě poslední dvě odpovědi neznačí správné pochopení pojmu, neboť se bavíme o škodlivém softwaru, nikoliv o člověku nebo nástroji pro ochranu zařízení.

Dále nás zajímal pohled respondentů na pojem logická bomba, přičemž vybírali z odpovědí *Škodlivý software, který má za úkol spustit svou škodlivou činnost za předem určených podmínek, které stanovil autor tohoto škodlivého softwaru*, tato odpověď měla označovat správné pojetí, kdežto další dvě odpovědi *Programátorská chyba v programu, která dokáže být bránou pro škodlivý software*, nebo *Nástroj k odstranění jednodušších forem škodlivého softwaru* značí špatné pochopení.

Scareware jsme v naší práci definovali jako *Škodlivý software, který vypadá jako např. antivir, ten pak najde na zařízení spoustu falešných problémů pro jejichž odstranění je nutné si připlatit,* což byla jedna z odpovědí a dále se jednalo o odpovědi *Poplašná zpráva, která se snaží vystrašit uživatele, kteří si ji přečtou* a *Falešná webová stránka, která se vydává např. za stránky banky a tím vyláká od uživatele údaje k internetovému bankovnictví,* v prvním případě by se jednalo o chápání hoaxu a ve druhém o chápání phishingu.

Chápání pojmu zombie mohli respondenti formulovat pomocí odpovědí *Napadené zařízení, které hacker využívá k napadení ostatních zařízení v síti*, což bylo

správné pojetí a další dvě již zde byly zejména kvůli velmi zajímavému pochopení tohoto pojmu a to *Škodlivý software, který již byl v minulosti ze zařízení odstraněn, ale vyskytl se znovu* a *Zastaralá technologie, která je opět uvedena do provozu*.

Jako ransomware mohli studenti označit *Nástroj k odstranění jednodušších forem škodlivého softwaru* a *Škodlivý software, který má pouze za úkol zpomalení systému* nebo ze správné odpovědi *Škodlivý software, který zašifruje soubory, případně celý operační systém a žádá výkupné.*

U další dvojice otázek, které se zabývaly pojmem hoax mohli respondenti vybírat z jedné odpovědi, která vyznačovala správné chápání tohoto pojmu a to *Poplašná zpráva, která se snaží vystrašit uživatele, kteří si pak na základě tohoto výmyslu mohou např. smazat některá důležitá data* a z dalších dvou špatných *E-mailová zpráva, která vypadá jako např. z banky a snaží se od uživatele získat citlivé informace* a *Škodlivý software, který má za úkol najít a poslat třetí osobě hesla, která najde na napadeném zařízení.*

Poslední pojem byl phishing, zde byla opět jedna odpověď správná a to *Většinou e-mail, případně falešná stránka, která vypadá jako např. z banky a snaží se získat citlivé údaje od uživatele* a následně další dvě špatné *Nevyžádaná reklama* a *Poplašná zpráva, která se snaží vystrašit uživatele, kteří si pak na základě tohoto výmyslu mohou např. smazat některá důležitá data.*

U otázky 38. jsme opět uspořádali odpovědi studentů z předvýzkumu do několika kategorií a to *Zkvalitnění výuky na školách, Informační letáky a brožury, Reklamy v médiích, Televizní pořady věnující se této problematice, Kurzy, semináře a přednášky pro veřejnost, Literatura pro laiky, Výukové portály věnující se této problematice*, případně mohl dotazovaný využít možnost vlastní odpovědi.

U otázky č. 39 jsme udělali stejný postup, a tedy zvolili řazení do kategorií *od přátel/rodiny/partnera, na Internetu, u odborníků, v literatuře, z médií, ve škole, na pracovišti, nikde*, případně možnost vlastní odpovědi.

Na závěr přibyla ještě jedna další otázka, a to za jaký typ člověka se sami studenti považují, zda za technický či netechnický, nezávisle na oboru svého studia. Oproti dotazníku z předvýzkumu jsme vynechali požadavek o zpětnou vazbu k dotazníku.

Výzkumný dotazník tedy obsahoval celkem 43 otázek, z toho 16 otázek uzavřených, které se dále větvily podle odpovědi, 16 polouzavřených, 5 uzavřených, které se nevětvily, 5 výčtových s možností dopsání vlastního textu a pouze 1 otevřenou.

3.5 Popis výzkumného vzorku a průběhu výzkumu

3.5.1 Předvýzkum

Před výzkumem jsme uspořádali předvýzkum, který měl ověřit srozumitelnost dotazníku a poskytnout zajímavé odpovědi, které by mohly být využity pro sestavení dotazníku k hlavnímu výzkumu. Předvýzkum se realizoval na vzorku celkem 14 respondentů, z toho s jedním jsem dotazník vyplňovala v papírové podobě a na základě rozhovoru pro ověření srozumitelnosti jsem jej umístila na Internet, jeden z respondentů musel být vyřazen, jelikož nesplňoval podmínku studenta vysoké školy. Dotazníky byly vyplňovány na serveru Vyplňto.cz. Všechny dotazníky jsem posílala vybraným studentům, bohužel někteří studenti se nakonec předvýzkumného šetření nezúčastnili, ale poslali dotazník alespoň svým přátelům.

3.5.2 Hlavní výzkumné šetření

Samotný dotazník pro hlavní výzkumné šetření byl po vytvoření umístěn přímo na server Vyplňto.cz a je dostupný na webové adrese: https://www.vyplnto.cz/realizovane-pruzkumy/chapani-malware-vs-student/.

Výzkumný vzorek vysokoškolských studentů činil 96 respondentů. Bohužel muselo být dodatečně vyřazeno 5 respondentů, jelikož 4 nesplňovali podmínku vysokoškolského studenta a jeden byl vyřazen kvůli vulgarismům a tedy i nulovému přínosu pro celý výzkum. Konečný celkový počet respondentů použitý pro další zpracování výsledků výzkumu byl 91, což sice nenaplnilo naše očekávání, ale vzhledem k náročnosti dotazníku na přemýšlení se to dá pochopit. Oba použité dotazníky jsou součástí příloh této bakalářské práce.

3.6 Metody použité pro zpracování výsledků

V této bakalářské práci budeme používat pro ověření hypotéz test nezávislosti chí-kvadrát. Tohoto statistického testu využíváme v případech, kdy potřebujeme zjistit, zda je mezi dvěma jevy nějaká souvislost. Výsledky, které získáme dotazníkovým šetřením, je nutné zapsat do kontingenční tabulky. Dále je nutné formulovat nulovou

a alternativní hypotézu. Přičemž nulová hypotéza nepřipouští žádnou souvislost mezi zkoumanými jevy a alternativní hypotéza naopak předpokládá nějaký vztah mezi nimi. Společně s hypotézami si stanovíme i hladinu významnosti a to α=0,05 a spočítáme očekávané četnosti O, které odpovídají platnosti nulové hypotézy. Hodnoty očekávaných četností získáme tak, že násobíme odpovídající součty četností (součty řádků a sloupců) a tento součin následně vydělíme celkovou četností.

Následně pro každé pole kontingenční tabulky spočítáme hodnotu chí-kvadrát pomocí vztahu:

$$\chi^2 = \sum_{i=1}^{k} \frac{(\mathrm{P}_i - \mathrm{O}_i)^2}{\mathrm{O}_i},$$

kde k je počet polí kontingenční tabulky, P je námi naměřená hodnota a O je, jak jsme již zmínili, očekávaná hodnota.

Dále ještě zbývá určit stupeň volnosti ze vztahu:

$$f = (r-1).(s-1),$$

kde r je počet řádků a s počet sloupců dané kontingenční tabulky.

Ze statistických tabulek pak lze vyčíst pro daný stupeň volnosti a hladinu významnosti kritickou hodnotu. Tuto kritickou hodnotu pak musíme srovnat s hodnotou, kterou jsme získali výpočtem. Nulová hypotéza může být zamítnuta v případě, že by námi vypočítaná hodnota byla větší nebo rovna kritické hodnotě (Chráska, 2006).

Test chí-kvadrát jsme prakticky realizovali v programu STATISTICA 12.

3.7 Dokazování stanovených hypotéz

V této části se budeme snažit potvrdit platnost stanovených hypotéz.

3.7.1 Dokazování hypotézy H_1: Ženy se staly oběťm malwaru častěji než muži.

Při dokazování hypotézy si musíme určit nulovou hypotézu (v našem případě H_{01}) a alternativní hypotézu (H_{A1}). Dále určíme hladinu významnosti, tedy α=0,05.

H_{01}: Četnost napadení malwarem není závislá na pohlaví.

H_{A1}: Ženy se staly oběťmi malwaru častěji než muži.

Při dokazování této hypotézy jsme provedli rozdělení studentů do dvou skupin a to skupinu, kterým již malware napadl zařízení nezávisle na tom, zda stihl či nestihl

vykonat škodlivou činnost a druhá skupina zahrnovala ty studenty, kteří se nestali obětí malwaru. Studenty, kteří uvedli odpověď *Nevím*, jsme vynechali.

Tabulka č. 1: Kontingenční tabulka - Pozorované četnosti u rozdělení studentů do skupin podle napadení malwarem, dělení dle pohlaví

Kontingenční tabulka (Napadení malwarem) Četnost označených buněk > 10 (Marginální součty nejsou označeny)			
Pohlaví	**Ne**	**Ano**	Řádk. součty
Žena	25	29	54
Muž	12	19	31
Vš.skup.	37	48	85

Tabulka č. 2: Kontingenční tabulka - Očekávané četnosti u rozdělení studentů do skupin podle napadení malwarem, dělení dle pohlaví

Souhrnná tab.: Očekávané četnosti (Napadení m Četnost označených buněk > 10 Pearsonův chí-kv. : ,461135, sv=1, p=,497094			
Pohlaví	Ne	Ano	Řádk. součty
Žena	23,50588	30,49412	54,00000
Muž	13,49412	17,50588	31,00000
Vš.skup.	37,00000	48,00000	85,00000

Program STATISTICA 12 nám vypočítal pravděpodobnost chyby p=0,497094, vzhledem k tomu, že tato hodnota přesahuje námi zvolenou hladinu významnosti α=0,05, nelze odmítnout nulovou hypotézu. **Hypotéza H_1 nebyla dokázána.**

3.7.2 Dokazování hypotézy H_2: Muži dokáží častěji správně definovat pojem malware než ženy.

Při dokazování hypotézy si musíme určit nulovou hypotézu (v našem případě H_{02}) a alternativní hypotézu (H_{A2}). Dále určíme hladinu významnosti, tedy α=0,05. V tomto případě bylo nutné zařadit respondenty do dvou kategorií na ty, co svou odpovědí prokázali znalost tohoto pojmu a na ty, co tento pojem nechápou správně, případně ho vůbec neslyšeli.

H_{02}: Chápání pojmu malware nezávisí na pohlaví.

H_{A2}: Muži dokáží častěji správně definovat pojem malware než ženy.

