Univerzita Hradec Králové
Fakulta informatiky a managementu

Počítačová kriminalita

Bakalářská práce

Autor: Vojtěch Hartman
Studijní obor: Informační management

Vedoucí práce: JUDr. Jan Janeček, Ph.D.

Hradec Králové duben 2015

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 29.4.2015 Vojtěch Hartman

Poděkování:

Rád bych poděkoval JUDr. Janu Janečkovi, Ph.D. za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce.

Anotace

Bakalářská práce je zaměřena na problematiku počítačové kriminality. V teoretické části práce je stručně shrnuta historie vývoje počítačové kriminality, jsou vysvětleny některé důležité pojmy týkající se dané problematiky, a jsou popsány samotné formy počítačové kriminality. V neposlední řadě je řešena otázka právní úpravy, ve vztahu k uvedeným formám. Cílem praktické části je nastínit situaci dnešní doby a pokusit se formou dotazníkového šetření zjistit, jak studenti postupují v souvislosti s ochranou svých osobních údajů vůči hrozbám na internetu a jak nakládají s nelegálně získaným softwarem dostupným na internetu.

Annotation

Title: Computer crime

The bachelor thesis is focused on computer crime. Theoretical part briefly summarizes the history of development of computer crime, it explains some important terms related to issue and describes itself forms of computer crime. Furthermore, it deals with question of legislation in regard to these forms of computer crime. Practical part is about to outline the situation of present time and by the form of questionnaire tries to find out, to how students doing in relation to the protection of their personal data against online threats and how they deal with illegally obtained software available on the internet.

Obsah

Seznam použitých zkratek

ASCII – americký standartní kód pro výměnu informací
BSA – organizace, která v Česku bojuje proti nelegálnímu užívání softwaru
CD – typ digitálního optického datového nosiče
ČPU – Česká protipirátská unie
ČR – Česká republika
ČSSR – Československá socialistická republika
DVD – typ digitálního optického datového nosiče
IMB – poskytovatel řešení a služeb informačních technologií
ISO – soubor obsahující digitální kopii dat z optického disku
IT – informační technologie
MP3 – formát zvukových souborů
P2P – typ počítačových sítí, ve kterých spolu klienti komunikují
PC – Personal Computer, osobní počítač
PČR – Policie České republiky
SMS – služba krátkých textových zpráv
TCP/IP – hlavní komunikační protokol celosvětové sítě Internet
USB – univerzální sériová sběrnice, způsob připojení periferií k počítači

1 Úvod

V dnešní uspěchané době je počítač zcela přirozenou a nedílnou součástí života každého člověka a je takřka nemožné nalézt oblast, kam by informační technologie nezasahovaly. Jedinci, kteří namítají, že se jich tato problematika netýká, protože nevlastní osobní počítač, jsou na omylu. Pravdou je, že počítač a veškeré informační technologie nás ovlivňují natolik, že si tohoto nesporného faktu nemusíme vůbec všimnout.

Například, navštívíme-li úřad práce, setkáme se tam s úřednicí, která bude naše požadavky vyřizovat pomocí počítače a dat, které ji tento přístroj vygeneruje. Dokáže ulehčit práci mnoha lidem nejen na úřadech, ale i na ve školství, zdravotnictví, státní správě, armádě či v soukromém sektoru. Dále počítač dokáže řídit křižovatky, chránit vlaky před srážkou a vykonává mnoho dalších důležitých a záslužných činností.

Jak již bylo zmíněno, počítač poskytuje velké výhody široké skupině lidí. Avšak každá mince má svůj rub i líc a nic není pouze černé a bílé, což téměř stoprocentně platí i v této oblasti.

Počítačová kriminalita je fenomén dnešní doby, ukusujíc z pomyslného koláče páchané kriminality rok od roku větší část. V 21. století, dosahuje počítačová kriminalita obrovský rozmach spojený s revolucí v oblasti vývoje hardwaru a softwaru. Tento vývoj přináší nové možnosti nejen poctivým lidem, ale i lidem pro které je počítač prostředkem pro páchání nelegální činnosti.

2 Cíl a metodika práce

Teoretická část této práce vymezuje základní pojmy v oblasti počítačové kriminality, těmi jsou *kyberprostor, kybernalita a informace.* Dále zahrnuje stručný historický pohled na vývoj počítačové kriminality v období od 70. do konce 90. let minulého století a zaměřuje se zejména na analýzu současného stavu počítačové kriminality, kde popisuje některé formy počítačové kriminality, kterými jsou softwarové pirátství, hacking, spamming a šíření škodlivého softwaru, spolu s jejich právní úpravou. Jsou zde zohledněny také organizace zabývající se bojem proti počítačové kriminalitě.

Cílem praktické části je nastínit situaci dnešní doby a pokusit se formou dotazníkového šetření zjistit, jak studenti postupují v souvislosti s ochranou svých osobních údajů vůči hrozbám na internetu. Dotazník byl zcela anonymní a sestaven tak, aby odpovídal cílům dotazníkového šetření a stanoveným předpokladům. Obsahoval celkem 15 otázek týkajících se oblasti počítačové kriminality.

Praktická část práce se zabývá nejen metodikou dotazníkového šetření, ale i jakým způsobem probíhalo. Dále se věnuje jeho výsledkům.

V návaznosti na obecný cíl dotazníkového šetření jsou stanoveny širší výzkumné cíle, s nimiž jsou shodné dílčí výzkumné otázky a hypotézy.

2.1 Širší výzkumné cíle

Cíl 1: Zjistit, zda je dosaženo u studentů dostatečného zabezpečeni před počítačovými hrozbami.

Cíl 2: Stanovit si, kolik % studentů má založený účet na Facebooku a sdílí prostřednictvím něj osobní informace.

Cíl 3: Zjistit, zda studenti přicházejí do styku s nevyžádanou poštou a zda ji otvírají.

Cíl 4: Zjistit, jakým způsobem studenti nakládají s nelegálním softwarem dostupným na internetu.

2.2 Výzkumné otázky

Otázka 1: Je zabezpečení PC před počítačovými hrozbami dostačující?

Otázka 2: Jaké procento studentů sdílí osobní informace prostřednictvím sociální sítě Facebook?

Otázka 3: Jak často přichází studenti do styku s nevyžádanou poštou?

Otázka 4: Jaký je vztah studentů k nelegálnímu softwaru a jeho užívání?

2.3 Formulace hypotézy

Hypotéza 1:

- více než 50% studentů používá Freeware – bezplatnou ochranu svých dat
- většina studentů volí heslo obsahující pouze kombinaci písmen a čísel s délkou do pěti znaků

Hypotéza 2:

- účet na sociální síti Facebook vlastní všichni z dotazovaných a zhruba čtvrtina z nich zde o sobě sdílí osobní informace

Hypotéza 3:

- 25% respondentů obdrží zhruba 30 spamů měsíčně, nadpoloviční většina z nich ale tuto poštu neotevírá

Hypotéza 4:

- 90 % studentů vlastní nelegální software v podobě filmů, hudby, her…
- pro studenty je snadno-přístupný a opatřují si ho nejčastěji na Filehostingových stránkách

3 Teoretická část

3.1 Vymezení pojmů kyberprostor, kybernalita, informace

Lidská společnost se neustále posouvá vpřed. Velký vliv na to má vzájemné ovlivňování společnosti a jedince. K tomu vždy docházelo ve fyzickém prostředí. Významný posun v mezilidské komunikaci a výměně informací s sebou přinesla výpočetní technika a internet. Možnost vytváření nesmrtelných virtuálních jedinců a potlačená potřeba kompromisů byly jenom některé z příčin, které vedly ke vzniku nového „kybernetického" světa - **kyberprostoru**. Pro mnohé se stal kyberprostor v určitých směrech snesitelnější a příjemnější než ten reálný. Ačkoliv tento prostor přejímá rysy současné společnosti, nárokuje si také vlastní pravidla, které společnost musí přijímat, nebo jim čelit, pokud chce v kyberprostoru přežít. Tímto způsobem popisuje změny v prostředí mezilidské komunikace Václav Jirovský (2007).

O kyberprostoru můžeme tedy hovořit jako o rozsáhlé počítačové síti, která umožňuje komunikaci a výměnu informací. Kyberprostor má své výhody, jsou jimi především rychlost a do jisté míry také anonymita internetu. Tento fakt vedl ke zformování specifického druhu kriminality – kybernality.

Počítačovou kriminalitou, neboli **kybernalitou**, jak ji nazývá Václav Jirovský (2007)**,** se rozumí taková činnost, kterou se porušuje zákon, nebo je v rozporu s morálními pravidly společnosti. Může být namířena proti samotným počítačům, tedy jejich hardwaru, softwaru, datům a sítím, nebo v ní naopak počítač může vystupovat jako nástroj, kterým se trestný čin páchá. Také počítačová síť, ke které jsou připojená zařízení, může být prostředím, v němž se taková činnost odehrává.

S počítačovou kriminalitou souvisí i jisté trendy. Jejich význam roste spolu s vývojem počítačové kriminality. Například se objevuje rozchod v deviantním chování a jeho stará podoba v nových formách (např. krádež dat). Zdokonalují se techniky pro páchání trestných činů (hacking, počítačové útoky s využitím virů). Také

se ale rozvíjí metody pro vyšetřování trestných činů a nová pravidla pro jurisdikci a trestání. (Gřivna, Polčák, 2008)

Kyberprostor nepředstavuje pouze jakési pole působnosti počítačové kriminality, ale umožňuje jeho uživatelům komunikovat a vyměňovat si informace. Pojem **informace** se objevuje v různých souvislostech, ať už jde o informace o dané události, výsledky nějakého experimentu, nebo informace v daném spise. Jedna z mnoha definic tvrdí, že účelem informací je organizování elementů do systematických celků.

Přestože je informace pouhé sdělení, někdy i jednoduché číslo, můžeme s údivem sledovat, vlastnosti systémů, které jsou prostřednictvím informací organizované. Stejně tak pozoruhodné je sledovat efekty spontánního vytváření, zpracovávání a výměny informací v prostředí informační společnosti. Docházíme tak k závěru, že ve společnosti, kde není bráněno vzájemné výměně informací, a kde je využívána každodenní komunikace, ať už sdělení novinek, či banální sdělení pozdravu, dochází k budování fyzické a logické informační infrastruktury, což má za následek rozvoj přirozených základních společenských hodnot, jako je například slušnost, rovnost, solidarita a pořádek. (Gřivna, Polčák, 2008)

3.2 Stručný popis historického vývoje počítačové kriminality

Pohledem do historie počítačové kriminality, lze zjistit, že možnosti pachatele byly limitovány soudobým stavem techniky. Jak uvádí Vladimír Smejkal (1999), jeden z prvních případů, které lze označit za počítačovou kriminalitu, se odehrál v 70. letech na území dnešní ČR. Jednalo se o pracovníka úřadu důchodového zabezpečení, který za pomoci magnetu poškodil záznamy na magnetických páskách a který tímto jednáním naplnil skutkovou podstatu trestného činu sabotáže (později bylo dané jednání překvalifikováno). Tímto činem způsobil pozastavení výplat důchodu v celé ČSSR.

Z historického hlediska jsou důležitým bodem 80. léta, která představují zcela novou éru v oblasti informačních technologií a tedy současně i počítačové kriminality.

Tehdy uvedla americká firma IBM na trh první počítač typu IBM PC. Tím se vytvořily všechny předpoklady k tomu, aby se osobní počítač dostal do každé domácnosti a kanceláře. Dochází také ke sloučení telefonní linky s počítačem. Čím dál více počítačů a modemů se vzájemně propojovalo skrze sítě a tím prakticky došlo k rozšíření předchůdce dnešního internetu.

V této éře figurovalo hned několik významných zahraničních hackerů. Kevin Mitnick je známý především pro své útoky na počítače firmy Digital Equipment z roku 1988. Dalším byl Robert Morris, ten vypustil v roce 1988 do světa první počítačový virus, který tehdy upozornil na nový typ počítačové kriminality. Do třetice, Kevin Poulsen je známý především svým činem v roce 1991, kdy se naboural do telefonních linek kalifornské rozhlasové stanice.