Tabulka č. 3: Kontingenční tabulka - Pozorované četnosti u rozdělení studentů do skupin podle chápání pojmu malware, dělení dle pohlaví

Kontingenční tabulka (Znalost pojmu malware) Četnost označených buněk > 10 (Marginální součty nejsou označeny)			
Pohlaví	Správné chápání	Špatné chápání	Řádk. součty
Žena	20	38	58
Muž	19	14	33
Vš.skup.	39	52	91

Tabulka č. 4: Kontingenční tabulka - Očekávané četnosti u rozdělení studentů do skupin podle chápání pojmu malware, dělení dle pohlaví

Souhrnná tab.: Očekávané četnosti (Znalost pojr Četnost označených buněk > 10 Pearsonův chí-kv. : 4,58011, sv=1, p=,032345			
Pohlaví	Správné chápání	Špatné chápání	Řádk. součty
Žena	24,85714	33,14286	58,00000
Muž	14,14286	18,85714	33,00000
Vš.skup.	39,00000	52,00000	91,00000

Program STATISTICA 12 nám vypočítal pravděpodobnost chyby p=0,032345, vzhledem k tomu, že tato hodnota nepřesahuje námi zvolenou hladinu významnosti α=0,05, můžeme odmítnout nulovou hypotézu a přijmout alternativní. **Hypotéza H_2 byla dokázána.**

3.7.3 Dokazování hypotézy H_3: Studenti, kteří měli své zařízení napadené malwarem zálohují svá data častěji než ti studenti, kteří neměli své zařízení napadené malwarem.

Při dokazování hypotézy si musíme určit nulovou hypotézu (v našem případě H_{03}) a alternativní hypotézu (H_{A3}). Dále určíme hladinu významnosti, tedy α=0,05.

H_{03}: Studenti zálohují stejně, nezávisle na předchozí zkušenosti s malwarem.

H_{A3}: Studenti, kteří měli své zařízení napadené malwarem zálohují svá data častěji než ti studenti, kteří neměli své zařízení napadené malwarem.

Zde jsme opět respondenty rozdělili do dvou kategorií, na ty, co se již s malwarem na svém zařízení setkali a na ty, co ne. Dále na ty, co zálohují a pak na ty co nezálohují. Přitom jsem vyloučila ty studenty, kteří nevěděli, zda jejich zařízení již bylo napadeno a dále ty, kteří nevěděli, co to zálohování znamená.

Tabulka č. 5: Kontingenční tabulka - Pozorované četnosti u rozdělení studentů do skupin podle předchozí zkušenosti s malwarem, dělení dle zálohování

Kontingenční tabulka (Předchozí zkušenost a zá Četnost označených buněk > 10 (Marginální součty nejsou označeny)			
Zálohová ní	Předchozí zkušenost Ne.	Předchozí zkušenost Ano.	Řádk. součty
Ne.	11	10	21
Ano.	26	38	64
Vš.skup.	37	48	85

Tabulka č. 6: Kontingenční tabulka - Očekávané četnosti u rozdělení studentů do skupin podle předchozí zkušenosti s malwarem, dělení dle zálohování

Souhrnná tab.: Očekávané četnosti (Předchozí z Četnost označených buněk > 10 Pearsonův chí-kv. : ,888978, sv=1, p=,345755			
Zálohová ní	Předchozí zkušenost Ne.	Předchozí zkušenost Ano.	Řádk. součty
Ne.	9,14118	11,85882	21,00000
Ano.	27,85882	36,14118	64,00000
Vš.skup.	37,00000	48,00000	85,00000

Program STATISTICA 12 nám vypočítal pravděpodobnost chyby p=0,345755, vzhledem k tomu, že tato hodnota přesahuje námi zvolenou hladinu významnosti α=0,05, nelze odmítnout nulovou hypotézu. **Hypotéza H_3 nebyla dokázána.**

3.7.4 Dokazování hypotézy H_4: Studenti, kteří se považují za technický typ člověka, vyhledávají informace z oblasti zabezpečení častěji na Internetu než studenti, kteří se pokládají za netechnický typ.

Při dokazování hypotézy si musíme určit nulovou hypotézu (v našem případě H_{04}) a alternativní hypotézu (H_{A4}). Dále určíme hladinu významnosti, tedy α=0,05.

H_{04}: Studenti, kteří se považují za technický typ člověka, vyhledávají informace z oblasti zabezpečení na Internetu stejně často jako studenti, kteří se pokládají za netechnický typ.

H_{A4}: Studenti, kteří se považují za technický typ člověka, vyhledávají informace z oblasti zabezpečení častěji na Internetu než studenti, kteří se pokládají za netechnický typ.

V tomto případě bylo nutné zařadit respondenty do dvou kategorií, v jedné byli studenti, kteří uvedli, že se vzdělávají na Internetu a ve druhé byli ti, co se na Internetu nevzdělávají.

Tabulka č. 7: Kontingenční tabulka 7 - Pozorované četnosti u rozdělení studentů do skupin podle vyhledávání informací z oblasti zabezpečení na Internetu oproti pohledu studentů na svou vlastní osobnost

Kontingenční tabulka (Typ člověka a vyhledávání Četnost označených buněk > 10 (Marginální součty nejsou označeny)			
Jak se student vidí.	Nevyhledává	Vyhledává	Řádk. součty
Technický typ	24	30	54
Netechnický typ	28	9	37
Vš.skup.	52	39	91

Tabulka č. 8: Kontingenční tabulka - Očekávané četnosti u rozdělení studentů do skupin podle vyhledávání informací z oblasti zabezpečení na Internetu, dělení dle pohledu studentů na svou vlastní osobnost

Souhrnná tab.: Očekávané četnosti (Typ člověka Četnost označených buněk > 10 Pearsonův chí-kv. : 8,74474, sv=1, p=,003105			
Jak se student vidí.	Nevyhledává	Vyhledává informace	Řádk. součty
Technický typ	30,85714	23,14286	54,00000
Netechnický ty	21,14286	15,85714	37,00000
Vš.skup.	52,00000	39,00000	91,00000

Program STATISTICA 12 nám vypočítal pravděpodobnost chyby p=0,03105, vzhledem k tomu, že tato hodnota nepřesahuje námi zvolenou hladinu významnosti α=0,05, můžeme odmítnout nulovou hypotézu a přijmout alternativní. **Hypotéza H_4 byla dokázána.**

3.8 Ověřování stanovených výzkumných předpokladů

V této části budeme ověřovat výzkumné předpoklady, které jsme si vymezili.

3.8.1 Ověřování výzkumného předpokladu VP_1: Více než 50 % studentů alespoň 8 z 15 pojmů týkajících se malwaru slyšelo.

Studentů jsme se v dotazníkovém šetření ptali na 15 pojmů a zejména na to, jestli o těchto pojmech slyšeli. Bylo nutné analyzovat otázky, ve kterých jsme se respondentů

dotazovali, zda znají jednotlivé pojmy a z toho jsme následně vytvořili 2 kategorie studentů, do první patřili studenti, kteří slyšeli 8 a více pojmů a v druhé kategorii byli studenti, kteří uvedli, že slyšeli 7 a méně pojmů.

Tabulka č. 9: Počet respondentů, kteří slyšeli alespoň o 8 pojmech týkajících se malwaru a počet respondentů, kteří neslyšeli alespoň o 8 o pojmech týkajících se malwaru.

Celkem respondentů	Slyšelo > 7 pojmů	Slyšelo < 8 pojmů
91	51	40
100%	56%	44%

Z výše uvedené tabulky vyplývá, že 51 respondentů (56 %) odpovědělo, že slyšeli nejméně 8 z 15 pojmů týkajících se malwaru, ostatních 40 respondentů (44 %) uvedlo, že slyšeli méně než 8 pojmů.

Dále jsme zjistili, že nebyl nikdo, kdo by neslyšel ani jeden pojem, nejméně pojmů, kteří studenti slyšeli, byly 2 a tuto skutečnost jsme zaznamenali konkrétně u 5 studentů, oproti tomu 9 studentů uvedlo, že slyšeli všech 15 pojmů. **Tímto se nám podařilo potvrdit náš výzkumný předpoklad VP_1.**

3.8.2 Ověřování výzkumného předpokladu VP_2: Více než 50 % studentů, kteří minimálně 8 z 15 pojmů slyšeli, neumí správně definovat 8 a více pojmů.

U tohoto výzkumného předpokladu, jsme vycházeli z hodnot, které jsme použili už při předchozím ověřování výzkumného předpokladu. Zde jsme zjistili, že 51 respondentů uvedlo, že již slyšeli 8 a více pojmů. Z toho nás zajímalo, kolik studentů dokázalo pojmy správně definovat.

Tabulka č. 10: Počet respondentů, kteří slyšeli alespoň o 8 pojmech a dokázali správně definovat alespoň 8 pojmů a počet respondentů, kteří nedokázali definovat alespoň 8 pojmů.

Celkem respondentů	Správně > 7 pojmů	Špatně < 8 pojmů
51	28	23
100%	55%	45%

Z tabulky můžeme vyčíst, že náš předpoklad byl špatný, neboť 28 respondentů (55 %) dokázalo definovat alespoň 8 pojmů správně a oproti tomu 23 respondentů (45 %) definovalo správně méně než 8 pojmů. Ze všech 51 pozorovaných respondentů (100 %) dokázali 3 správně definovat pouze 2 pojmy, což bylo nejméně a další 3 dokázali

definovat správně 14 pojmů, což bylo nejvíce správně definovaných pojmů. **Kvůli této skutečnosti se nám náš výzkumný předpoklad VP_2 nepodařilo potvrdit.**

3.8.3 Ověřování výzkumného předpokladu VP_3: Více než 50 % studentů si myslí, že současná společnost není dobře vzdělaná v oblasti malwaru.

Tento výzkumný předpoklad jsme ověřovali na základě odpovědí na otázku, která se objevila v hlavním výzkumném šetření, kde nás zajímalo, zda si respondenti myslí, že je naše společnost dobře vzdělaná v oblasti malwaru.

Tabulka č. 11: Spokojenost respondentů se vzděláním společnosti v oblasti malwaru.

Celkem respondentů	Spokojeno	Nespokojeno	Nedokázali posoudit
91	6	69	16
100%	7%	75,5%	17,5%

Tato tabulka ukazuje, že z celkového počtu 91 studentů (100 %) je nespokojeno 69 studentů (75,5 %), což je více jak 50 %. **Tímto se nám podařilo potvrdit náš výzkumný předpoklad VP_3.**

3.9 Analýza vybraných odpovědí

Kvůli velkému rozsahu dotazníkového šetření jsme se podrobně věnovali pouze těm otázkám, které byly spojeny s dokazováním hypotéz a výzkumných předpokladů a dále uvedeme i ty, které byly nějakým způsobem zajímavé nebo překvapivé.

3.9.1 Analýza otázky č. 4: Stal/a jste se někdy obětí škodlivého softwaru (např. vir, trojský kůň, …)?

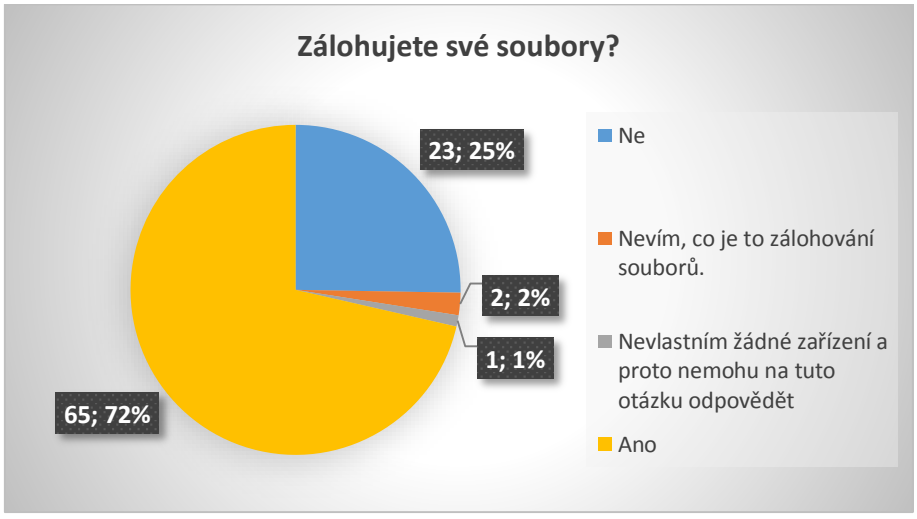
Otázka, na které byly založeny hned dvě hypotézy a to H_1 a H_3, zněla: *Stal/a jste se někdy obětí škodlivého softwaru (např. vir, trojský kůň, ...)?*

Graf č. 1: Otázka č. 4 - Stal/a jste se někdy obětí škodlivého softwaru (např. vir, trojský kůň, ...)?

Nejvíce studentů tedy 40 (44 %), se již s malwarem setkalo, ale buď nestihl vykonat žádnou škodlivou činnost, nebo o tom neví. Dále 37 studentů (41 %) nemá s malwarem žádnou zkušenost, 6 (6 %) si není jistých. Pak zbylých 8 studentů (9 %) zodpovědělo, že malware stihl vykonat na jejich zařízení škodlivou činnost.

3.9.2 Analýza otázky č. 6: Zálohujete své soubory?

Třetí hypotéza (H_3) se zakládala kromě otázky na pohlaví respondentů i na tom, jestli studenti zálohují.



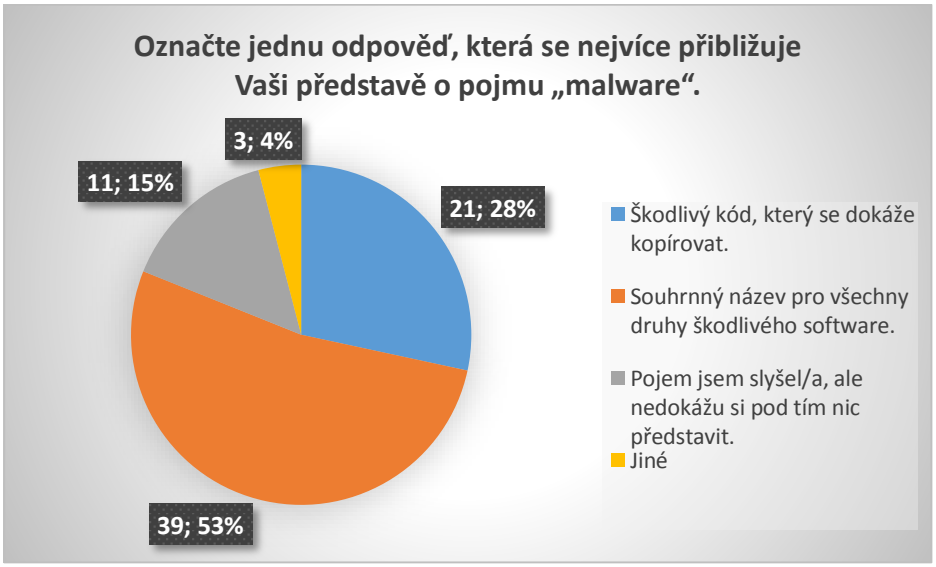
Graf č. 2: Otázka č. 6 - Zálohujete své soubory?

Nejvíce respondentů označilo, že soubory zálohují, a to celkem 65 (72 %) z 91 (100 %). Dále 23 studentů (25 %) uvedlo, že nezálohují, 2 respondenti (2 %)

nevěděli, co je to zálohování a překvapivě 1 respondent (1 %) uvedl, že nevlastní žádné zařízení a proto nemůže na otázku odpovědět, i když v úplně první otázce dotazníkového šetření uvedl, že využívá mobilní telefon s operačním systémem.

3.9.3 Analýza otázky č. 8: Označte jednu odpověď, která se nejvíce přibližuje Vaši představě o pojmu „malware".

V dotazníku dále dostali respondenti otázku, zda v minulosti slyšeli o pojmu malware. Respondenti, kterých bylo celkem 74 (81 %), uvedli, že tento pojem již slyšeli. Dále tedy dostali tito respondenti za úkol označit odpověď, která se nejvíce přibližovala jejich představě o pojmu malware.



Graf č. 3: Otázka č. 8 - Označte jednu odpověď, která se nejvíce přibližuje Vaši představě o pojmu „malware".

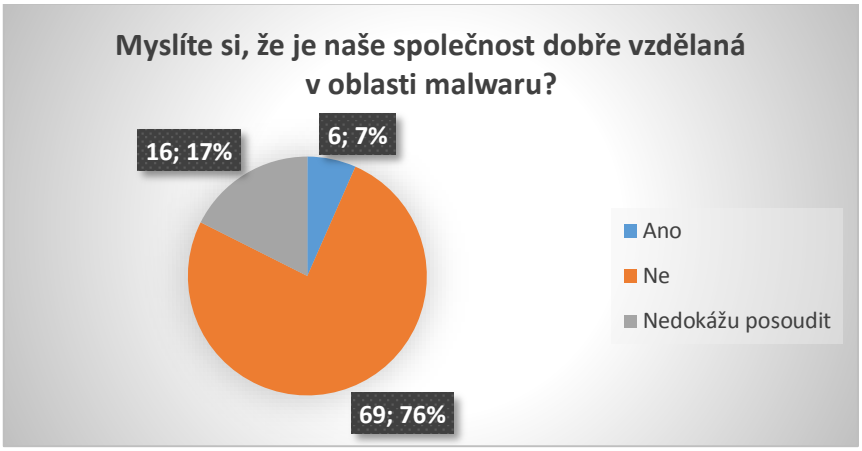
Z grafu vyplývá, že ze 74 studentů (100 %), kteří na tuto otázku odpovídali, se 39 studentů (53 %) shodlo na tom, že malware je *Souhrnný název pro všechny druhy škodlivého softwaru*, což se nejvíce přibližuje i teorii uvedené v této bakalářské práci. Dalších 21 studentů (28 %) odpovědělo, že se jedná o *Škodlivý kód, který se dokáže kopírovat*, což není zcela přesné vyjádření a spíš bychom si pod touto odpovědí měli představit viry, případně červa. Jedenáct respondentů (15 %) uvedlo, že sice pojem slyšeli, ale nedokáží si pod tím nic představit. Zbylí 3 respondenti (4 %) uvedli svou vlastní odpověď, i když by ve svém jádru byly všechny jejich odpovědi pravdivé, jejich pochopení pojmu malware je nepřesné a spíše si zaměňují pojem malware s jeho

konkrétními druhy. Nikdo z dotázaných se nenechal zmást a nezvolil možnost, že se jedná o *Nemoc počítačů, při které dochází k totální destrukci systému*.

Musíme tedy podotknout, že pouze 39 studentů (43 %) ze všech 91 dotázaných chápe pojem malware správně a zbylých 52 studentů (57 %) buď má nějakou představu, která není zcela přesná, nebo vůbec netuší, o co jde.

3.9.4 Analýza otázky č. 37: Myslíte si, že je naše společnost dobře vzdělaná v oblasti malwaru?

V této otázce měli studenti zhodnotit, jestli je naše společnost dobře vzdělaná v oblasti malwaru, my jsme na základě jejich responsí mohli ověřit třetí výzkumný předpoklad.

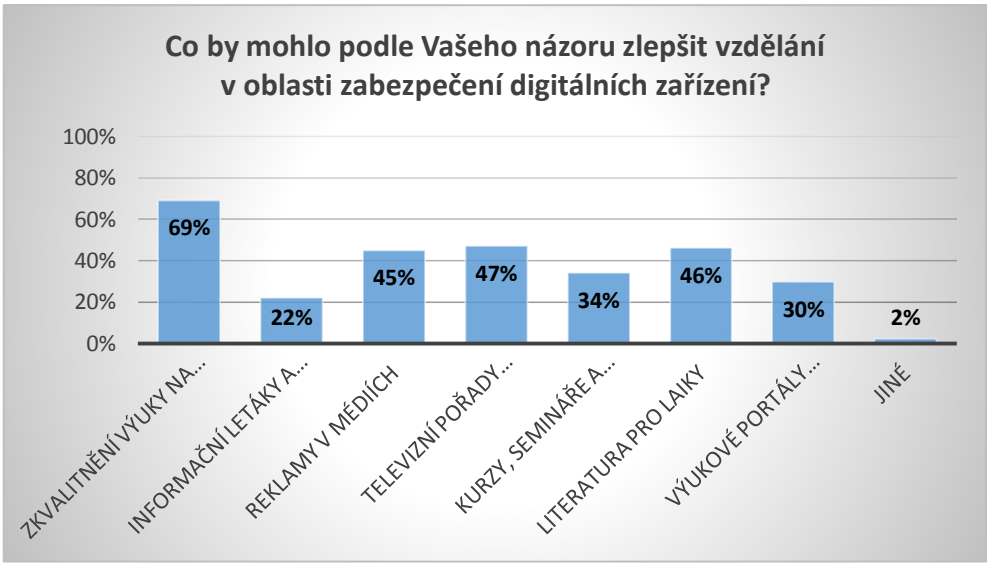


Graf č. 4: Otázka č. 37 – Myslíte si, že je naše společnost dobře vzdělaná v oblasti malwaru?

Nejvíce studentů se shodlo na tom, že naše společnost není dobře vzdělaná v oblasti malwaru a to celkem 69 studentů (75,5 %), 16 studentů (17,5 %) odpovědělo, že tuto situaci nedokážou posoudit a 6 studentů (7 %) si myslí, že je naše společnost dobře vzdělaná v této oblasti.

3.9.5 Analýza otázky č. 38: Co by mohlo podle Vašeho názoru zlepšit vzdělání v oblasti zabezpečení digitálních zařízení?

Zjišťovali jsme, co by podle dotazovaných studentů mohlo zlepšit kvalitu vzdělání v oblasti zabezpečení.