Co se počítačového pirátství týče, zásadní věcí, která umožnila jeho rozmach, byl vznik médií pro digitální záznam dat neboli kompaktních disků. Postupem času a snižováním ceny za vypalovací software se pirátem mohl stát kdokoliv, kdo počítač s patřičným softwarem vlastnil.

V roce 1994 byla prostřednictvím počítače provedena bankovní loupež, která tehdy pachateli, ruskému matematikovi Vladimirovi Levinovi, vynesla 10 milionů dolarů. Jedná se o případ Citibank. Právě tento čin ukázal, kam se bude počítačová kriminalita ubírat. (Matějka, 2002)

3.3 Analýza současného stavu počítačové kriminality

S vývojem technologií se mění i definice počítačové kriminality. Pojmem počítačová kriminalita je třeba chápat páchání trestné činnosti, v níž počítač figuruje jako soubor technického a programového vybavení, nebo pouze komponenta či větší množství počítačů propojených do počítačové sítě, a to buď jako předmět této činnosti, vyjma majetkové trestné činnosti, nebo jako nástroj trestné činnosti.

Z pohledu trestního práva bylo v minulých letech vymezeno, kdy není počítačovou kriminalitou chápána trestná činnost, jejímž objektem zájmu pachatele majetkového trestného činu je výpočetní technika (například krádež počítače).

Může však docházet k prolínání takových činností, kdy je výpočetní technika objektem zájmu čistě „počítačového“ trestného činu, ale pokud je tato technika poškozena, tento fakt vede k souběhu s majetkovým trestným činem.

Z hlediska kriminalistiky lze provést základní dělení počítačové kriminality na:

- ✓ Porušování autorského práva - počítačové pirátství (§ 152 tr. zák.).
- ✓ Poškození a zneužití záznamu na nosiči informací (§ 257a tr. zák.), a to jako útok z vnějšku subjektu, zevnitř subjektu, případně útoky kombinované.
- ✓ Ostatní počítačová trestná činnost (činy které využívají výpočetní techniku jako prostředek k páchání trestných činů, nikoliv jako přímý objekt zájmu pachatele, avšak objektem zájmu mohou být počítačová data). (www.mvcr.cz)

Tato analýza vychází z některých nejběžnějších forem počítačové kriminality, se kterou se mohou dostat do styku právě studenti Fakulty informatiky a managementu Univerzity Hradec Králové, na které je směřováno dotazníkové šetření.

V současnosti je nejvyšší pozornost věnována problému porušování autorského práva – softwarovému pirátství. Podle společnosti IDC (www.idc-czech.cz), jedné z nejvýznamnějších světových analytických a poradenských společností, se míra softwarového pirátství v Česku aktuálně pohybuje kolem 34%.

Druhým nejčastějším problémem je u nás narušování informačních systémů (tzv. hacking). Při něm dochází k průnikům do počítačových sítí a neoprávněnému čtení nebo změně dat. Škoda, která je tímto jednáním způsobena, závisí na způsobu využívání webových stránek. Napadeny mohou být například školní stránky, kde jsou vystaveny informace, které tu onu školu popisují, přičemž jejich případné poškození lze snadno opravit. Naopak značnou škodu může způsobit poškození stránek komerční firmy, která jejich prostřednictvím řeší objednávky svých produktů. (www.mvcr.cz)

3.3.1 Formy počítačové kriminality

Jednotlivé druhy počítačové kriminality lze rozdělit ze dvou hledisek, jak uvádí Matějka (2002), jednak z hlediska pozice, ve které je počítač při páchání trestné činnosti a za druhé podle typu činu.

a) Podle postavení počítače při páchání trestné činnosti se dělí na:

- ✓ Protiprávní jednání, kde je počítač *terčem útoku*
- ✓ Protiprávní jednání spáchané s počítačem jako *nástrojem takové činnosti*

b) Podle typu činu se pak dělí na:

- ✓ Protiprávní jednání *tradiční*, kde je počítač v pozici ať už terče, nebo nástroje útoku. Takovým jednáním může být například krádež, loupež, zpronevěra, co se útoku na počítač týče, nebo podvody, padělání, extremismus na internetu a výpalné co se týče jednání s využitím počítače.

- ✓ Protiprávní jednání *nová*, která se objevila až s nástupem moderních informačních technologií a v jiných oblastech života se neobjevují vůbec. Příkladem jednání proti počítači může být hacking, krádeže dat a zneužití osobních údajů, na straně druhé s využitím počítače například spamming, neoprávněné užívání softwaru – softwarové pirátství, škodlivý software.

SOFTWAROVÉ PIRÁTSTVÍ

Jak již bylo uvedeno výše, je u nás velká pozornost věnována především neoprávněnému užívání softwaru, který je chráněn autorskými právy, neboli softwarovému pirátství, konkrétněji ***pirátství autorských práv***. To bývá často označováno za krádež. Z toho přirozeně vyplívá, že cokoliv podléhá autorským právům, je možné ukrást a zároveň téměř vše, co stojí za autorskou ochranu, stojí za to ukrást.

Pro mnoho lidí je těžké si představit, že ubližují někomu tím, když si nahrají televizní pořad, stáhnou hudbu, nebo kamarádovi zkopírují film. Digitální kopie neztrácejí

kopírováním svou kvalitu, tím pádem se mohou rozmnožit třeba na milion kopií. Nejsou to padělky ani repliky originálu, ale totožné kopie se zachovalou kvalitou. Z toho vyplívá, že reálnou škodu způsobí právě digitální pirátství.

Zábavní průmysl v čele s vlastníky autorských práv se snaží pirátství v médiích vylíčit jako zločin na stejné úrovni jako je třeba loupež nebo krádež auta. Snaží se nás přesvědčit, že kopírováním bez zaplacení připravujeme jejich zaměstnance o příjmy, popř. o práci. Naopak piráti se brání tím, že majitele o jeho majetek nepřipravují. Tvrdí, že rozdíl mezi krádeží a pirátstvím je ten, že zatímco krádež znamená odcizení věci, pirátství znamená pouhé zkopírování věci. Argumentují tím, že majitele připraví maximálně o potencionální výdělek. Hodnota tohoto výdělku je však pochybná, protože se nedá odhadnout, kolik lidí by si jejich tvorbu koupilo.

Pro představu jakým způsobem tento druh pirátství probíhá, je důležité vymezit prostor, aktéry a předměty dění. To vše zahrnuje tzv. ***pirátská scéna***, neboli Warez scéna. Ta popisuje soubor sdružených pirátských sítí a pirátských nadšenců, kteří získávají a kopírují nové filmy, hudbu a hry a distribuují je přes internet, často před oficiálním uvedením na trh. Většinu prvků pirátství, ať už jde o pouliční prodavače nebo filmy a hudbu, spojuje společný zájem, tím je právě warez scéna. Je poháněna jednoduchým pravidlem: každý chce něco, a jediným způsobem jak to získat, je nabídnout něco, co chce někdo jiný.

I když je každá pirátská scéna odlišná, všichni piráti sdílí stejnou touhu po softwaru a médiích zdarma. Každým rokem se objeví nová forma pirátství, nebo nový druh ochrany proti kopírování. Jedinou jistotou pirátství je evoluce, v důsledku toho pirátství nadále existuje a je schopné čelit každé nově vytvořené technologii, která by jim měla znemožnit jejich činnost.

Každý pirát má různé speciální dovednosti, podle toho, na jaký druh média se zaměřuje. Podle zájmů se softwaroví piráti často sdružují do skupin. Taková skupina, ač dobře organizovaná je pouze volný spolek jejich členů, takže ji nedefinuje prakticky nic než hranice „chat-roomů“ kde se pohybují. (Craig,Honick, 2008)

Pro autorská díla, se kterými je nakládáno v rozporu s autorským právem existuje souhrnný název ***Warez***. Tato díla bývají distribuována softwarovými piráty nebo jejich skupinami. Pro každý druh média existuje jiný druh piráta. Běžným terčem útoku bývají následující média:

- ✓ *Hudba*

Hudba je dnes beze sporu nejrozšířenější pirátské médium na světě. Hudební pirátství není tak časově náročné. Hudební sobory jsou menší a snadnější na přenos, než jiné soubory. Na hudební pirátské scéně se vydá v průměru o mnoho více titulů než například na herní pirátské scéně. Hudba navíc není chráněná tolik co například hry nebo filmy. Mnoho nahrávacích společností dnes sice používá na svých albech nějaký druh ochrany DRM, avšak většina pirátů ji lehce prolomí.

- ✓ *Filmy*

Většinou jsou filmy vydávány na DVD nosičích až několik týdnů po uvedení premiéry. Tvůrci tak maximalizují svůj zisk. Skalní fanoušci však nechtějí čekat na film několik týdnů, chtějí ho vidět hned, takže budou-li mít tu možnost, stáhnou si nekvalitně nahranou kopii oblíbeného filmu, jakmile to bude možné. Pirátské filmové tituly se znatelně liší velikostí i kvalitou. Čím více se soubor zkomprimuje a zabere méně místa, tím více ztratí na kvalitě a naopak.

- ✓ *Televizní pirátství*

Tento druh pirátství není tak častý jako pirátství nejžádanějších filmových hitů. Dříve o pirátské televizní programy neměl téměř nikdo zájem. Nebyl důvod nahrávat nekvalitní televizní program, když běžel v televizi. Spolu se zlepšováním pirátské televizní scény se však zlepšovala i kvalita jejích programů a často se na internetu objevovaly dříve než v televizi samotné. Piráti si tak postupně získali pozornost scény. Dnešní počítačoví piráti vydávají televizní program ve vysoké kvalitě, navíc bez reklam a chyb.

- ✓ *Hry*

Cílem pirátů jsou samozřejmě i všechny hry určené pro PC a konzole jako jsou XBOX nebo PlayStation. Piráti her se specializují na crackování a vydávání her, buď v jejich ISO podobě nebo naripované podobě. Skupiny hackerů se navzájem předhánějí, která vydá hru jako první. U PC her stačí, aby skupina vydala cracknutou hru. U konzolí je potřeba navíc modchip, což je zařízení, které se používá pro omezení protipirátské ochrany.

- ✓ *E-knihy a bookware*

S rozvojem přenosných počítačů, neustále roste i obliba digitálních kopií různých tištěných materiálů (bookware). Knihy nevynikají takovou ochranou jako jiná média a proti pirátům se chrání velice obtížně. Každý autor s tím musí počítat. Tištěné verze knih piráti většinou nepoužívají. Na internetu se nachází spousta e-knihoven, kde je možné si předplatit přístup k online e-knihám. Piráti si přístup k takové knihovně koupí většinou podvodem a následně použijí aplikaci, která za pomocí skeneru převede veškerý obsah i s obrázky a formátováním do dalšího dokumentu. Tím vznikne nová digitální kopie. Tato metoda je sice časově náročná, ale mimo to vyžaduje pouze aplikaci na konverzi e-knih a počítač se scannerem.

- ✓ *Zábava pro dospělé*

Nejprodávanějším a nejúspěšnějším druhem zábavy na internetu je dlouhodobě pornografie. Filmů pro dospělé se vydá asi dvakrát tolik než v Hollywoodu. Ani tento druh lechtivé zábavy samozřejmě neuniká pozornosti pirátů. Filmoví producenti však nemohou v tomto ohledu dělat nic, protože pirátství video-pornografie není považováno za zločin. Ochrana proti kopírování zde neexistuje a zdá se, že pirátství porna nikoho tolik netrápí.

- ✓ *Ostatní*

Cílem pirátů bývá často vydávání všemožných aplikací a počítačového softwaru nebo aplikací pro chytré telefony. Piráti se zaměřují nejčastěji na složité vědecké aplikace, se kterými umí pracovat jen málo lidí a aplikace které běžně stojí mnoho peněz, a tudíž jsou i většině lidí nedostupné. Dalším titulem a cílem pirátských skupin je tzv. Learningware, který slouží k učebním a studijním účelům, například encyklopedie nebo příručky. Postupy používané na pirátské scéně se dají použít prakticky na všechno. (Craig, Honick, 2008)

HACKING

Dalším problémem, který se navíc z globálního hlediska počítačové kriminality jeví jako jeden z nejstarších protiprávních jednání, je hacking. Mnoho počítačových nadšenců využívá své znalosti k hackování her. To znamená, že na internetu hledají způsob jak s použití cheatů obelstít své počítačové hry. Ačkoliv se pro hackování počítačů používá stejný výraz, jedná se zde o něco naprosto odlišného. Zatímco hackování her se nese v duchu nesportovního chování a ulehčování si herního postupu, hackování počítače znamená trestný čin.