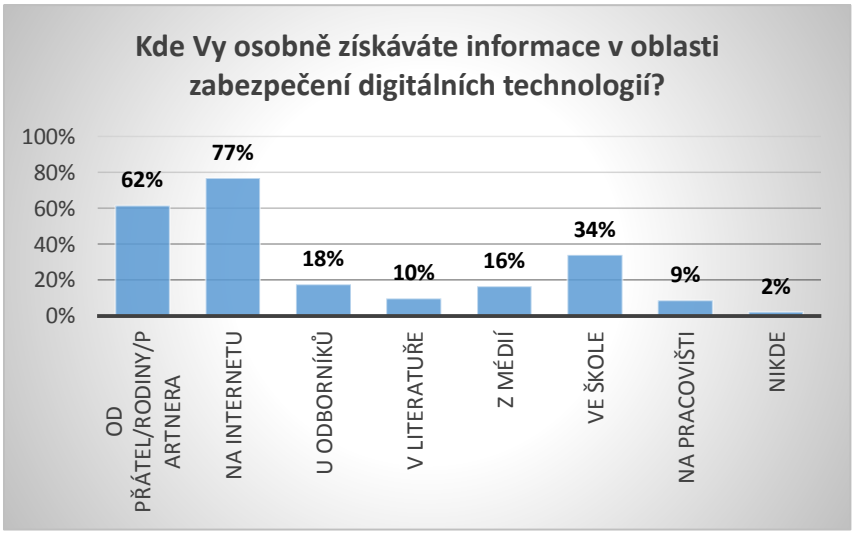


Graf č. 5: Otázka č. 38 - Co by mohlo podle Vašeho názoru zlepšit vzdělání v oblasti zabezpečení digitálních zařízení?

Studenti mohli zvolit více odpovědí, nejvíce respondentů, tedy 63 (69 %) označilo odpověď *Zkvalitnění výuky na školách*, 43 studentů (47 %) uvedlo, že by mohly být přínosné i *Televizní pořady věnující se této problematice*, dále pak 42 respondentů (46 %) označilo odpověď *Literatura pro laiky*. Dalších 41 studentů (45 %) by vidělo smysl v odpovědi *Reklamy v médiích*, 31 respondentů (34 %) by uvítalo *Kurzy, semináře a přednášky pro veřejnost*, *Výukové portály věnující se této problematice* by ocenilo 27 studentů (30 %). 20 studentů (22 %) zvolilo odpověď *Informační letáky a brožury*. Objevily se i 2 další odpovědi (2 %), které studenti sami vepsali, jednou z odpovědí bylo to, že by pomohl jen zázrak a další respondent by ocenil technickou podporu pro lidi, kterým malware napadl zařízení, což však neřeší otázku, jak zlepšit vzdělání.

3.9.6 Analýza otázky č. 39: Kde Vy osobně získáváte informace v oblasti zabezpečení digitálních technologií?

Při dokazování čtvrté hypotézy jsme dále využili poznatků, které jsme získali pomocí otázky: *Kde Vy osobně získáváte informace v oblasti zabezpečení digitálních technologií?*

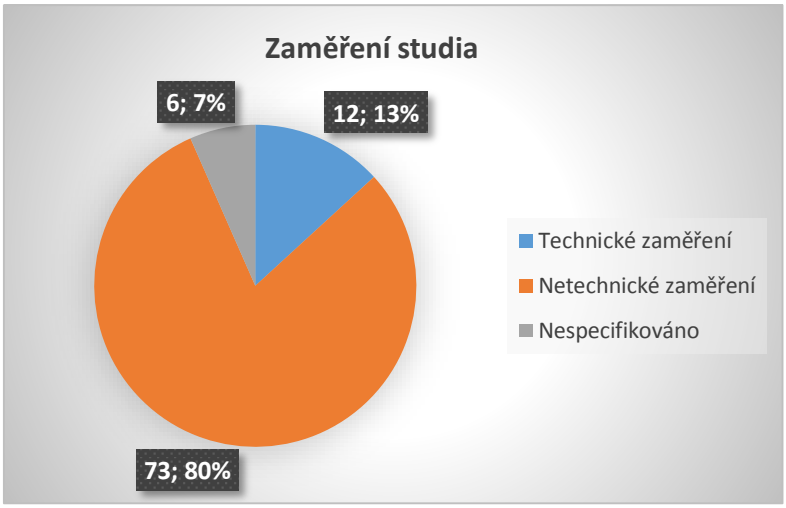


Graf č. 6: Otázka č. 39 - Kde Vy osobně získáváte informace v oblasti zabezpečení digitálních technologií

Dalo se předpokládat, že Internet bude nejvyhledávanějším zdrojem informací vzhledem k dnešnímu životnímu stylu vysokoškolských studentů, proto tuto odpověď označilo celkem 70 studentů (77 %). Vedle toho si mohli vybrat i z dalších odpovědí, tedy 56 studentů (62 %) uvedlo odpověď *Od přátel/rodiny/partnera* a 31 (34 %) uvedlo, že získávají informace *Ve škole*. 16 studentů (18 %) uvádí, že *U odborníků*, 15 responsí (16 %) získala odpověď *Z médií*. Celkem 9 dotázaných (10 %) získává informace pomocí literatury a 8 studentů (9 %) získává informace i *Na pracovišti*. Pouze 2 studenti (2 %) uvedli, že informace *Nikde* nezískávají.

3.9.7 Analýza otázky č. 41: Zaměření studia

Studenty jsme rozdělili do třech kategorií podle zaměření studia, a to technické zaměření, netechnické zaměření a nespecifikováno, pro studenty, kteří neuvedli přesně obor svého studia.

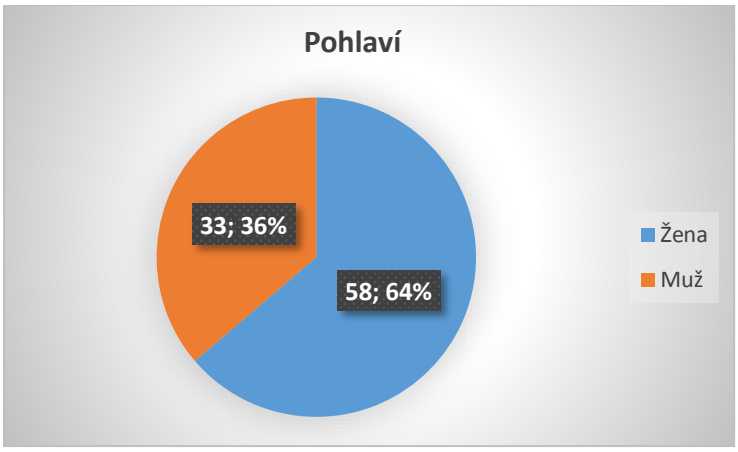


Graf č. 7: Otázka č. 41 - Zaměření studia

Z grafu vyplývá, že nejvíce studentů (73) studuje obor netechnického zaměření, ale když se podíváme na odpovědi z otázky č. 43, zde uvedlo 54 studentů, že se považují za technický typ člověka. Samozřejmě člověk, který studuje netechnický obor, se může vzdělávat v oblasti digitálních technologií ve volném čase nezávisle na oboru studia, proto jsme otázku č. 43 zařadili do výzkumu.

3.9.8 Analýza otázky č. 42: Pohlaví respondentů

Jedna z velmi důležitých otázek, na které byly založeny hned 2 hypotézy a to H_1 a H_2, týkala se pohlaví respondentů.

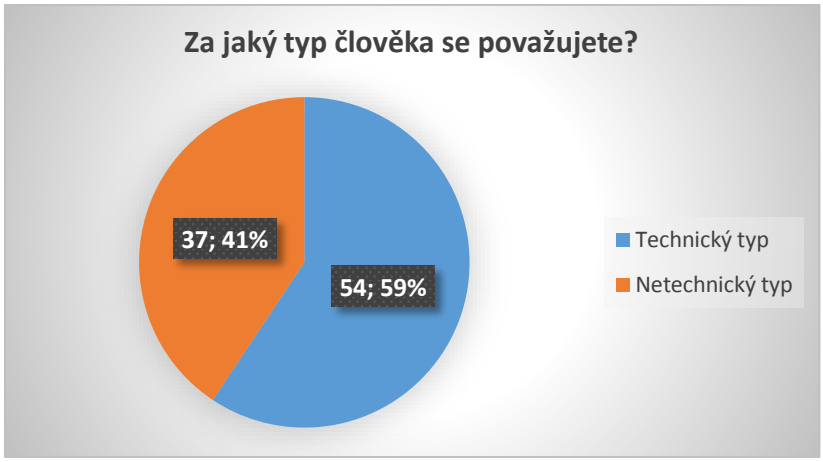


Graf č. 8: Pohlaví respondentů

Z grafu vyplývá, že dotazníkového šetření se z celkového počtu 91 studentů (100 %) zúčastnilo více žen, celkem 58 (64 %) a mužů bylo 33 (36 %).

3.9.9 Analýza otázky č. 43: Za jaký typ člověka se považujete?

Při dokazování hypotézy H_4 jsme museli využít poznatků z otázky, u které nám šlo zejména o to, jak se sami studenti vidí nezávisle na vzdělání, tedy jestli se cítí být technickým typem člověka, či netechnickým typem člověka.

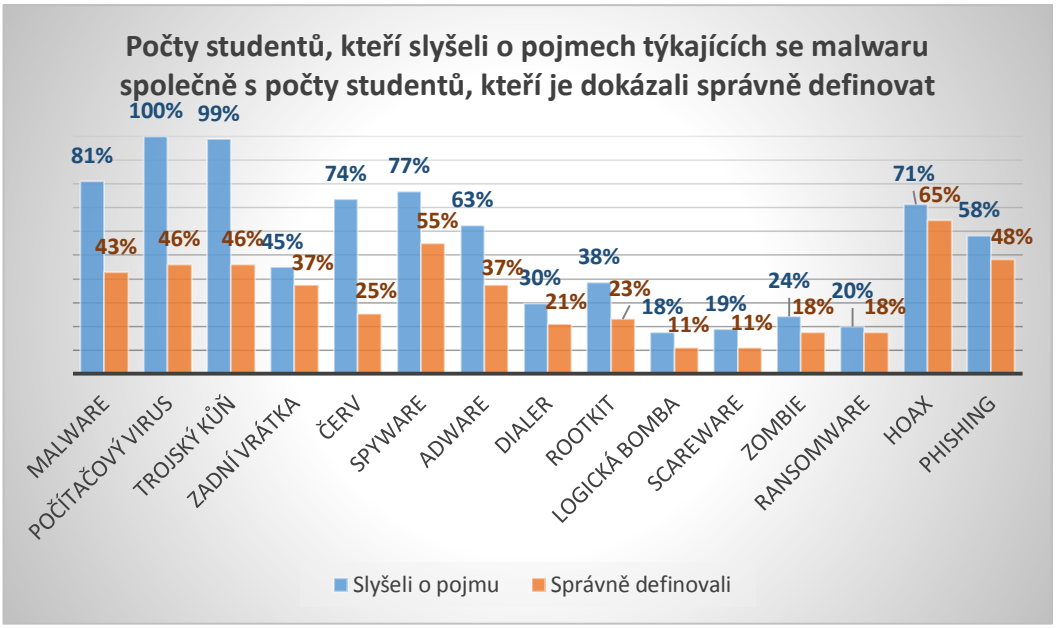


Graf č. 9: Otázka č. 43 - Za jaký typ člověka se považujete?

Z 91 studentů (100 %) se 54 respondentů (59 %) považovalo za technický typ a zbylých 37 studentů (41 %) se označilo za netechnický typ člověka.

3.9.10 Analýza pojmů týkajících se malwaru

U ověřování prvních dvou výzkumných předpokladů jsme vycházeli z poznatků, které jsme získali dotazníkovým šetřením, kde jsme se respondentů ptali na celkem 15 pojmů. Jeden z hlavních pojmů – malware je zde již podrobněji analyzován, nás ale zajímaly kromě tohoto pojmu i další s ním související a na základě odpovědí respondentů jsme vytvořili pro každý pojem dvě kategorie. První kategorie obsahuje studenty, kteří daný pojem slyšeli, a druhá kategorie obsahuje studenty, kteří dokázali správně tento pojem definovat. Vzhledem k velkému rozsahu je budeme analyzovat pouze stručně.



Graf č. 10: Počty studentů, kteří slyšeli o pojmech týkajících se malwaru z celkového počtu studentů společně s počty studentů, kteří je dokázali správně definovat z celkového počtu studentů

Překvapivě všech 91 respondentů (100 %) odpovědělo, že v minulosti již o pojmu počítačový vir slyšeli, ale správně definovat ho dokázalo jen 42 studentů (46 %). V celém výzkumném šetření to byl výsledek s nejvýraznějším skokem mezi respondenty, kteří o tomto pojmu slyšeli a mezi těmi, kteří jej dokázali správě definovat.

Pojem trojský kůň již slyšelo 90 respondentů (99 %) a z toho 42 dokázalo tento pojem správně definovat, což odpovídá 47 % z dotazovaných 90 respondentů.

Zadní vrátka byl pro většinu studentů nový pojem, protože pouze 41 studentů (45 %) označilo odpověď, že o tomto pojmu již slyšeli. Je však pozitivní, že z těchto 41 respondentů pouze 7 nedokázalo tento pojem správně definovat.

Dalším pojmem byl červ, celkem 67 respondentů (74 %) uvedlo, že o pojmu slyšeli. V případě definování pojmů byl počet studentů výrazně nižší a to konkrétně 23 respondentů, což odpovídalo 34 % z 67 dotazovaných.

Pojem spyware již slyšelo 70 respondentů (77 %) ze všech 91 dotazovaných. Z těchto 70 respondentů dokázalo tento pojem 50 definovat, což odpovídá 71 %, což je oproti předchozím čtyřem pojmům velmi dobrý výsledek i vzhledem k celkovému počtu studentů.

Dále nás zajímal v dotazníkovém šetření i pojem adware, o tomto pojmu slyšelo 57 respondentů (63 %) a více než polovina z nich, konkrétně 34 respondentů (60 %), dokázala tento pojem správně definovat.

Pojem dialer znalo z dřívějška pouze 27 studentů (30 %) a z toho 19 studentů pojem správně definovalo.

Rootkit byl dalším pojmem, který nás zajímal. U tohoto pojmu uvedlo 35 studentů (38 %), že ho již slyšeli a dále ještě méně respondentů označilo správnou definici, konkrétně 21 respondentů.

Dalším pojmem, na který jsme se dotazovali, byla logická bomba. U tohoto pojmu jsme zaznamenali nejhorší výsledky, neboť pouze 16 studentů (18 %) uvedlo, že již o pojmu slyšeli a z toho 10 jich dokázalo tento pojem správně definovat.

Pojem scareware měl také horší výsledky, 17 respondentů (19 %) uvedlo, že o pojmu již slyšeli a z toho stejně tak jako u pojmu logická bomba, pouze 10 z nich dokázalo tento pojem definovat.

Další pojem zombie taktéž nedopadl nejlépe, slyšelo o něm pouze 22 studentů (24 %) a z toho 16 zvolilo správnou definici tohoto pojmu.

Ransomware na tom překvapivě také nebyl moc dobře, slyšelo o něm pouze 18 studentů (20 %), ale 16 z nich dokázalo ransomware správně definovat.

Pojem hoax dopadl, co se týče znalosti respondentů, nejlépe. Sice 65 respondentů (71 %) uvedlo, že tento pojem zná z doslechu, ale také jsme vyhodnotili celkem 59 správných definic tohoto pojmu a toto číslo přesáhlo naše očekávání.

Posledním pojmem byl phishing, zde uvedlo 53 respondentů (58 %), že se s tímto pojmem již v minulosti setkali a z toho 44 studentů dokázalo tento pojem správně definovat. I když jsou výsledky o poznání lepší než u některých dalších pojmů, předpokládali jsme mnohem větší počet studentů, kteří o tomto pojmu slyšeli, neboť se o něm v poslední době hodně mluví v médiích.

3.10 Diskuze hlavních výsledků výzkumu

V našem výzkumu jsme se přesvědčili, že opravdu existuje problém v chápání pojmu malware, studenti si jej nejčastěji pletou s pojmem počítačový vir a vzhledem k tomu, že se nám podařilo dokázat druhou hypotézu, která se týkala závislosti pohlaví studentů na správném definování pojmu malware, je velmi pravděpodobné, že chápání tohoto pojmu souvisí i s pohlavím, neboť oblast digitálních technologií bývá bližší mužům, než ženám.

Dále jsme zjistili, že si studenti zaměňovali i pojmy, které ve všech případech označovaly škodlivý kód, za software, který by měl sloužit k prospěchu uživatelů (např.

antivir, firewall, …). Také jsme zjistili, že si studenti v několika případech zaměňovali pojem phishing za hoax, případně spyware za adware a naopak.

Nejvíce studentů umělo správně definovat pojem hoax, a to celkem 59. Nejméně známý pojem byla u respondentů logická bomba hned po ní scareware a ransomware. U ransomwaru jsme tuto skutečnost nepředpokládali, neboť v současnosti je velmi rozšířený.

Velmi překvapivé bylo, že všichni dotazovaní studenti se shodli na tom, že slyšeli pojem počítačový vir, 90 studentů uvedlo, že slyšeli pojem trojský kůň, i když ve většině případů oba tyto pojmy definovali nesprávně a překvapivě pojem malware v minulosti slyšelo jen 81 % studentů.

Skutečnost, že se nám nepodařilo dokázat první hypotézu, že ženy se staly obětmi malwaru častěji než muži, mohla být způsobena nejen malým počtem dotazovaných studentů, ale také by mohlo záviset na době, kterou ženy a muži tráví na svých digitálních zařízeních, což by mohlo být předmětem dalšího výzkumu.

U hypotézy třetí, kde jsme dokazovali, zda studenti, jejichž zařízení již bylo napadeno malwarem, zálohují častěji než ostatní, mohl hrát hlavní roli stejný faktor jako u dokazování první hypotézy a to malý počet respondentů. Dalším faktorem by mohlo být, že vysokoškolští studenti mají ve svých zařízeních důležité soubory potřebné k úspěšnému dokončení studia jako např. kvalifikační práce, a proto zálohují bez ohledu na předchozí zkušenosti. Je možné, že u jiného výzkumného vzorku bychom získali odlišné údaje.

Hypotézu čtvrtou se nám podařilo dokázat a tudíž studenti, kteří se považují za technické typy lidí, vyhledávají informace z oblasti zabezpečení častěji na Internetu, než netechnické typy studentů. Tuto skutečnost můžeme přisoudit tomu, že technické typy studentů budou mít blíže k věcem týkajících se digitálních zařízení a tudíž budou preferovat i vyhledávání na Internetu.

U ověřování výzkumných předpokladů jsme zjistili, že více než 50 % respondentů slyšelo alespoň 8 z 15 pojmů z oblasti malwaru, ale náš předpoklad, že tito studenti nebudou ve většině případů schopni tyto pojmy správně definovat, byl špatný. Je možné, že u prvních pojmů studenti odpovídali podle skutečných znalostí, ale na závěr si možná chtěli ulehčit vyplňování dotazníku a vyplňovali pouze otázky, které chtěli, případně u kterých si byli jistí, že je umí správně definovat a u jiných pojmů označili, že o nich nikdy předtím neslyšeli, i když pravda byla jiná.

Také se nám potvrdil předpoklad, že studenti nejsou spokojení se současným vzděláním naší společnosti v oblasti malwaru, k tomuto zjištění mohli dojít zejména na základě sebereflexe.

Co se týká zlepšení vzdělání, 69 % studentů by zkvalitnilo výuku na školách, s tímto musíme plně souhlasit. Rozhodně by se měla v učebnicích uvádět alespoň správná terminologie, nikoliv označovat viry za souhrnný název pro všechny druhy malwaru. Na základních školách by se nemuselo jít v oblasti malwaru až tak do hloubky, určitě by mohly být zmíněny některé ze základních druhů malwaru, jako jsou tedy viry, trojský kůň, červ, phishing a hoax. Dále na středních školách by se mohly zařadit i pojmy méně známé jako ransomware, dialer, apod. Určitě je lepší, když samotní studenti budou vědět, jaké druhy malwaru existují, jak se dokáží tyto druhy šířit a jak se proti nim efektivně bránit. Jak jsme viděli v otázce č. 4, je alarmující, že více než polovina studentů čelila útoku malwaru, pozitivní je, že ve většině případů nejspíš nestihl vykonat žádnou škodlivou činnost, ale je otázkou času, kdy se někteří studenti stanou obětí, např. phishingových útoků, z důvodu nedostatečné informovanosti, či nekvalitní výuky na školách.

Závěr

Tato bakalářská práce byla vytvořena zejména z toho důvodu, aby podala ucelený pohled na problematiku, někdy ne zcela správně chápanému, pojmu malware. Myslím, že je toto téma velmi zanedbávané a přitom velmi důležité.

Teoretická část této bakalářské práce se zaměřovala na definování pojmu malware, kterou jsem obohatila svou vlastní definicí, dále jsem malware rozdělila dle jeho druhů, zde byly uvedeny i speciální druhy malwaru a to phishing a hoax, ačkoliv tyto dva pojmy ne zcela splňují definice některých autorů, je velmi důležité je znát, protože denně jich několik přibývá.

Byla zmíněna i skutečnost, že se malware může vyskytovat i na jiných digitálních zařízeních než je počítač, spousta lidí totiž podceňuje takovýto malware, je to zejména z toho důvodu, že se o něm zatím moc nemluví. Dále byly v práci uvedeny nejznámější konkrétní exempláře malwaru, které změnily pohled společnosti ať v pozitivním, či negativním slova smyslu. Práce se zabývala i kybernetickou kriminalitou, určitě některé čtenáře při čtení této bakalářské práce napadla myšlenka, zda oběť malwaru může být trestně stíhána za to, že napomáhá šíření malwaru. V práci bylo uvedeno, že je důležité prokázat úmysl, což je většinou obtížné prokázat i u samotného tvůrce malwaru.