Kdo je hacker?

Obecně můžeme říci, že hacker je osoba, která bez povolení pronikne do nějakého počítačového systému či sítě, nebo osobních dat jiné osoby. Jeho činnost se dá nazvat hackingem. Některé programátorské skupiny o sobě tvrdí že jsou hackeři a zároveň tvrdí, že hackování není nic jiného než extrémně chytrý způsob programování. Široká veřejnost považuje hackery za zločince a vandaly. Zprvu většina hackerů pocházela ze spolků chytrých studentů informatiky a počítačových nadšenců. Takové studenty často charakterizuje samota a touha po slávě.
(Mc Carthy, Weldon – Siviy, 2013)

Typy hackerů podle časové náročnosti hackování

Naučit se Hackovat je náročné a samotné hackerské útoky trvají poměrně dlouhou dobu. Vzhledem k času, který hackování zabírá, a zvyšující se nebezpečnosti dělíme hackery do těchto kategorií:

- ✓ *Odborníci na zabezpečení*

Umí hackovat, ale z morálních či ekonomických důvodů tuto činnost neprovozují. Veškerými opatřeními proti hackování se dá utržit mnohem více peněz než jeho provozováním. Proto střední a větší společností zaměstnávají hackery k testování svých systému zabezpečení. Stovky hackerů nyní pracují u velkých firem.

- ✓ *Script kiddies*

Představují skupinu nezkušených hackerů – jsou to například studenti, kteří studují druhý stupeň základní školy, střední či vysokou školu. Finančně jsou podporovány rodiči, a pokud pracují, pak jen na částečný úvazek. Tyto hackeři využívají k provádění útoku vlastní počítače nebo (univerzitní) rozsáhlejší zdroje, které umožňuje škola. Bezstarostně se pohybují kybernetickým prostorem a pátrají po možných cílech. Většina chce pouze oslnit své vrstevníky a nebýt chycena při činu. Obvykle člověk jejich činnost nepostřehne, pokud ovšem nevlastní programy na varování nebo firewall, který zaznamená útoky do kontrolních záznamů. Tito hackeři se účastní na 90% hackerské činnosti. Tato skupina hackuje hlavně proto, aby si obstarali něco zadarmo, např. programy a hudbu. Vyměňují si mezi sebou pirátský software, z CD vyrábějí zvukové nahrávky v komprimovaných souborech MP3 a vyměňují si sériová čísla důležitá pro odblokování plné funkčnosti demo verzí softwaru, který mohou stáhnout na Internetu.

- ✓ *Dospělý hackeři bez práce*

Sem patří sem studenti, kteří byli vyhozeni ze školy nebo dospělý hackeři, kteří přišli nezaměstnaní nebo z nějakých důvodů nemohou sehnat zaměstnání na plný úvazek. Obvykle jim peníze stačí akorát tak na nájem. Pravděpodobně je hackování jejich koníčkem a v tomto oboru jsou opravdu dobří. Nejsou to zločinci, protože jejich

úmyslem není zničit ostatní, ale většina z nich jsou piráti (softwaroví nebo mediální). Tato skupina také vytváří většinu programových virů.

- ✓ *Ideologičtí hackeři*

Tato skupina hackuje, aby podpořila nějaký politický cíl. Obvykle znehodnocují stránky svých ideologických odpůrců nebo proti nim směrují útoky s důsledkem odepření služby. Pro své útoky využívají pozornosti médií, a protože většinou přicházejí z cizích zemí, často využívají tiché podpory ze strany vlády a nelze je na základě místních zákonů stíhat. (Stebe, Perkins, 2003)

- ✓ *Kriminální hackeři*

Jejich motivací je zisk za každou cenu. Napadají servery na internetu, aby ukradly čísla kreditních karet a převedly z banky peníze. Do této skupiny můžeme zahrnout i hackery najímané s cílem provádět průmyslovou či obchodní špionáž. (Jirovský, 2011)

- ✓ Nespokojení zaměstnanci

Pro firmu představují velké bezpečnostní riziko. Veřejně rozšiřují vnitrofiremní záležitosti, kradou a prodávají firemní tajemství a jinak nelegálně nakládají s vybavením nebo daty firmy. (Stebe, Perkins, 2003)

Typy hackerů podle charakteru činnosti

Co se týče bezpečnosti, můžeme rozdělit hackery na 3 hlavní skupiny. První skupinou jsou ti hodní (White hats), druhou skupinou jsou zločinci (Black hats) a do třetí skupiny (Grey hats) spadají jedinci pohybující se na pomezí mezi oběma póly. Odlišit tyto skupiny, tedy hlavně třetí skupinu od ostatních nebývá často jednoduché.

- ✓ White hats

„Bílé klobouky" je označení pro bezpečnostní experty, kteří používají stejné techniky jako Černé klobouky, ale na rozdíl od nich se záměrem odhalovat padouchy pomocí využití bezpečnostních nástrojů k objevování bezpečnostních děr a k testování

a zlepšování bezpečnosti. Takové činnosti nazýváme etické hackování. Používají se pro shromažďování důkazů, které jsou potřeba k odhalování a usvědčení počítačových zločinců. Tento proces se nazývá forenzní informatika.

- ✓ *„Black hats“*

Černé klobouky jsou zločinci. Jsou to lidé, kteří páchají elektronické zločiny. Mezi ně patří například krádež osobních dat, vyřazení sítě z provozu, pronikání do počítačových systémů a rozesíláním virů a červů.

- ✓ *„Gray hats“*

Někde mezi bílými a černými klobouky stojí šedé klobouky. Tito hackeři někdy pronikají do systému společnosti jen pro to, aby zjistili jeho obsah. Nijak systém neporuší a ospravedlňují se tím, že pokud nepoškodí žádný soubor, nepáchají trestný čin. Často si po útoku zažádají o místo, jako jsou bezpečnostní technici a konzultanti a jejich omluvy pro předešlé útoky bývají ty, že pokud se nabourají do systému firmy, u které pracují, jenom tím trénují a zdokonalují se ve své práci. Navíc mnohdy informují společnost o jejich slabých stránkách a bezpečnostních rizikách, které hrozí jejich počítačům. (Mc Carthy, Weldon – Siviy, 2013)

Nástroje hackerů

Žádný hacker nepoužívá ke své činnosti pouze znalosti a dovednosti, ale využívá jisté nástroje, většinou ve formě programů, které jim danou činnost usnadní. Dnes se dají nástroje pro hackování volně stáhnout na internetu. Stačí ve vyhledávači na internetu zadat hledat výraz: „free hacker tools“ a mezi výsledky s trochou trpělivosti najít ty správné nástroje. Proto, aby s nimi byly problémy, je jich na internetu ke stažení dostatek a jejich počet neustále roste. Pokud jsou tyto nástroje testovány například na hodině informatiky ve škole pod dohledem, je to v pořádku, ale je důležité mít na paměti, že hackování počítačů jako takové, je nezákonné.

- ✓ *Skenovací nástroje*

Pomocí skenovacích nástrojů hacker prohledává počítač připojený k internetu a hledá zranitelná místa. Zjišťuje, jak jsou ve vašem počítači chráněny body připojení k internetu, zda máte v počítači nainstalované aktualizace eliminující negativní dopady bezpečnostních děr operačního systému, nebo kontroluje jeho firewall a do jaké míry je počítač chráněn před útoky všeho druhu. Tyto skenovací nástroje nepoužívají pouze Bíle klobouky. Testovat zabezpečení systému může i běžný uživatel PC, stačí vyzkoušet jeden z bezplatných skenovacích nástrojů, jako je například volně dostupný program Shield UP od společnosti Gibson Research Company.

- ✓ *Prolamování hesel*

Mezi základní výbavu hackera patří nástroje na prolamování hesel. Tyto programy nejsou na poli počítačové kriminality žádnou novinkou. Fakt, že dokáží celkem efektivně prolomit většinu uživatelských hesel, je částečně způsoben tím, že většina uživatelů nevyvine při tvorbě hesla téměř žádné úsilí. Při prolamování hesla se hacker spoléhá v první řadě na jednoduché hádání. Většina uživatelů používá pro svůj účet jednoduchá hesla, například jména svá, dětí, dalších členů rodiny nebo svých domácích mazlíčků. Hackeři, kteří prolamují hesla, pak mohou nahrát celý slovník, nebo obsah knihy s dětskými jmény a tím mohou odhalit spoustu hesel. Skupina slabých hesel zahrnuje obvykle také čísla v běžném formátu, jako jsou telefonní čísla nebo čísla životního pojištění. Spousta uživatelů si běžně nastaví stejné uživatelské jméno a heslo pro všechny své účty. Tím pádem ulehčí hackerům spoustu práce a po odhalení jediného hesla pak mají přístup ke všem ostatním účtům.

- ✓ *Rootkit*

Hlavním cílem hackerů je získat absolutní kontrolu nad systémem, navíc tak, aby si toho pokud možno nikdo nevšiml. Souborem nástrojů, pomocí kterých hacker získá plný přístup k nezabezpečenému počítači a následně za sebou zamete stopy, je tzv. Rootkit. Hlavními dvěma cíli hackerů, kvůli kterým rootkity používají,

jsou tedy získání přístupu k počítačové síti nebo počítači a následně zamaskování faktu, že tyto sítě nebo počítače byly zneužity. Rootkity mohou deaktivovat bezpečnostní programy, mohou se skrývat za jinými programy, které v systému běží. Nejčastěji se rootkit dostane do počítače skrze nějakou bezpečnostní díru v systému, nebo pomocí virů. (Mc Carthy, Weldon – Siviy, 2013)

Techniky hackování

Mezi dovednosti hackera patří i jisté techniky hackování, pomocí kterých hacker dosahuje svých cílů, ať už jsou jakékoliv. K těm nejčastějším, podle jednoduchosti hackování, patří:

- ✓ *Odposlech a špehování*

Nejčastější metodou, jak se může hacker nabourat do sítě, je odposlouchávání síťového provozu. Je to i ta nejjednodušší metoda, neboť počítače, které jsou připojené v síti, tak jak jsou od dodavatele operačního systému nastavené ve své původní konfiguraci, poskytují doslova otevřené dveře ke svému obsahu. Hacker může komunikovat s počítačem nepřímo, skrze další počítače, na jejichž služby se počítač spoléhá. To jsou například počítače, poskytující na internetu službu DNS (Domain Name Service).

- ✓ *Odepření služby*

Dalším způsobem jak zaútočit na síť, je zakázat počítači přístup k síti nebo k některým jejím službám. Většina hackerů útočí na počítače pomocí protokolu TCP/IP, jakožto nejrozšířenějšího protokolu pro tvorbu sítí. Počítač v síti je přinucen, aby o sobě prozradil dostatečné množství informací pro jeho prolomení.

- ✓ *Zneužívání protokolů*

Cílem útoku je napadení chyby ve veřejné službě na internetu a tím získat větší přístup, než by bylo obvykle možné. Nejčastějším typem zneužití protokolu je tzv. přetečení vyrovnávací paměti. Za běžných okolností dojde k selhání programu, potažmo zcizení nebo ztrátě dat z počítače.

- ✓ *Převzetí totožnosti*

Když hacker doposud nezískal přístup k počítači, může se pokusit převzít totožnost jiného počítače, který je také připojen k síti a tím se dostat k informacím které chce. Prostřednictvím převzetí totožnosti jiného počítače oklame počítač a napadený počítač pak vyzradí informace, s jejichž použitím se dostane přes zabezpečení sítě. Tento způsob získávání informací je oproti předešlým složitější a intenzita útoků nižší než při útoku skrze zneužití protokolu. Hackeři tento způsob volí tehdy, když mají v plánu zaútočit na konkrétní počítač.