Praktická část této bakalářské práce se zaměřovala na výzkumné šetření, k čemuž byl použit pro sběr dat dotazník. Bylo zjištěno, že zásadním problémem v chápání pojmu malware je skutečnost, že si tento pojem mnozí studenti zaměňují s pojmem počítačový vir. Vzhledem k tomu, že se nám podařilo dokázat druhou hypotézu a tedy jsme potvrdili, že muži častěji chápou správně pojem malware než ženy, je velmi pravděpodobné, že pohlaví může být hlavním faktorem, na kterém závisí celé chápání pojmu malware a souvisejících pojmů. Toto podporuje i všeobecně známá skutečnost, že většinou muži mají k technice blíže než ženy.

Bylo překvapivé, že se nám nepodařilo dokázat hypotézu první a tedy že pohlaví studentů nijak neovlivňuje, zda jeho zařízení bylo, či nebylo napadeno malwarem. Očekávali jsme, že ženy budou častěji obětmi malwaru než muži. Je možné, že toto závisí na době, kterou obě pohlaví tráví na svých zařízeních, případně ženy bývají všeobecně opatrnější než muži a bylo by jistě zajímavé tyto závislosti dále zkoumat v mé diplomové práci.

Taktéž i třetí hypotéza nebyla dokázána a tedy studenti, jejichž zařízení bylo napadeno malwarem, zálohují stejně často jako studenti bez předchozí zkušenosti. Mohlo

by být přínosné zkoumat, jaké konkrétní soubory studenti zálohují. Může to být způsobeno tím, že studenti často píší kvalifikační práce, které si pravděpodobně zálohují a soubory, které považují za méně důležité již ne.

Hypotézu čtvrtou se nám podařilo dokázat, a tedy studenti, kteří se pokládají za technické typy, častěji vyhledávají informace z oblasti malwaru na Internetu než ti, kteří se pokládají za netechnické typy. Zde nebyl výsledek až tak překvapivý, neboť technické typy lidí budou mít k digitálním zařízením blíže a tudíž budou preferovat i vyhledávání informací na Internetu.

K nejdůležitějším poznatkům výzkumu dále patří, že se studenti ztotožňují s naším názorem, že by se měla zkvalitnit výuka na základních a středních školách. Bylo zjištěno, že některé školy používají učebnice, které předávají svou formou žákům a pedagogům špatné informace v oblasti malwaru a tedy výuka nemůže být v žádném případě efektivní. V dalším výzkumu by se mohla analyzovat výuka informatiky, případně informačních a komunikačních technologií na různých školách a zejména analyzovat to, jaké učebnice se při výuce používají a zda korespondují se správným chápáním malwaru a jeho druhů. Pokud by bylo nutné sestavit novou učebnici, mohlo by se využívat poznatků z této bakalářské práce. Samozřejmě tyto nové učebnice by pomohly pouze budoucím generacím. Lidé, u nichž již toto vzdělání bylo zanedbáno, by se měli alespoň nějak motivovat, aby se v oblasti malwaru sami vzdělávali, k tomu by mohly pomoci například reklamní spoty v médiích.

Je možné, že u většího počtu respondentů bychom zaznamenali jiné souvislosti a závislosti, případně u úplně jiného výzkumného vzorku bychom mohli dojít k odlišným výsledkům, než byly uvedeny v této bakalářské práci. Bylo by zajímavé zkoumat odpovědi lidí kolem 50 let, kteří ještě neměli takové možnosti vzdělání, neboť počítače byly v době jejich studia novinkou. Případně zkoumat odpovědi žáků středních škol, kteří se již do světa plného digitálních technologií narodili. Mohlo by být taktéž zajímavé zjišťovat, od kolika let žáci používají digitální zařízení, případně jestli si uvědomují, jaké dopady může mít malware právě na jejich zařízení.

Seznam bibliografických citací

AYCOCK, John. 2006. *Computer viruses and malware*. New York: Springer, xvi, 227 s. ISBN 978-0-387-30236-2.

BARKER, Ian. 2014. Sneaky Android malware calls premium rate numbers when you're not looking. *Betanews* [online]. [cit. 2014-11-20]. Dostupné z: http://betanews.com/2013/12/11/sneaky-android-malware-calls-premium-rate-numbers-when-youre-not-looking/

BELL, Steve. 2014. Which is the worst computer virus in history? Here's our TOP 10. *BullGuard* [online]. [cit. 2015-01-9]. Dostupné z: http://www.bullguard.com/blog/2014/03/which-is-the-worst-computer-virus-in-history-heres-our-top-10.html

CRIDDLE, Linda. 2010. What are Bots, Botnets and Zombies?. *ILOOKBOTHWAYS: The Human Factor in Online Safety* [online]. [cit. 2014-11-17]. Dostupné z: http://www.webroot.com/us/en/home/resources/tips/pc-security/security-what-are-bots-botnets-and-zombies

ČT24. 2013. První počítačový červ zřejmě vznikl omylem. In: *ČT24* [online]. [cit. 2014-11-14]. Dostupné z: http://www.ceskatelevize.cz/ct24/media-it/248727-prvni-pocitacovy-cerv-zrejme-vznikl-omylem/

DOČEKAL, Daniel. 2007. Červ Storm největší současnou hrozbou. *Hospodářské noviny: www.ihned.cz* [online]. [cit. 2015-01-9]. Dostupné z: http://tech.ihned.cz/c1-21749150-cerv-storm-nejvetsi-soucasnou-hrozbou

DUNNIGAN, James F. 2004. *Bojiště zítřka: tváří v tvář globální hrozbě kybernetického terorismu*. Vyd. 1. Praha: Baronet, 356 s. ISBN 80-721-4642-4.

DUPAUL, Neil. 2013. Common Mobile Malware Types: Cybersecurity 101. *VERACODE* [online]. [cit. 2014-12-13]. Dostupné z: https://www.veracode.com/blog/2013/10/common-mobile-malware-types-cybersecurity-101

ERBEN, Lukáš. 2014. Příchod hackerů: I Love You, Melissa. *ROOT.cz: Informace nejen ze světa Linuxu* [online]. [cit. 2015-01-12]. Dostupné z: http://www.root.cz/clanky/prichod-hackeru-i-love-you-melissa/

GARNAEVA, Maria, Victor CHEBYSHEV, Denis MAKRUSHIN, Roman UNUCHEK a Anton IVANOV. 2014. Kaspersky Security Bulletin 2014: Overall statistics for 2014. *Securelist* [online]. [cit. 2015-01-03]. Dostupné z:

http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/

GEIER, Eric a Jan BEDNAŘÍK. 2011. Tip: Jak zbavit počítač škodlivého malware - 2.díl. *PCWorld* [online]. [cit. 2015-02-13]. Dostupné z: http://pcworld.cz/software/tip-jak-zbavit-pocitac-skodliveho-malware-2-dil-43437

HÁK, Igor. 2005. *Moderní počítačové viry* [online]. Hradec Králové, [cit. 2014-06-4]. Dostupné z: http://www.viry.cz/go.php?id=kniha/index. Bakalářská práce. Univerzita Hradec Králové. Vedoucí práce Doc. RNDr. Josef Zelenka, CSc.

HÁK, Igor. 2012. Prevence před útokem. *VIRY.CZ* [online]. [cit. 2015-01-09]. Dostupné z: http://www.viry.cz/prevence-pred-utokem/

HOAX. 2015. Co je to hoax?. *HOAX* [online]. [cit. 2015-02-18]. Dostupné z: http://www.hoax.cz/hoax/co-je-to-hoax

HOSCH, William L. 2013. Malware. *Encyclopædia Britannica* [online]. [cit. 2014-07-08]. Dostupné z: http://www.britannica.com/EBchecked/topic/1477142/malware

HOUSER, Robert. 2012. Aby antiviry neotravovaly život. *Extra PC: Moderní technologie pro lidi*. Brno: Extra Publishing, roč. 2012, č. 1-2, s. 49.

HYPPONEN, Mikko. Malware Goes Mobile. *Scientific American* [online]. 2006 [cit. 2014-12-8]. Dostupné z: http://www.scientificamerican.com/article/malware-goes-mobile/

CHRÁSKA, M. 2006. *Úvod do výzkumu v pedagogice.* Olomouc: VUP. ISBN 80-244-1367-1.

JALŮVKA, Josef. 2000. *Moderní počítačové viry: Podstata, prevence, ochrana*. Praha: Computer Press, 224 s. ISBN 80-7226-402-8.

JIROVSKÝ, Václav. 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 284 s. ISBN 978-80-247-1561-2.

JIROVSKÝ, Václav. 2009. *Základní definice, vztahující se k tématu kybernetické bezpečnosti.* [online]. Praha: Ministerstvo vnitra České republiky, [cit. 2014-06-4]. Dostupné z: www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx

KASÍK, Pavel. 2014. Vlezlý Facebook i Google vědí o vašem věku, těhotenství i zálibách. *Technet.cz* [online]. [cit. 2014-11-14]. Dostupné z:

http://technet.idnes.cz/co-o-vas-vi-online-spolecnosti-dep-/tec_technika.aspx?c=A140624_152745_tec_technika_pka

KASPERSKY LAB. 2014. The very first mobile malware: how Kaspersky Lab discovered Cabir. *Kaspersky Lab* [online]. [cit. 2014-12-14]. Dostupné z: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir

KUCHAŘ, Martin. 2005. Firewall - obrňte své počítače... *PCtuning* [online]. [cit. 2015-03-24]. Dostupné z: http://pctuning.tyden.cz/software/ochrana-pocitace/4296-firewall-obrnte_sve_pocitac

MACHÁČEK, Miroslav. 2013. Počítačová kriminalita a bezpečnost. *Internet pro všechny* [online]. [cit. 2014-02-03]. Dostupné z: http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/

MATEJKA, Ján. 2001. Porušují (ne)vědomí rozesílatelé virů zákon?. *LUPA.cz: Server o českém internetu* [online]. [cit. 2015-02-4]. Dostupné z: http://www.lupa.cz/clanky/porusuji-nevedomi-rozesilatele-viru-zakon/

NAVRÁTIL, Pavel. 2006. *S počítačem nejen k maturitě*. Vyd. 6. Kralice na Hané: Computer Media, 175 s. ISBN 80-866-8660-4.

NAVRÁTIL, Pavel. 2010. *S počítačem na základní škole: pro druhý stupeň základní školy.* Vyd. 4. Bedihošť: Computer Media, 152 s. Vzdělávání, které baví. ISBN 978-80-7402-068-1.

NIEMEYER, Frederik a Petr KRATOCHVÍL. 2011. Mobilní viry: I váš telefon může být cílem. *Chip* [online]. [cit. 2015-01-4]. Dostupné z: http://www.chip.cz/casopis-chip/earchiv/vydani/r-2011/chip-11-11/mobil-viry/

NYKODÝMOVÁ, Helena. 2006. Rootkity? Raději nepřehlížet. *LUPA.cz: Server o českém internetu* [online]. [cit. 2014-11-20]. Dostupné z: http://www.lupa.cz/clanky/rootkity-radeji-neprehlizet/

PADRTA, Aleš a Karel NYKLES. 2013. Ransomware: „policejní virus“ na pitevním stole. *ROOT.CZ: Informace nejen ze světa Linuxu* [online]. [cit. 2014-11-24]. Dostupné z: http://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/

PETROWSKI, Thorsten. 2014. *Bezpečí na internetu: pro všechny*. Překlad Tomáš Kurka. Liberec: Dialog, 241 s. Tajemství. ISBN 978-80-7424-066-9.

Počítačový červ. 2014. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, [cit. 2014-11-12]. Dostupné z:

http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv

ROUSE, Margaret. 2012. Adware. *TechTarget* [online]. [cit. 2014-11-13]. Dostupné z: http://searchsecurity.techtarget.com/definition/adware

ROUSE, Margaret. 2014. Ransomware. *WhatIs.com* [online]. [cit. 2014-11-21]. Dostupné z: http://whatis.techtarget.com/definition/ransomware-cryptovirus-cryptotrojan-or-cryptoworm

ROUSE, Margaret. 2010. Scareware. *WhatIs.com* [online]. [cit. 2014-11-20]. Dostupné z: http://whatis.techtarget.com/definition/scareware

STRICKLAND, Jonathan. 2008. 10 Worst Computer Viruses of All Time. *HowStuffWorks* [online]. [cit. 2015-01-15]. Dostupné z: http://computer.howstuffworks.com/worst-computer-viruses7.htm

Úvod do antivirové problematiky - Jak dělíme počítačové viry. 2010. TrustPort: Keep IT secure [online]. *TrustPort*, [cit. 2014-06-5]. Dostupné z: http://www.trustport.com/manuals/antivirus/csy/techvirsdiv.htm

VŠETEČKA, Roman. 2014. Nový podvodný e-mail obsahuje nebezpečný vir. Přílohu nespouštějte. *Technet.cz* [online]. [cit. 2015-03-10]. Dostupné z: http://technet.idnes.cz/spam-s-virem-win32-trojandownloader-tiny-nkk-win32-injector-bsco-pv2-/sw_internet.aspx?c=A140428_131643_sw_internet_vse

ZACHAR, Martin. 2009. Co je to: Adware, Spyware, ... *Stahuj.cz: Magazín* [online]. [cit. 2015-03-24]. Dostupné z: http://magazin.stahuj.centrum.cz/co-je-to-adware-spyware/

Zákon č. 40/2009 Sb. ze dne 8. ledna 2009, Trestní zákoník. In: *Sbírka zákonů*. 9. 2. 2009, částka 11. ISSN 1211-1244

Seznam tabulek

Seznam grafů

Seznam příloh

Příloha č. 1

Citace ze zákona č. 40/2009, Sb. § 230 Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo

b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) způsobí-li takovým činem značnou škodu,

c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,

d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo

e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

(5) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

Příloha č. 2

Citace ze zákona č. 40/2009, Sb. § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části, bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.

(2) Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.

Příloha č. 3

Citace ze zákona č. 40/2009, Sb. § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat, a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.

Příloha č. 4

Dotazník předvýzkumného šetření

Dobrý den,

studuji na Univerzitě Palackého v Olomouci a chtěla bych Vás požádat o vyplnění tohoto dotazníku, který má posloužit jako součást mé bakalářské práce s názvem „Problematika chápání pojmu malware u vysokoškolských studentů."

Dotazník je anonymní a jeho výsledky budou použity pouze pro výše uvedenou bakalářskou práci a nebudou poskytovány dalším osobám.

Prosím, snažte se vyplnit všechny otázky.

Předem děkuji za Váš čas,

Michaela Studená

1. Které z následujících digitálních zařízení používáte? (můžete označit i více odpovědí)

* Notebook/netbook
* Stolní počítač
* Mobilní telefon s operačním systémem (např. Android, iOS, …)
* Tablet
* Jiné, prosím uveďte jaké:_____
* Žádné (přejděte na otázku č. 6)

2. Napište, k jakým účelům používáte Vaše zařízení:

_____

_____

3. Pokud by Vaše zařízení napadl nějaký škodlivý software (např. počítačový vir, trojský kůň, atd.), z čeho byste měl/a největší obavy? Prosím, vepište.

_____

_____

4. Stal/a jste se někdy obětí škodlivého softwaru (např. vir, trojský kůň, …)? Pozn. škodlivou činností rozumíme např. smazání dat, krádež hesel, atd. Zakroužkujte pouze jednu odpověď.

a) Ano, ale nestihl vykonat žádnou škodlivou činnost nebo o tom nevím.

b) Ano, stihl vykonat škodlivou činnost. Napište jakou: _____

_____

c) Ne

d) Nevím

5. Zálohujete své soubory? Zakroužkujte pouze jednu odpověď.

a) Ano. Napište jak často:_____

b) Ne

6. Napište, co si představujete pod pojmem „malware“:

_____

_____

7. Napište, co si představujete pod pojmem „počítačový vir“:

_____

_____

8. Napište, co si představujete pod pojmem „trojský kůň“ z oblasti digitálních technologií:

_____

_____

9. Napište, co si představujete pod pojmem „zadní vrátka, tzv. backdoor“ z oblasti digitálních technologií:

_____

_____

10. Napište, co si představujete pod pojmem „červ, tzv. worm“ z oblasti digitálních technologií:

_____

_____

11. Napište, co si představujete pod pojmem „spyware“:

_____

_____

12. Napište, co si představujete pod pojmem „adware“:

_____

_____

13. Napište, co si představujete pod pojmem „dialer“:

_____

_____

14. Napište, co si představujete pod pojmem „rootkit“:

_____

_____

15. Napište, co si představujete pod pojmem „logická bomba“:

_____

_____

16. Napište, co si představujete pod pojmem „scareware“:

_____

_____

17. Napište, co si představujete pod pojmem „zombie“ z oblasti digitálních technologií:

_____

_____

18. Napište, co si představujete pod pojmem „ransomware“:

_____

_____

19. Napište, co si představujete pod pojmem „hoax“:

_____

_____

20. Napište, co si představujete pod pojmem „phishing“:

_____

_____

21. V rámci otevřených otázek 6. - 20. jsem se ptala na jednotlivé druhy malwaru. Malware je zjednodušeně řečeno souhrnný název pro všechny hrozby, které mohou napadnout Vaše digitální zařízení a způsobit např. smazání důležitých dat.
Myslíte si, že je naše společnost dobře vzdělaná v oblasti zabezpečení proti těmto hrozbám? Zakroužkujte pouze jednu odpověď.

a) Ano

b) Ne

c) Nedokážu posoudit.

22. Napište, co by mohlo podle Vašeho názoru zlepšit vzdělání v oblasti zabezpečení digitálních zařízení:

_____

_____

23. Napište, kde Vy osobně získáváte informace v oblasti zabezpečení digitálních technologií:

_____

_____

24. Používáte alespoň na jednom svém digitálním zařízení nějaký bezpečnostní program/aplikaci (např. antivir, firewall, apod.)? Zakroužkujte pouze jednu odpověď.

a) Ano

b) Ne

c) Nevím

25. Jste:

a) Žena

b) Muž

26. Napište, jaký obor studujete:

_____

27. Na závěr prosím o zpětnou vazbu k dotazníku, byly všechny otázky srozumitelné, případně, změnil/a byste něco?

_____

_____

Příloha č. 5

Dotazník hlavního výzkumného šetření

Dobrý den,

studuji na Univerzitě Palackého v Olomouci a chtěla bych Vás požádat o vyplnění tohoto anonymního dotazníku, který má posloužit jako součást mé bakalářské práce.

Předem děkuji za Váš čas,

Michaela Studená

1. Které z následujících digitálních zařízení používáte? (můžete označit i více odpovědí)

* Notebook/netbook
* Stolní počítač
* Mobilní telefon s operačním systémem (např. Android, iOS, …)
* Tablet
* Žádné

2. K jakým účelům používáte Vaše zařízení? (můžete označit i více odpovědí)

* Sociální sítě a komunikace (např. Facebook, telefonování, e-mail …)
* Internetové bankovnictví
* Hry a multimédia (např. poslech hudby, sledování filmů, …)
* Studium
* Práce
* Vyhledávání informací a aktuálního zpravodajství
* Online nakupování
* Stahování dat
* Správa webových stránek/blogu
* Nevlastním žádné zařízení a proto nemohu na tuto otázku odpovědět
* Jiné: _____

3. Pokud by Vaše zařízení napadl nějaký škodlivý software (např. počítačový vir, trojský kůň, atd.), z čeho byste měl/a největší obavy?

* Ztráta dat smazáním nebo zašifrováním
* Únik citlivých údajů (např. osobní údaje, údaje k bankovnímu účtu, hesla, …)
* Ovládnutí zařízení jinou osobou (hackerem)
* Ztráta finančního obnosu
* Znemožnění přístupu do svého zařízení
* Nemám obavy
* Nevlastním žádné zařízení a proto nemohu na tuto otázku odpovědět
* Jiné:_____

4. Stal/a jste se někdy obětí škodlivého softwaru (např. vir, trojský kůň, …)? Pozn. Škodlivou činností rozumíme např. smazání dat, krádež hesel, atd. Označte pouze jednu odpověď.

a) Ano, ale nestihl vykonat žádnou škodlivou činnost nebo o tom nevím.
b) Ano, stihl vykonat škodlivou činnost. (přejít na otázku č. 5)
c) Ne.
d) Nevím.

5. Jakou škodlivou činnost stihl škodlivý software na Vašem zařízení vykonat? (Můžete označit i více odpovědí)

* Ztráta dat smazáním nebo zašifrováním
* Únik citlivých údajů (např. osobní údaje, údaje k bankovnímu účtu, hesla, …)
* Ovládnutí zařízení hackerem
* Ztráta finančního obnosu
* Znemožnění přístupu do svého zařízení
* Jiné: _____

6. Zálohujete své soubory? Označte pouze jednu odpověď.

a) Ne.
b) Nevím, co je to zálohování souborů.
c) Nevlastním žádné zařízení a proto nemohu na tuto otázku odpovědět.
d) Ano. Uveďte, jak často: _____

7. Slyšel/a jste někdy o pojmu „malware“?

a) Ano

b) Ne (přeskočit otázku 8)

8. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „malware“:

a) Škodlivý kód, který se dokáže kopírovat.

b) Souhrnný název pro všechny druhy škodlivého softwaru.

c) Nemoc počítačů, při které dochází k totálnímu zničení systému.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

9. Slyšel/a jste někdy o pojmu „počítačový vir“?

a) Ano

b) Ne (přeskočit otázku 10)

10. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „počítačový vir“:

a) Škodlivý kód, který se dokáže kopírovat.

b) Souhrnný název pro všechny druhy škodlivého softwaru.

c) Nemoc počítačů, při které dochází k totálnímu zničení systému.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

11. Slyšel/a jste někdy o pojmu „trojský kůň“ z oblasti digitálních technologií?

a) Ano

b) Ne (přeskočit otázku 12)

12. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „trojský kůň“ z oblasti digitálních technologií:

a) Druh počítačového viru, který se dokáže ukrýt v zařízení tak dobře, že ho neodhalí ani zabezpečovací prvky systému.

b) Software, který vypadá užitečně, ale po vniknutí do systému je škodlivý.

c) Škodlivý software, který se rozesílá jako skrytá příloha e-mailu, po jehož otevření, dojde ke zničení systému.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