- ✓ *Prostředník*

Útok z pozice prostředníka je jedním z druhů převzetí totožnosti jiného počítače. Jako příklad si představme běžné uživatele počítače, kteří si myslí, že komunikují se serverem, server, který si myslí, že komunikuje s uživateli a hackera, který skrze svůj počítač sleduje a pozměňuje všechnu komunikaci která mezi uživateli a serverem probíhá. Proti útokům skrze prostředníka je obtížné se bránit, avšak provést samotný útok, tak aby byl úspěšný, není nikterak jednodušší.

- ✓ *Zcizení spojení (únos spojení)*

V tomto případě dochází ke zcizení již ustaveného spojení. Hacker opět provádí útoky ve vrstvách síťového protokolu a tak se naboural do sdíleného připojení sítě. Složitost závisí na míře zabezpečení serveru, který by na internetu zbytečně neměl vystavovat některé své relace. (Stebe, Perkins, 2003)

ŠKODLIVÝ SOFTWARE

Výše byl popsán celosvětový problém hackingu, při kterém hackeři používají různé programy k dosažení svých cílů, potažmo k protiprávnímu jednání. Používání těchto nástrojů pro hacking se velmi často prolíná i s používáním dalšího, škodlivého softwaru.

V internetovém kyberprostoru nachází spousta škůdců, tedy programů, které se dají souhrnně pojmenovat jako „malware“ – z anglického „malicious software“ neboli

„škodlivý software“. Potencionálně nechtěné programy (PUP – Potentially Unwanted Programs) útočí na počítačové systémy a sbírají data v nich uložená. Bez našeho vědomí kradou informace uložené v počítači a odesílají je zainteresované straně, nebo tyto informace ukládají do určitých souborů pro pozdější užití. Často se objevují případy, kdy jsou tyto informace použity třetí stranou k cílené reklamě. Tedy jedním důvodem tohoto počínání může být snaha jak uživatelům napadeného počítače něco prodat. Dalším důvodem bývá zneužití identity tohoto uživatele k ovládnutí jeho počítače. Nejběžnějšími typy těchto programů, které sbírají osobní informace a odesílají je třetí straně, jsou tzv. Adware a Spyware.

- ✓ *Spyware*

Primárním účelem spywaru je špehování uživatele PC. Paul Craig, (2008) uvádí výraz „data miner“ (jakýsi „důl na informace“), kterým se spyware často označuje. Na rozdíl od virů červů se sám nereplikuje, avšak často se do počítače dostane skrze škodlivé nebo poškozené webové stránky, nainstaluje se a běží na pozadí, často aniž by si toho uživatel vůbec všiml. Je to škodlivý software, který sbírá informace o uživateli, jaké stránky navštěvuje, co dělá, to vše bez uživatelova vědomí. Informace, které spyware nasbírá, pak odesílá zainteresované straně. Spyware umí sbírat a odesílat osobní informace, kterými můžou být mimo soukromých zpráv i uživatelská jména nebo hesla k bankovním účtům. Spyware se může nacházet prakticky na jakékoliv typu webové stránky, proto je nutné tento druh malware odstraňovat. Vyjma zmíněného typu spywaru, o kterém uživatel napadeného počítače netuší, pravděpodobně existují i takové typy, které si uživatel do svého osobního počítače nebo smartphonu přizve sám, aniž by si byl vědom, že se o spyware může jednat.

S tímto druhem škodlivého programu, jakožto nástroje pro „špehování“ souvisí i jistá fakta týkající se sociální sítě Facebook. Na webových stránkách (www.ibnlive.in.com) je zveřejněno vyjádření amerického bezpečnostního internetového specialisty Jonathana Zdziarski, který tvrdí, že nová aplikace Facebook Messenger, která byla stažena již více než 500 milionkrát na různých

zařízeních s operačním systémem Android, může obsahovat spyware, který dohlíží na zprávy v chatu a ostatní informace sdílené pomocí této aplikace. Konstrukce aplikace podle jeho slov obsahuje velmi mnoho zdrojového kódu, který naznačuje že Facebook analyzuje nejen zprávy zaslané pomocí chatu, ale prakticky vše co je možné na uživatelově zařízení sledovat.

Od 1. ledna 2015 na Facebooku platí nová pravidla a podmínky týkající se soukromí, užívání a inzerce. Má to však háček, v těchto podmínkách je zdánlivě účelně vynecháno to nejpodstatnější, navíc nové provedení efektivně znemožňuje porovnat původní a nová pravidla. Facebook shromažďuje o jeho uživatelích mnoho informací, které souvisejí s jeho používáním. Tyto informace pak Facebook používá, k čemu uzná za vhodné, bez ohledu na názor jeho uživatelů. Může uživatele manipulovat poskytováním zkreslených informací v newsfeedu. Na druhé straně uživatele přesvědčuje, že je to pro jejich dobro, a aby mohl dodávat lepší služby. Shromážděné informace slouží také k cílení reklamy a marketingovým nabídkám. V pravidlech Facebooku je doslovně uvedeno, že předají informace o uživatelích na základě právních žádostí, pokud jednají v dobré víře, že je nutné na dotaz odpovědět. Pro případ, že by o jakémkoliv uživateli bylo potřeba něco zjistit i v budoucnu, ponechává si Facebook zablokované účty v databázi minimálně rok. Jediným způsobem, jak se vyhnout novým podmínkám je, že uživatel přestane svůj profil používat. To ale Facebooku nezabrání, aby vytvořil stínový profil uživatele a do nekonečna shromažďoval jeho informace. Stále bude získávat informace od jeho přátel i cizích lidí, a nezáleží na tom, jestli to budou adresáře, fotografie či zprávy. Z toho všeho vyplívá, že čím více informací se shromažďuje, tím větší je i možnost úniku těchto informací, stejně jako možnost jejich zneužití. (www.lupa.cz)

- ✓ *Adware*

Mnoho lidí často spojuje spyware a adware jako by šlo o totéž. Adware, na rozdíl od spywaru, je typ programu který do webového prohlížeče přidává cílený reklamní obsah. Děje se tak na základě shromažďování informací o tom, co uživatel na internetu dělá a jaké navštěvuje stránky. Inzerenti zde používají metodu behaviorálního zacílení, což je zacílení podle chování uživatele. Na základě online

aktivit uživatele pak směřují reklamy na spotřebitele, u kterých je nejvyšší pravděpodobnost, že si daný produkt koupí. Většina adwaru však operuje v mezích zákona, protože od uživatelů vyžaduje souhlas k instalaci programu. Stejně tak jako některé stránky umožňují stáhnout si bezplatný program, v případě že si spolu s ním uživatel přijme i adware. Také se však stává, že se adware dostane do počítače bez uživatelova vědomí, například může být obsažen v balíčku bezplatných nástrojů, jako jsou spořiče obrazovky, nebo se stáhne, když uživatel navštíví škodlivou webovou stránku.

- ✓ *Keyloggery*

Nedílnou součástí některých adwarových a spywarových programů jsou i tzv. keyloggery (key = klávesa, logger =záznamník). Na druhou stranu se některé keyloggery instalují samostatně, jako programy pro rodičovský nebo zaměstnanecký dohled. Jsou to programy, které zaznamenávají každý úhoz klávesy při psaní na počítači. I zde existuje mnoho rizik, například pro uživatele sociálních sítí, zejména Facebooku, stejně tak jako uživatele internetového bankovnictví, který na klávesnici zadává své číslo a heslo bankovního účtu, podobně jako riziko zcizení osobních údajů, posílá-li uživatel po síti například životopis nebo žádost o platební kartu.

- ✓ *Viry*

Podobným způsobem jako například spyware, tedy většinou bez vědomí uživatele, se do počítače dostávají i viry. Jsou to škodlivé programové kódy, které mají na počítač spoustu negativních účinků. Mezi ty nejčastější patří vypínání počítače, změna nebo smazání souborů na pevném disku. Virová nákaza se šíří specifickým způsobem. Nejčastěji se do počítače dostane skrze stažený software, nebo přílohu e- mailu. Většina virů je tvořena tak, aby se dokázaly samy zkopírovat a automaticky se šířit z jednoho počítače na druhý.

- ✓ *Falešné antivirové programy*

Část uživatelů se před nákazou počítače virem chrání pomocí antivirových programů, které se snaží viry eliminovat, nebo upozornit uživatele na možnou hrozbu. Vedle pravých antivirových programů existují na internetu i falešné antivirové programy. Tyto programy jsou často nazývány jako tzv. „scareware“. Jsou to aplikace, které pomocí neetických marketingových praktik svádí uživatele k tomu, aby si stáhl a zaplatil škodlivý nebo bezcenný program, který se přitom tváří jako bezpečnostní počítačový program. Nejčastěji tyto programy operují tím způsobem, že na počítači zobrazí poplašnou zprávu, která uživateli oznamuje, že je jeho systém infikován spywarem. Tyto zprávy mívají často velice podobný formát jako upozornění od pravých antivirů. Vyjímkou nejsou ani názvy, stejná loga a styly vyskakovacích oken, jako používají např. Microsoft Windows pro ohlášení reálných hrozeb. Cílem podvodníka je pak prodat uživateli program pro odstranění „hrozeb“ na jeho počítači. Neznalý uživatel tak pouze nainstaluje jiný, nový spyware a obvykle mu zůstane počítač, který nemůže dále používat.
(Mc Carthy, Weldon – Siviy, 2013)

SPAMMING

Dalším zásadním druhem počítačové kriminality, který zasahuje do každodenního života obrovského množství uživatelů internetu, e-mailu, je spam. E-mail, potažmo internet, umožňuje velmi jednoduchou, rychlou, a levnou komunikaci. Není potřeba zasílat velké množství dopisů a platit za poštovní známky. Díky tomu vznikl spam.

- ✓ *Spam*

Názory na to, jak přesně definovat spam jsou různé. Martin Adámek (2009) ve své knize uvádí, že Spamem se obecně rozumí nežádoucí pošta reklamně-komerčního, potažmo obchodního sdělení nebo jiná nevyžádaná zpráva, která je hromadně rozesílána více příjemcům, kteří si tuto poštu nevyžádali a nemají možnost si odběr těchto zpráv zrušit. Některé tyto zprávy například obsahují nabídku nelegálního software, nebo dokonce nabídku univerzitního diplomu. Obvykle jsou zahraničního původu, čemuž odpovídá i jazyk, ve kterém jsou psány.

- ✓ *Reklama*

Obsahem většiny nevyžádané pošty je reklama a propagace různých produktů. Za spam se ovšem nedají považovat zprávy, zasílané zpravidla českými firmami, které jsou většinou odesílány jednorázově, navíc často v důsledku vyžádaného odběru informací. Na rozdíl od spamu jako takového, obsahují možnost odběr dalších zpráv zrušit.

- ✓ *Viry a trojské koně*

Dalším druhem spamu jsou emaily obsahující viry nebo trojské koně. Tyto spamy se snaží napadnout počítač. Na rozdíl od běžného spamu, kdy je jeho účelem vylákat z adresáta peníze nebo mu prodat svůj produkt, rozesílání zavirovaných e mailů může mít více důvodů. Běžným účelem těchto spamů bývá převzetí kontroly nad počítačem, který pak automaticky dále rozesílá spam na další adresy. Tím častějším důvodem bývá získávání citlivých údajů. Když adresát otevře takovou zprávu, nainstaluje si škodlivý program, který sleduje, co uživatel dělá, jaké navštěvuje stránky a jaká na nich zadává hesla. To může být problém, obzvláště pokud se jedná o hesla pro přístup do bankovních aplikací, pomocí kterých se dají zadávat platební příkazy.

- ✓ *Podvodné emaily - Phishing*

Činnost, kterou vystihuje nachytání uživatele na falešné emailové zprávy, se nazývá „phishing“, z anglického slova „fishing“ – rybaření. Podvodníci zde však neloví ryby, ale informace, či finanční údaje o uživateli. Falešná e-mailová zpráva vypadá jako by byla zaslána společností, se kterou uživatel spolupracuje, zná ji a věří ji. Předmětem zpráv bývá sdělení o problému s účtem, o jeho nezákonném použití a paradoxně i žádosti o ověření informací z důvodu zlepšení ochrany účtu uživatele. Nepozorný uživatel se může snadno nechat oklamat a sdělit tak podvodníkovi informace které chtěl znát. (Mc Carthy, Weldon – Siviy, 2013)

3.3.2 Úvod do právní úpravy

Několik předchozích dekád na našem území platil původní zákon č. 40/1964 Sb. Ten se však nezabýval počítačovou kriminalitou tak podrobně jako jeho nástupce. Nový trestní zákoník, konkrétně zákon č. 40/2009 Sb., vychází z Úmluvy o počítačové kriminalitě. Ta byla schválena Výborem ministrů Rady Evropy a Česká republika ji podepsala v roce 2005. Po o 8 letech, tj. v roce 2013, ČR tuto úmluvu ratifikovala a zařadila se mezi 40 zemí, pro které je Úmluva závazná. Jedním z pravděpodobných důvodů, proč došlo k ratifikaci po tak dlouhé době, může být fakt, že teprve v roce 2012 u nás byla zavedena povinnost stíhat za zakázaná jednání i právnické osoby.

Členské státy jsou povinny stíhat i veškeré úmyslné formy účasti a trestné činy ve fázi pokusu. Úmluva dále upravuje například zásady právní pomoci, prozatímních opatření a vyšetřovacích organizací. Každý členský stát je také povinen provozovat určené kontaktní místo, u nás je to Policejní prezidium. (www.pravniradce.ihned.cz)

3.3.3 Právní úprava vybraných forem počítačové kriminality

Softwarové pirátství

Každý kdo užívá počítač, užívá zároveň i software. Autor softwaru má stejně jako autor čehokoliv jiného nárok na odměnu. Práva autorů softwaru v ČR popisuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). Kromě autorského zákona uživatel nelegálního softwaru porušuje i mnoho jiných práv. Za porušení autorského práva v organizaci je odpovědný ten, kdo úmyslně toto právo porušil, například věděl, že jde o nelegální kopii softwaru a přesto ji užíval, nebo neoprávněně instaloval nelegální kopii či zkopíroval počítačový program. Ten, kdo nelegální užívání softwaru organizoval, naváděl k němu a poskytoval k němu pomoc, je účastníkem na tomto trestném činu a hrozí mu stejný trest jako hlavnímu pachateli. Následky nakládání s nelegálním softwarem jsou přímo závislé na rozsahu porušení daného zákona. Zahrnují zejména peněžitý trest, trest odnětí

svobody na dobu až 8 let a další postihy, například od finančního úřadu a podobně. (www.microsoft.com)

Hacking

Český trestní zákon v současnosti neobsahuje skutkovou podstatu žádného trestného činu, která by hovořila přímo o „hackování“. Takové jednání se nejčastěji posuzuje podle § 257a tr. zákona, kde je pojmenováno jako „Poškození a zneužití záznamu na nosiči informací“. Podle tohoto ustanovení platí, že potrestán bude ten, kdo jakýmkoliv způsobem získá přístup k nosiči informací (harddisk, USB flash disk apod.) a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch tyto informace neoprávněně užije, zničí, poškodí, změní nebo učiní nepotřebnými, nebo učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení.

V takovém případě hrozí pachateli trest odnětí svobody až na jeden rok, nebo zákaz činnosti, který je možný uložit až na 10 let, nebo peněžitý trest až do výše 5 milionů, nebo trest propadnutí věci, kterou ke spáchání použil nebo propadnutí jiné majetkové hodnoty. (www.zakony.kurzy.cz)

Spamming

Nejprve je důležité uvést, co může být za určitých okolností obchodním sdělením. Zákon č. 482/2004 Sb. o některých službách informační společnosti (dále jen „ZNS“) upravuje šíření obchodních sdělení elektronickými prostředky. Takové šíření zakazuje, pokud šiřitel nemá jasný a výslovný souhlas adresáta. Souhlas musí být kdykoliv prokazatelný. Obchodní sdělení pak musí obsahovat zřetelnou možnost jednoduchým způsobem a zdarma, nebo na účet odesílatele další zaslání odmítnout. Veškerá obchodní sdělení musí být jasně označena jako obchodní sdělení, nesmí skrývat totožnost odesílatele a také musí obsahovat platnou adresu, na kterou může adresát případně zaslat nesouhlas s dalším zasíláním obchodního sdělení. Od 1. 1. 2012 byla definice samotného obchodního sdělení upravena podle zákonu č. 468/2011 Sb. tak, že obchodním sdělením se rozumí všechny formy sdělení včetně reklamy a vybízení k návštěvě internetových stránek, určeného k přímé

či nepřímé podpoře zboží či služeb nebo image podniku osoby, která je podnikatelem nebo vykonává regulovanou činnost. Pojem „sdělení“ je dle Směrnice o soukromí a elektronických komunikacích definováno jako jakákoliv informace, která se vyměňuje nebo přenáší mezi určitým počtem zúčastněných stran prostřednictvím veřejně dostupné služby elektronických komunikací.

Právní úprava vedle e-mailů, které obsahují pouze klasickou nabídku, zakazuje také zasílání e-mailů obsahujících pouhé odkazy na webové stránky bez dalšího textu. Pro podřazení jednání pod ZNS je nutné vědět, že zde musí být splněna podmínka obchodního charakteru sdělení. Jinými slovy, musí buď přímo nebo nepřímo podporovat nabídku zboží či služeb podnikatelského subjektu. Druhou nutnou podmínkou je zaslání sdělení elektronickými prostředky. Podle sankčního ustanovení ZNS je rozsah pokuty za porušení zákona pro fyzickou osobu stanoven do 10 000,- Kč, a pro právnickou osobu je to až 10 mil. Kč. (www.pravoit.cz)

3.3.4 Organizace zabývající se počítačovou kriminalitou

Jak je uvedeno výše, existuje jistý právní řád, upravující činnosti týkající se počítačové kriminality. Vedle toho, u nás i ve světě působí určité společnosti, které se zabývají počítačovou kriminalitou. Boj proti počítačové kriminalitě, se v mnohém neliší od boje proti běžným formám trestné činnosti. Z toho vyplívá, že tento boj by nebyl efektivní, kdyby nebyly uplatněny obě jeho hlavní složky, jimiž jsou prevence a represe. V rámci počítačové kriminality panuje mezi odbornou veřejností názor, že právě prevence zde má vůdčí postavení. Velmi důležitým opatřením, pozitivně působícím proti počítačové kriminalitě je psychologická prevence, například v podobě utváření povědomí o nemorálnosti a společenské nepřijatelnosti protiprávních činů týkajících se tohoto druhu kriminality.

V České republice působí také různá zájmová sdružení či organizace, zabývající se bojem proti počítačové kriminalitě, buď v rámci prevence, pomocí různých kampaní a sloganů, jejichž cílem je odradit od páchání protiprávní činnosti,

nebo pomocí analýzy informací o počítačové kriminalitě a následném odhalování a postihování trestné činnosti.

Bussiness Software Alliance

Tato instituce byla založena v roce 1988 a působí ve více než 80 zemích světa, včetně ČR. Sdružuje také důležité výrobce softwaru. Mezi nejdůležitější patří například Microsoft, Adobe Systems, Autodesk. BSA je známá především svými „protipirátskými" aktivitami a kampaněmi zaměřenými na vzdělávání veřejnosti v oblasti správy softwaru a ochrany autorských práv. Prostřednictvím webových stránek BSA má kdokoliv možnost podat anonymní oznámení o porušení autorských práv, což je předním účelem těchto stránek. (ww2.bsa.org)

Česká protipirátská unie

Česká protipirátská unie byla založena v roce 1992 a jejím účelem je ochrana autorského práva k audiovizuálním dílům a ostatních práv souvisejících s právem autorským. ČPU se dále věnuje sledování a analýze informací, které se týkají autorských práv, právních kroků proti jejich porušování, spolupráci s orgány činnými v trestním řízení a ostatními orgány a spolupráci na přípravě nových právních předpisů. ČPU též sdružuje různé video distributory a poskytovatele kabelového a televizního vysílání. Na její činnosti se podílí také protipirátské oddělení mezinárodní organizace Motion Pictures Association. (www.cpufilm.cz)

Policie ČR

Tomáš Gřivna (2008) ve své knize uvádí, jak u Ředitelství služby kriminální policie kriminálního úřadu Policejního prezidia od roku 1999 začala působit tzv. Skupina informační kriminality. Toto pracoviště se zabývá jednak odhalováním a vyšetřováním kriminality týkající se duševního vlastnictví, respektive oblasti informačních technologií a jednak odhalováním a vyšetřováním trestné činnosti na internetu. Od května 2005 byl při úřadu služby kriminální policie a Policejního prezidia ČR zřízen Odbor informační kriminality, jako specializované pracoviště pro vyšetřování počítačové kriminality a kriminality páchané za pomoci počítačů.

Na hlavní stránce internetových stránek PČR, www.policie.cz, lze od roku 2012 nalézt odkaz na formulář, který umožňuje nahlásit závadný obsah nebo aktivity na internetu.

4 Praktická část

Praktická část práce se zabývá nejen metodikou dotazníkového šetření, ale i jakým způsobem toto šetření probíhalo. Dále se věnuje jeho výsledkům.

4.1 Metodika

S pomocí anonymního dotazníku bylo zjištěno, jak lidé vnímají počítačovou kriminalitu ve svém okolí. Dotazníkové šetření se zaměřuje na dopad kyberprostoru na společnost. Zejména pak na její bezpečnostní standarty při pohybu v kyberprostoru a na páchání nelegálních činností související s autorským právem, filmovým, hudebním a softwarovým průmyslem. Dotazník obsahuje 15 uzavřených otázek a jeho vzor je uveden v příloze č. 1.

Při jeho realizaci bylo využito služby www.vyplnto.cz, která se specializuje na vytváření a hodnocení dotazníkových šetření.

Etapy realizace dotazníkového šetření

Přípravné období (leden – únor 2015)
V tomto období proběhlo studium dané problematiky, výběr literatury, stanovení cílů a předpokladů, příprava anonymního dotazníku.

Období sběru dat (březen 2014)
Nahrání finálního dotazníku na webovou stránku vyplnto.cz a následná analýza vyplněných anonymních dotazníků od oslovených respondentů z Univerzity Hradec Králové - Fakulty informatiky a managementu.

Období vyhodnocení a interpretace výsledků (duben 2015)
Kontrola vyplněných dotazníků, kvantitativní a kvalitativní vyhodnocení, zpracování výsledků v souladu se stanovenými cíli, ověření předpokladů.

K vyhodnocení výsledků bylo použito 70 dotazníků. Získaná data z provedeného šetření byly zaznamenány do přehledných grafů a tabulek a vyjadřovala *absolutní četnosti* ($\mathbf{n_i}$), *relativní četnosti* ($\mathbf{p_i}$) a *celkovou četnost* - $\sum$ (suma) pomocí tzv.

četnostní (frekvenční) tabulky. Výsledky byly zpracovány v tabulkovém Editoru Microsoft Excel. Pořadí tabulek a grafů je shodné s pořadím otázek v dotazníku.

4.2 Charakteristika respondentů

Dotazníkové šetření na téma počítačové kriminality bylo provedeno mezi studenty na Fakultě informatiky a managementu Univerzity Hradec Králové. K účelům šetření bylo využito online dotazníkové služby (www.vyplnto.cz). Dotazník byl rozeslán studentům Fakulty informatiky a managementu s prosbou o vyplnění. Dotazník byl zcela anonymní, bez nutnosti uvést osobní údaje. Struktura dotazníku byla tvořena čtyřmi oblastmi, do kterých bylo zařazeno několik otázek k dané problematice. Na dotazník ke dni 20. 3. 2015 odpovědělo 70 studentů.