13. Slyšel/a jste někdy o pojmu „zadní vrátka, tzv. backdoor“ z oblasti digitálních technologií?

a) Ano

b) Ne (přeskočit otázku 14)

14. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „zadní vrátka, tzv. backdoor“ z oblasti digitálních technologií:

a) Jakýkoliv způsob, kterým se obejde zabezpečení systému a tím dává prostor hackerovi ovládnout cílové digitální zařízení.

b) Obnovení systému ze zálohy po napadení digitálního zařízení škodlivým softwarem.

c) Způsob, kterým se maskuje aktivita škodlivého kódu na digitálním zařízení.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

15. Slyšel/a jste někdy o pojmu „červ, tzv. worm“ z oblasti digitálních technologií?

a) Ano

b) Ne (přeskočit otázku 16)

16. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „červ, tzv. worm“ z oblasti digitálních technologií:

a) Druh škodlivého softwaru, který se vyznačuje tím, že maže pouze části souborů a tím se zvětšuje on sám.

b) Škodlivý software, který se dokáže šířit pouze pomocí USB flash disků.

c) Škodlivý software šířící se pomocí sítě.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

17. Slyšel/a jste někdy o pojmu „spyware“?

a) Ano

b) Ne (přeskočit otázku 18)

18. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „spyware“:

a) Škodlivý software, který shromažďuje informace z infikovaného digitálního zařízení a odesílá je jiné osobě.

b) Škodlivý software, který je jedním z druhů počítačových virů.

c) Software, který má za úkol sledovat, jestli se v systému nenachází škodlivý software nebo jiná hrozba.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

19. Slyšel/a jste někdy o pojmu „adware“?

a) Ano

b) Ne (přeskočit otázku 20)

20. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „adware“:

a) Škodlivý software, který se dostane do digitálního zařízení kliknutím na reklamu na nedůvěryhodných stránkách.

b) Škodlivý software, který způsobuje zobrazování vyskakovacích reklam.

c) Software, ve kterém lze jednoduše vytvořit reklamu, a tu pak můžeme umístit na Internet.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

21. Slyšel/a jste někdy o pojmu „dialer“?

a) Ano

b) Ne (přeskočit otázku 22)

22. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „dialer“:

a) Člověk, který napomáhá k šíření škodlivého softwaru.

b) Vir na mobilní telefony a tablety.

c) Škodlivý software, který v případě počítačů mění způsob vytáčení čísla pro internetové připojení a v případě mobilních telefonů posílá prémiové SMS zprávy.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

23. Slyšel/a jste někdy o pojmu „rootkit“?

a) Ano

b) Ne (přeskočit otázku 24)

24. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „rootkit“:

a) Člověk, který napomáhá k šíření škodlivého softwaru.

b) Škodlivý software, který maskuje činnost dalších druhů škodlivého softwaru.

c) Nástroje sloužící pro opravu digitálního zařízení, které napadl škodlivý software.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

25. Slyšel/a jste někdy o pojmu „logická bomba“?

a) Ano

b) Ne (přeskočit otázku 26)

26. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „logická bomba“:

a) Nástroj k odstranění jednodušších forem škodlivého softwaru.

b) Programátorská chyba v programu, která dokáže být bránou pro škodlivý software.

c) Škodlivý software, který má za úkol spustit svou škodlivou činnost za předem určených podmínek, které stanovil autor tohoto škodlivého softwaru.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

27. Slyšel/a jste někdy o pojmu „scareware“?

a) Ano

b) Ne (přeskočit otázku 28)

28. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „scareware“:

a) Poplašná zpráva, která se snaží vystrašit uživatele, kteří si ji přečtou.

b) Falešná webová stránka, která se vydává např. za stránky banky a tím vyláká od uživatele údaje k internetovému bankovnictví.

c) Škodlivý software, který vypadá jako např. antivir, ten pak najde na zařízení spoustu falešných problémů, pro jejichž odstranění je nutné si připlatit.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

29. Slyšel/a jste někdy o pojmu „zombie“ z oblasti digitálních technologií?

a) Ano

b) Ne (přeskočit 30)

30. Označte jednu odpověď, která se nejvíce přibližuje Vaši představě o pojmu „zombie“ z oblasti digitálních technologií:

a) Napadené zařízení, které hacker využívá k napadení ostatních zařízení v síti.

b) Škodlivý software, který již byl v minulosti ze zařízení odstraněn, ale vyskytl se znovu.

c) Zastaralá technologie, která je opět uvedena do provozu.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

31. Slyšel/a jste někdy o pojmu „ransomware“?

a) Ano

b) Ne (přeskočit otázku 32)

32. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „ransomware“:

a) Nástroj k odstranění jednodušších forem škodlivého softwaru.

b) Škodlivý software, který zašifruje soubory, případně celý operační systém a žádá výkupné.

c) Škodlivý software, který má pouze za úkol zpomalení systému.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

33. Slyšel/a jste někdy o pojmu „hoax“?

a) Ano

b) Ne (přeskočit otázku 34)

34. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „hoax“:

a) Poplašná zpráva, která se snaží vystrašit uživatele, kteří si pak na základě tohoto výmyslu mohou např. smazat některá důležitá data.

b) E-mailová zpráva, která vypadá jako např. z banky a snaží se od uživatele získat citlivé informace.

c) Škodlivý software, který má za úkol najít a poslat třetí osobě hesla, která najde na napadeném zařízení.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

35. Slyšel/a jste někdy o pojmu „phishing“?

a) Ano

b) Ne (přeskočit otázku 36)

36. Označte jednu odpověď, která se nejvíce přibližuje Vaší představě o pojmu „phishing“:

a) Nevyžádaná reklama.

b) Většinou e-mail, případně falešná stránka, která vypadá jako např. z banky a snaží se získat citlivé údaje od uživatele.

c) Poplašná zpráva, která se snaží vystrašit uživatele, kteří si pak na základě tohoto výmyslu mohou např. smazat některá důležitá data.

d) Mám jinou představu. Uveďte jakou:_____

e) Pojem jsem slyšel/a, ale nedokážu si pod tím nic představit.

37. V rámci posledních 15 otázek jsem se ptala na jednotlivé druhy malwaru. Malware je zjednodušeně řečeno souhrnný název pro všechny hrozby, které mohou napadnout Vaše digitální zařízení a způsobit např. smazání důležitých dat. Myslíte si, že je naše společnost dobře vzdělaná v oblasti zabezpečení proti těmto hrozbám?

a) Ano

b) Ne

c) Nedokážu posoudit.

38. Co by mohlo podle Vašeho názoru zlepšit vzdělání v oblasti zabezpečení digitálních zařízení? (Můžete označit i více odpovědí)

* Zkvalitnění výuky na školách
* Informační letáky a brožury
* Reklamy v médiích
* Televizní pořady věnující se této problematice
* Kurzy, semináře a přednášky pro veřejnost
* Literatura pro laiky
* Výukové portály věnující se této problematice
* Jiné, napište:_____

39. Kde Vy osobně získáváte informace v oblasti zabezpečení digitálních technologií?

* od přátel/rodiny/partnera
* na Internetu
* u odborníků
* v literatuře
* z médií
* ve škole
* na pracovišti
* nikde
* jinde, uveďte kde:_____

40. Používáte alespoň na jednom svém digitálním zařízení nějaký bezpečnostní program/aplikaci (např. antivir, firewall, apod.)? Zakroužkujte pouze jednu odpověď.

a) Ano
b) Ne
c) Nevím

41. Jaký obor studujete?

_____

42. Jste:

a) Žena
b) Muž

43. Za jaký typ člověka se považujete?

a) Technický typ
b) Netechnický typ

ANOTACE

Jméno a příjmení:	Michaela Studená
Katedra:	Katedra technické a informační výchovy
Vedoucí práce:	doc. PhDr. Miroslav Chráska, Ph.D.
Rok obhajoby:	2015

Název práce:	Problematika chápání pojmu malware u vysokoškolských studentů
Název v angličtině:	The problem of understanding the term malware in university students
Anotace práce:	Bakalářská práce se zabývá problematikou různého pojetí pojmu malware, a to včetně všech jeho druhů, včetně speciálních případů. Jejím cílem je, na základě hlubší analýzy, podat ucelený pohled na tuto problematiku, která je ve společnosti velmi zanedbávaná, ale přitom velmi důležitá. Dále se bakalářská zaměřuje na problematiku malwaru i na jiných digitálních zařízeních než počítače. Zabývá se i právní problematikou, ale také motivací k tvorbě malwaru. Na závěr jsou uvedeny i metody prevence a zabezpečení zařízení proti malwaru. Praktická část bakalářské práce je zaměřena zejména na výzkum toho, zda vysokoškolští studenti mají problémy s chápáním pojmu malware a pojmů s tím souvisejících. Celý výzkum probíhal ve dvou etapách. V první etapě byl vytvořen dotazník pro předvýzkum, na základě kterého bylo ověřeno, zda je samotný dotazník srozumitelný. Jeho některé výsledky byly také dále využity v hlavním výzkumu (v dotazníku) jako možně odpovědi. Druhá část výzkumu byla provedena jako klasické kvantitativní dotazníkové výzkumné šetření. Byly stanoveny výzkumné problémy a dále byly ověřovány stanovené výzkumné hypotézy a předpoklady. Z výsledků výzkumného šetření jsme

	dospěli k závěru, že studenti mají opravdu problém s chápáním pojmu malware a častěji místo toho používají pojem počítačový vir, zjistili jsme, že tato skutečnost je závislá i na pohlaví studentů. Překvapivé bylo, že studenti si zaměňují i další pojmy.
Klíčová slova:	malware; rozdělení malwaru; kybernetická kriminalita; motivace; malware na dalších zařízeních; prevence; zabezpečení; nejznámější exempláře malwaru, dotazník
Anotace v angličtině:	Bachelor thesis deals with various conceptions of the term malware, including all of its types and special cases. Its purpose is, on the basis of a deeper analysis, to offer a comprehensive view on this issue, which is often being neglected in the society, but is nevertheless very important. In addition, Bachelor thesis focuses on the issue of malware in connection to other digital devices than just computers. Furthermore, it deals with legal issues but also the motivation to create malware. In conclusion, methods of prevention of malware and device security are listed as well. The practical part of the thesis is focused on researching whether college students have problems with understanding of the concept of malware and the concepts related to it. The research was conducted in two stages. A questionnaire for preliminary research was created in the first phase, based on which it has been verified that the questionnaire is understandable. Its results were also used in the main research (in the questionnaire) as possible answers. The second part of the research was performed as a classical quantitative questionnaire research. In the thesis, the research issues were established and a set of research hypotheses and assumptions was verified. As a result of the research investigation, we concluded that the students really do have problems with understanding of the term malware and more often use the term computer virus instead; it was also found that this fact is

	dependent on the sex. It was surprising that students often confuse other concepts as well.
Klíčová slova v angličtině:	malware; distribution of malware; cybercrime; motivation; malware on other digital devices; prevention; security; best known specimens of malware; questionnaire
Přílohy vázané v práci:	5
Rozsah práce:	64 stran + 20 stran příloh
Jazyk práce:	český