4.3 Výsledky dotazníkového šetření a jeho analýza

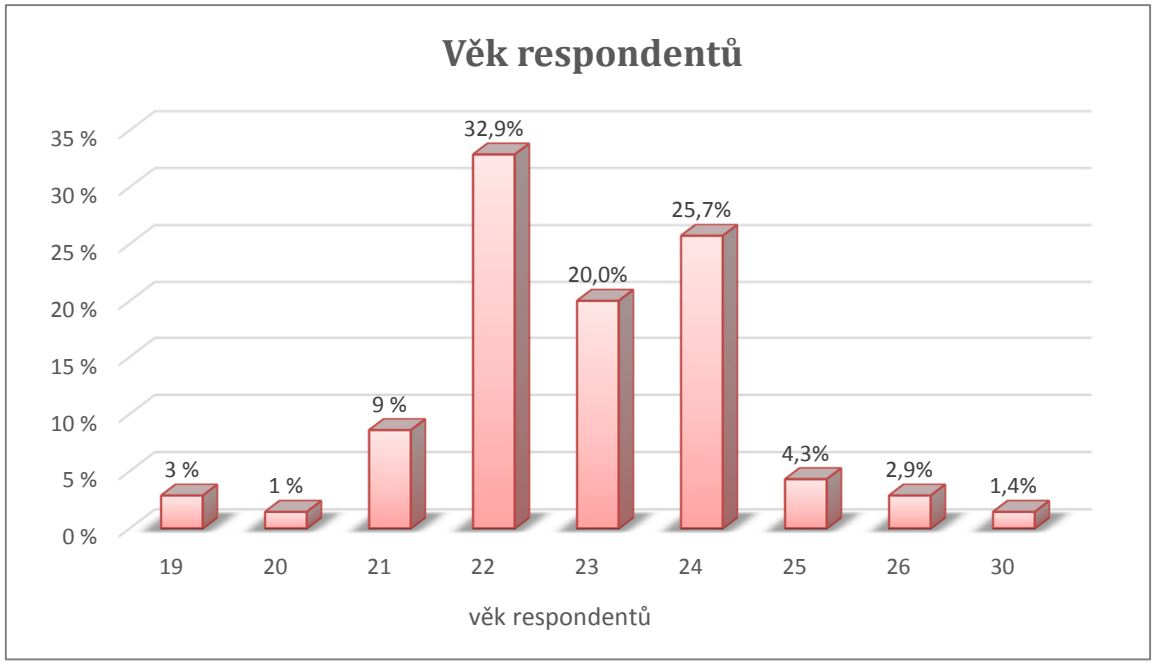
Otázka č. 1

Uveďte prosím Váš věk.

Věkového rozmezí 19 – 21 let znázorňuje 13 % dotazovaných studentů, nejčetnější věkovou skupinu 22 – 24 let tvoří 79 % respondentů a zbylých 8 % respondentů spadá do kategorie 25 – 30 let.

Odpovědi	n_i	p_i
19	2	3 %
20	1	1 %
21	6	9 %
22	23	33 %
23	14	20 %
24	18	26 %
25	3	4 %
26	2	3 %
30	1	1 %
Σ (suma)	**70**	**100 %**

Tabulka 1 Věk respondentů
Zdroj: Vlastní zpracování



Graf 1 Věk respondentů
Zdroj: Vlastní zpracování

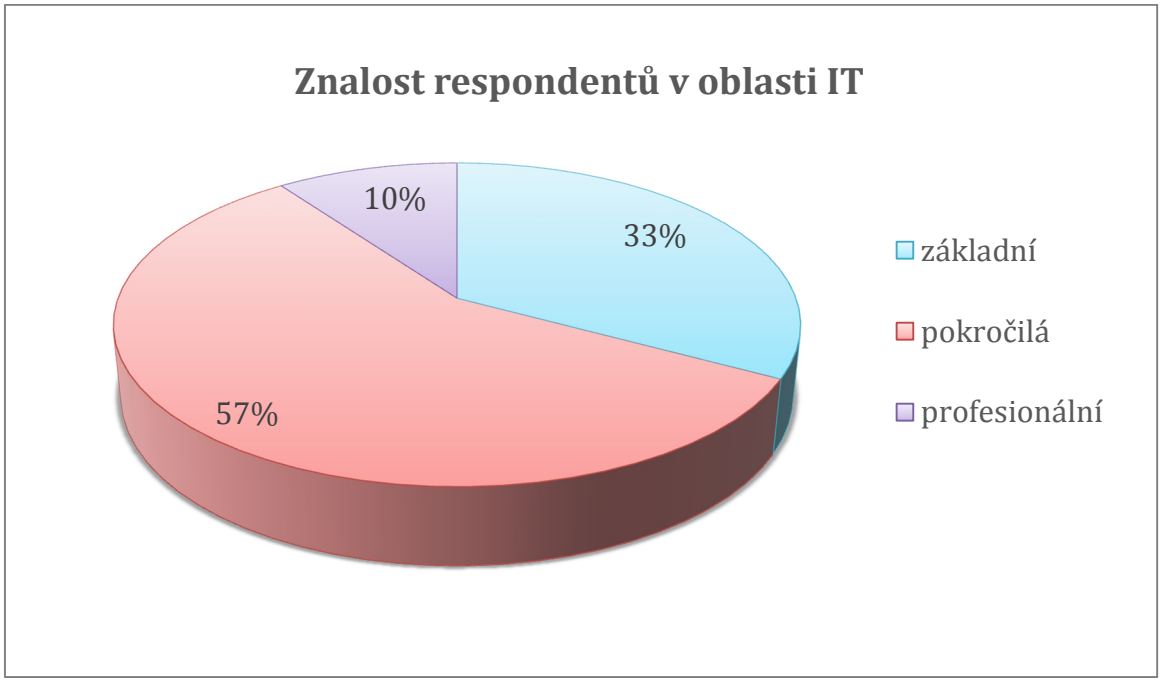
Otázka č. 2

Jaká je Vaše znalost v oblasti IT?

Více než polovina respondentů (57 %) tvoří skupinu pokročilých v oblasti IT. Dále 33% respondentu uvedlo základní znalosti a profesionální úroveň zaškrtlo 10 %.

Odpovědi	$\mathbf{n_i}$	$\mathbf{p_i}$
základní (práce s programy, Office, základní používání internetu)	23	33 %
pokročilá (reinstalace op. systému, řešení problému, základy programování)	40	57 %
profesionální (PC jako zdroj obživy, programátor, IT specialista)	7	10 %
∑ (suma)	**70**	**100 %**

Tabulka 2 Znalost respondentů v oblasti IT
Zdroj: Vlastní zpracování



Graf 2 Znalost respondentů v oblasti IT
Zdroj: Vlastní zpracování

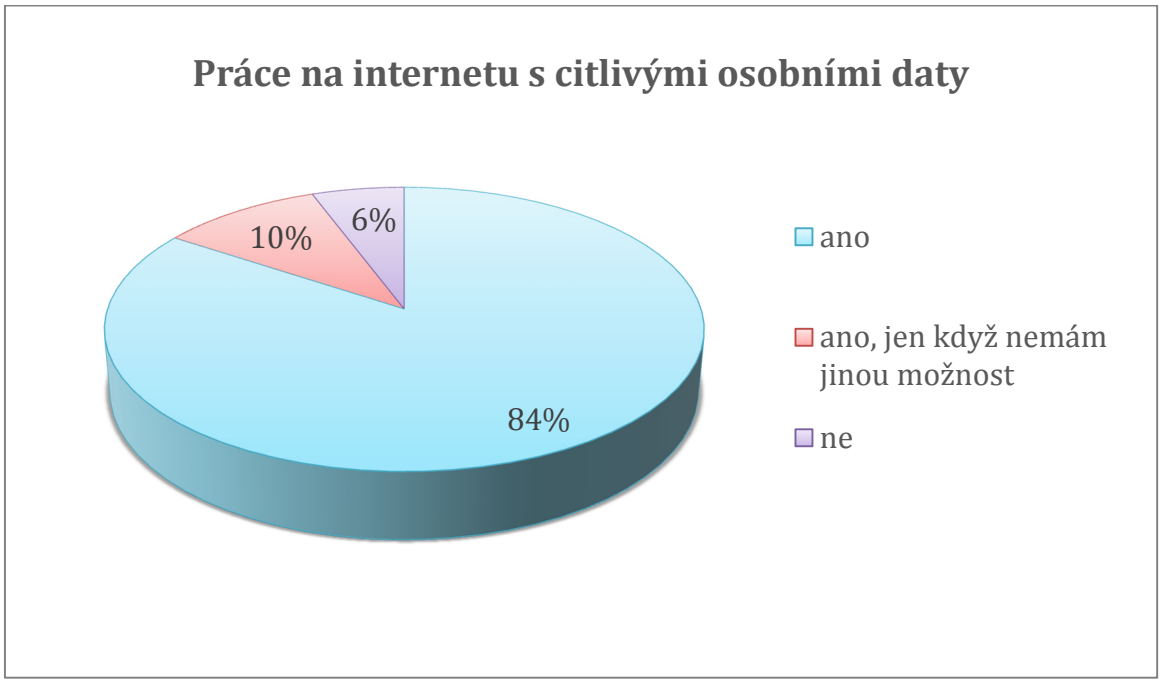
Otázka č. 3

Používáte internet pro práci s citlivými osobními daty? (internetové bankovnictví, účetnictví, atd. …)

Z dotazníkového šetření vyplývá, že 84 % respondentů používá internet pro práci s citlivými osobními daty, dále 10 % pouze tehdy, nemá-li jinou možnost. Zbylých 6 % dotazovaných internet k těmto účelům nevyužívá a volí jiné řešení.

Odpovědi	$\mathbf{n_i}$	$\mathbf{p_i}$
ano	59	84 %
ano, jen když nemám jinou možnost	7	10 %
ne	4	6 %
∑ (suma)	**70**	**100 %**

Tabulka 3 Práce na internetu s citlivými osobními daty
Zdroj: Vlastní zpracování



Graf 3 Práce na internetu s citlivými osobními daty
Zdroj: Vlastní zpracování

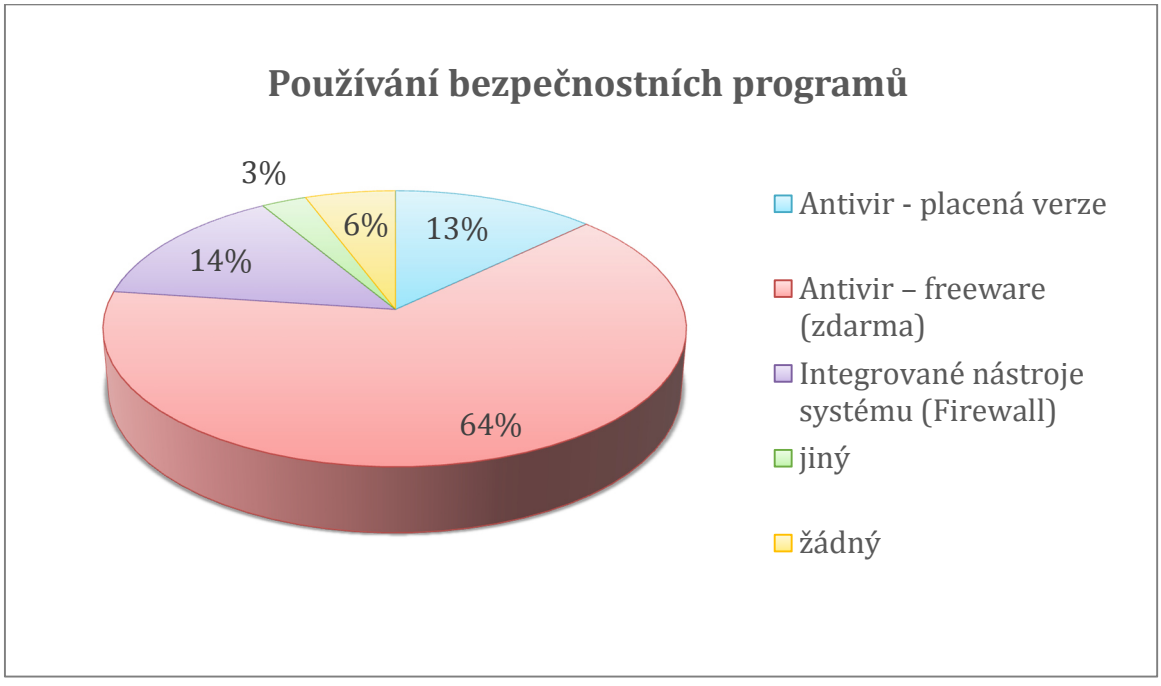
Otázka č. 4

Zaškrtněte, jaký bezpečnostní program na vašem počítači používáte.

Placenou verzi Antiviru používá pouze 13 % respondentů, ovšem Antivir – freeware (zdarma) vyžívá 64 % dotazovaných. Integrované nástroje systému jako je Firewall uplatňuje 14 %, 3 % vlastní jiný bezpečnostní program a ostatní 6 % nepoužívá žádný bezpečnostní program.

Odpovědi	$\mathbf{n_i}$	$\mathbf{p_i}$
Antivir - placená verze	9	13 %
Antivir – freeware (zdarma)	45	64 %
Integrované nástroje systému (Firewall)	10	14 %
jiný	2	3 %
žádný	4	6 %
∑ (suma)	**70**	**100 %**

Tabulka 4 Používání bezpečnostních programů
Zdroj: Vlastní zpracování



Graf 4 Používání bezpečnostních programů
Zdroj: Vlastní zpracování

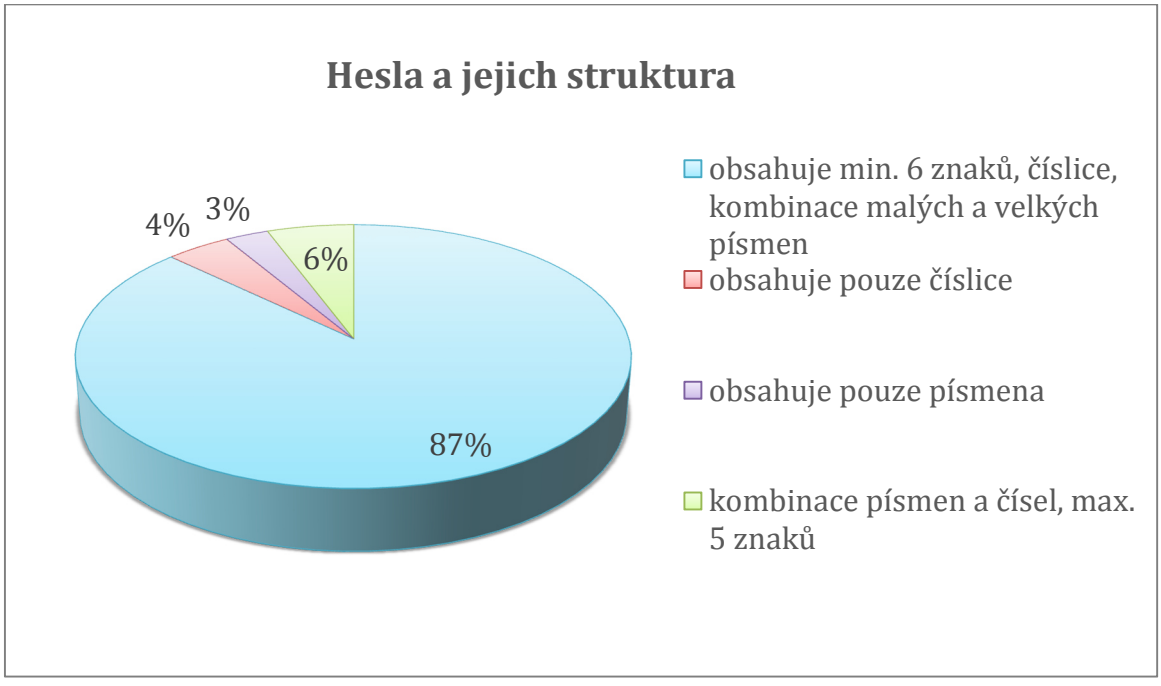
Otázka č. 5

Jak vypadá Vaše heslo, jež používáte pro přístup k Vašim citlivým údajům?

Dle výsledků z dotazníkového šetření, 87 % dotazovaných má sestavené heslo z minimálně 6 znaků, s obsahem číslic, ve střídavé kombinaci malá/velká písmena. Heslo složené pouze z číslic uvedly 4 % a pouze z písmen 3 % respondentů. Kombinace písmen a čísel s maximálně 5 znaky používá 6 % dotazovaných.

Odpovědi	**n_i**	**p_i**
obsahuje min. 6 znaků, číslice, kombinace malých a velkých písmen	61	87 %
obsahuje pouze číslice	3	4 %
obsahuje pouze písmena	2	3 %
kombinace písmen a čísel, max. 5 znaků	4	6 %
∑ (suma)	**70**	**100 %**

Tabulka 5 Hesla a jejich struktura
Zdroj: Vlastní zpracování



Graf 5 Hesla a jejich struktura
Zdroj: Vlastní zpracování

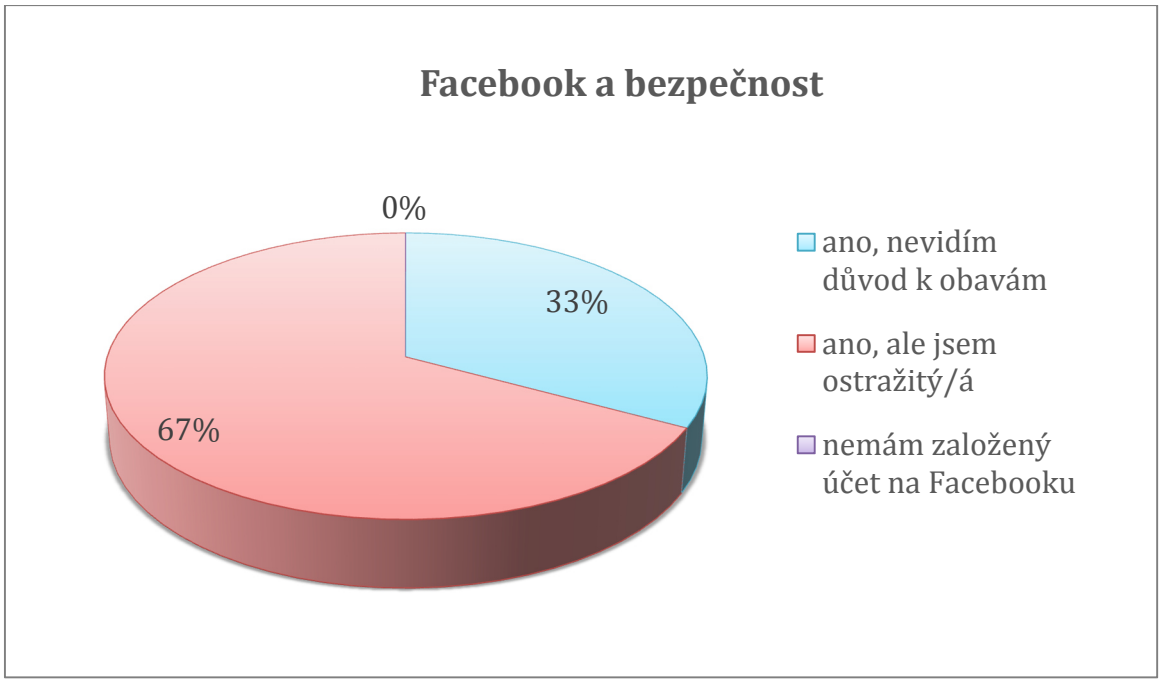
Otázka č. 6

Máte účet na sociální síti Facebook? Pokud ano, cítíte se zde bezpečně?

Účet na sociální síti vlastní 100 % z celkového počtu 70 dotazovaných. Z toho 67 % studentů se necítí na sociální síti bezpečně a jsou proto ostražití, zbylých 33 % nevidí žádný důvod k obavám.

Odpovědi	**n_i**	**p_i**
ano, nevidím důvod k obavám	23	33 %
ano, ale jsem ostražitý/á	47	67 %
nemám založený účet na Facebooku	0	0 %
∑ (suma)	**70**	**100 %**

Tabulka 6 Facebook a bezpečnost
Zdroj: Vlastní zpracování



Graf 6 Facebook a bezpečnost
Zdroj: Vlastní zpracování

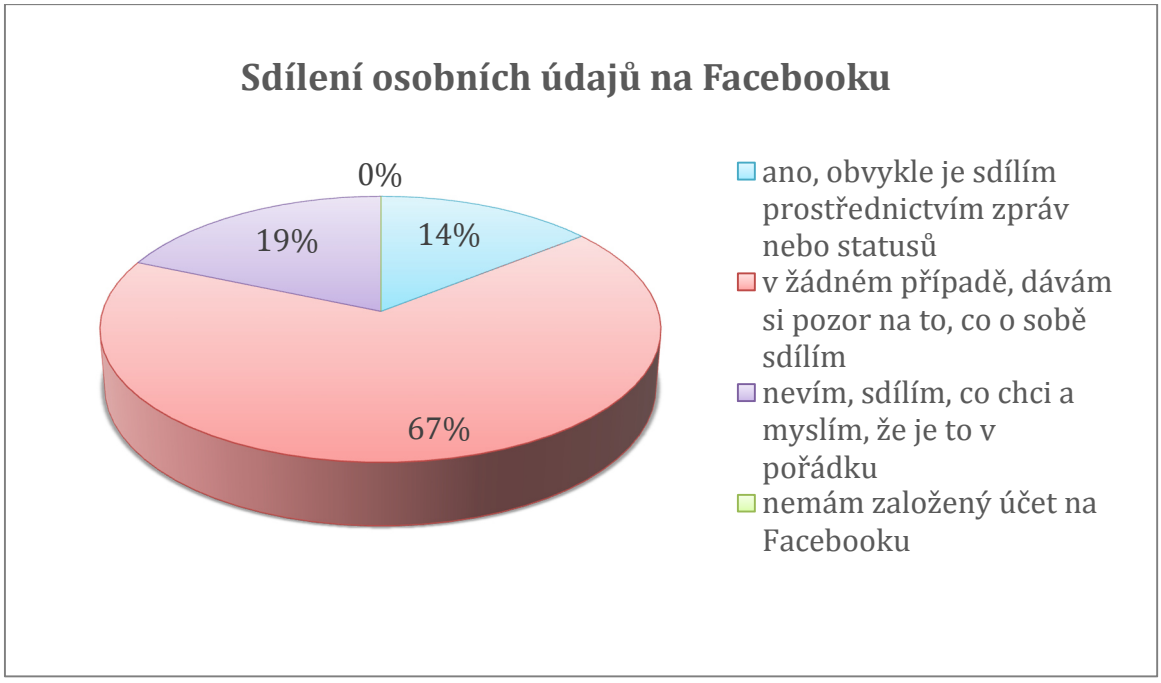
Otázka č. 7

Sdílíte prostřednictvím Facebooku svoje osobní údaje?

Na sociální síti Facebook sdílí své osobní informace 14 % respondentů. V žádném případě o sobě osobní údaje nešíří 67 % dotazovaných. Zbylých 19 % neví přesně, co sdílí, ale myslí si, že je to tak v pořádku.

Odpovědi	**n_i**	**p_i**
ano, obvykle je sdílím prostřednictvím	10	14 %
v žádném případě, dávám si pozor na to, co o sobě sdílím	47	67 %
nevím, sdílím, co chci a myslím, že je to v pořádku	13	19 %
nemám založený účet na Facebooku	0	0 %
∑ (suma)	**70**	**100 %**

Tabulka 7 Sdílení osobních údajů na Facebooku
Zdroj: Vlastní zpracování



Graf 7 Sdílení osobních údajů na Facebooku
Zdroj: Vlastní zpracování

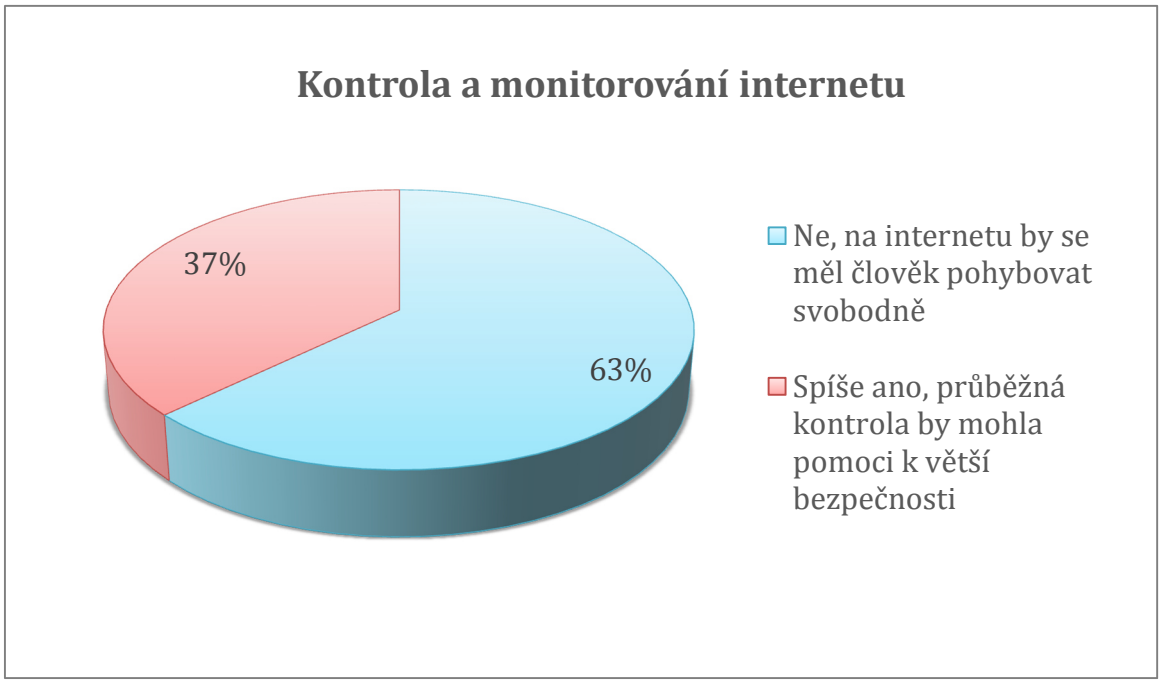
Otázka č. 8

Jste pro to, aby byl internet více monitorován a kontrolován?

Kontrolování a monitorování internetu by mohlo pomoci k větší bezpečnosti. O tomto faktu je přesvědčeno 37 % dotazovaných. Ovšem 63 % respondentů nesouhlasí s důkladnějšími kontrolami Internetu.

Odpovědi	**n_i**	**p_i**
Ne, na internetu by se měl člověk pohybovat svobodně	44	63 %
Spíše ano, průběžná kontrola by mohla pomoci k větší bezpečnosti	26	37 %
∑ (suma)	**70**	**100 %**

Tabulka 8 Kontrola a monitorování internetu
Zdroj: Vlastní zpracování



Graf 8 Kontrola a monitorování internetu
Zdroj: Vlastní zpracování

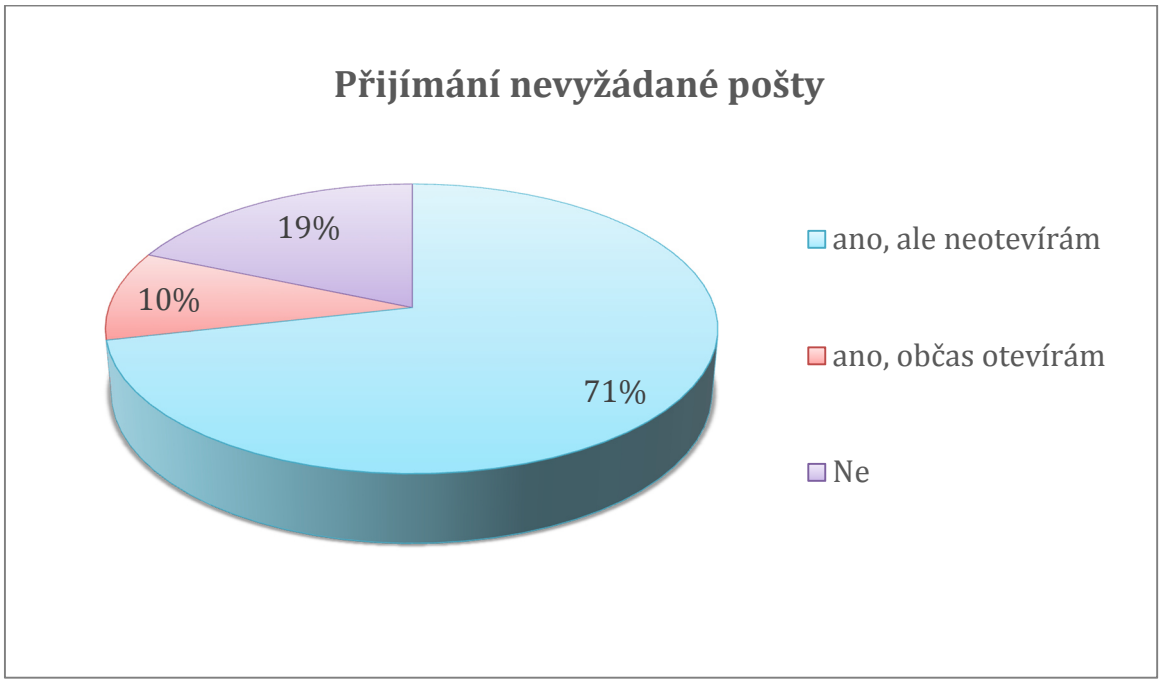
Otázka č. 9

Přichází Vám na emailovou stránku nevyžádaná pošta (spamy), pokud ano, otevíráte je?

Nevyžádaná pošta přichází do schránek 81 % respondentům, z toho pouze 10 % dotazovaných ji otevírá. Naopak 19 % nevyžádanou poštu svých schránkách nenachází.

Odpovědi	**n_i**	**p_i**
ano, ale neotevírám	50	71 %
ano, občas otevírám	7	10 %
Ne	13	19 %
∑ (suma)	**70**	**100 %**

Tabulka 9 Přijímání nevyžádané pošty
Zdroj: Vlastní zpracování



Graf 9 Přijímání nevyžádané pošty
Zdroj: Vlastní zpracování

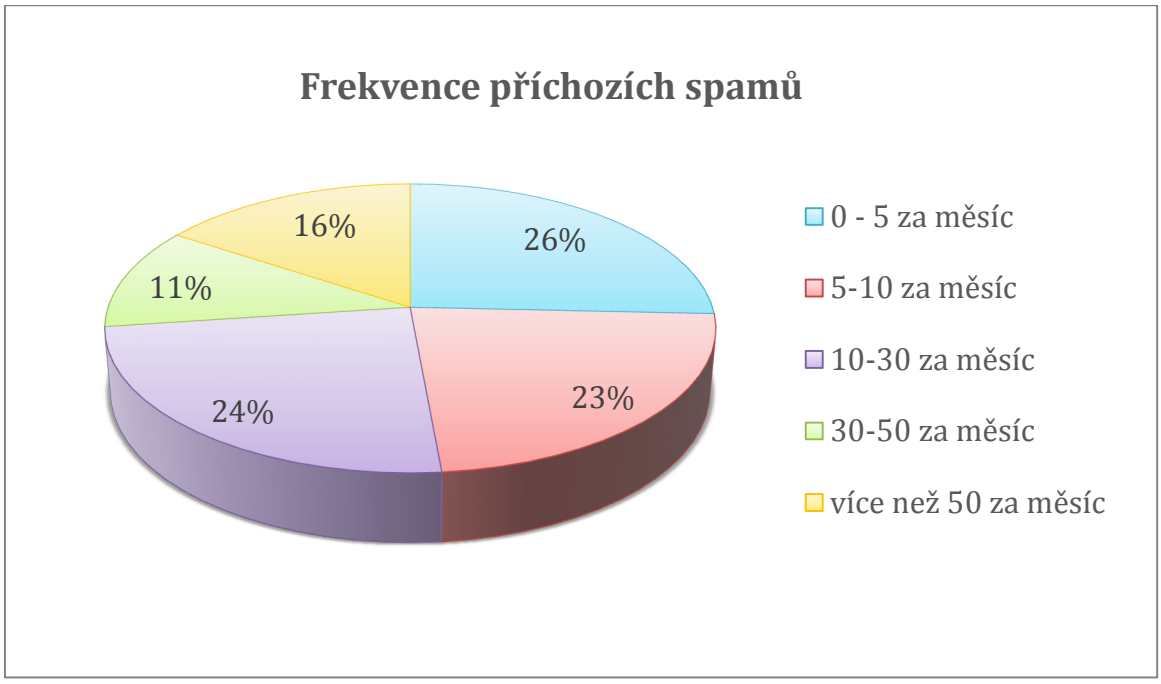
Otázka č. 10

Pokud ano, kolik spamu (nevyžádané pošty) ve Vaší emailové schránce nacházíte?

Maximálně 5 spamů měsíčně má ve své schránce 26 % respondentů, 5 – 10 spamů zakroužkovalo 23 % respondentů, 10 - 30 nevyžádaných zpráv ve schránce nachází 24 %, 30 – 50 spamů dostává 11 % a více než 50 spamů měsíčně obdrží 16 % respondentů.

Odpovědi	**n_i**	**p_i**
0 - 5 za měsíc	18	26 %
5-10 za měsíc	16	23 %
10-30 za měsíc	17	24 %
30-50 za měsíc	8	11 %
více než 50 za měsíc	11	16 %
∑ (suma)	**70**	**100 %**

Tabulka 10 Frekvence příchozích spamů
Zdroj: Vlastní zpracování



Graf 10 Frekvence příchozích spamů
Zdroj: Vlastní zpracování

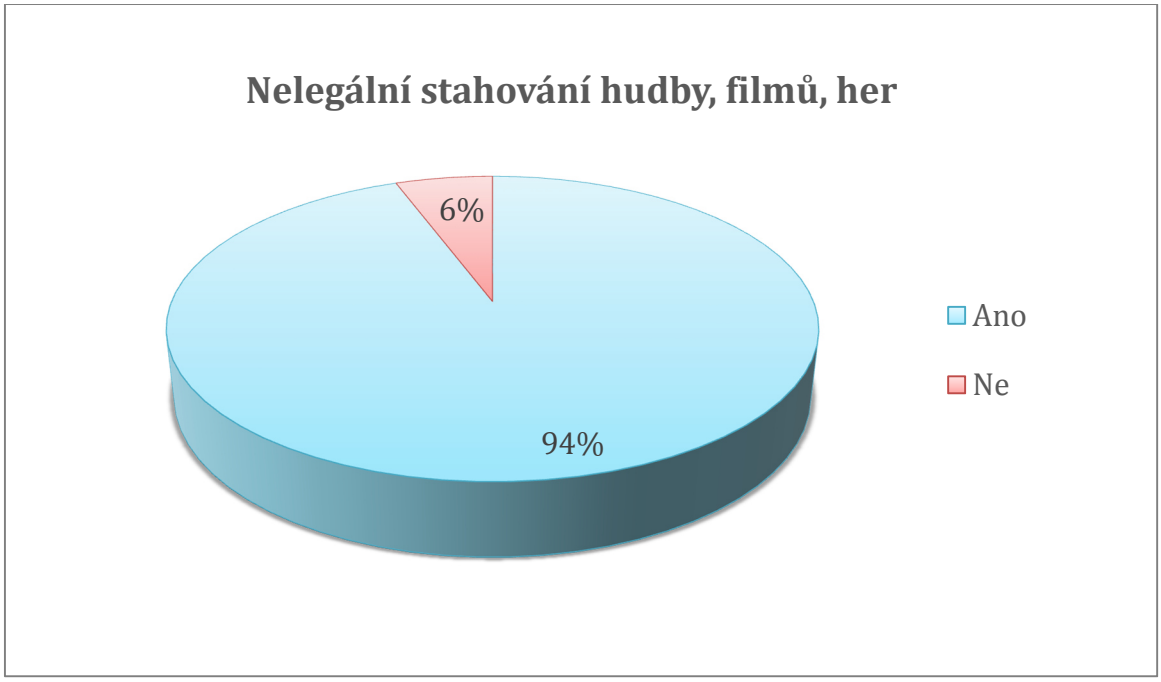
Otázka č. 11

Vlastníte nějakou kopii hudby, filmů, her, které jste nelegálně stáhli z internetu?

Nelegálně staženou kopii hudby, filmů či her vlastní 94 % dotazovaných. Zbylých 6 % nevlastní nelegální software.

Odpovědi	**n_i**	**p_i**
Ano	66	94 %
Ne	4	6 %
∑ (suma)	**70**	**100 %**

Tabulka 11 Nelegální stahování hudby, filmů, her
Zdroj: Vlastní zpracování



Graf 11 Nelegální stahování hudby, filmů, her
Zdroj: Vlastní zpracování

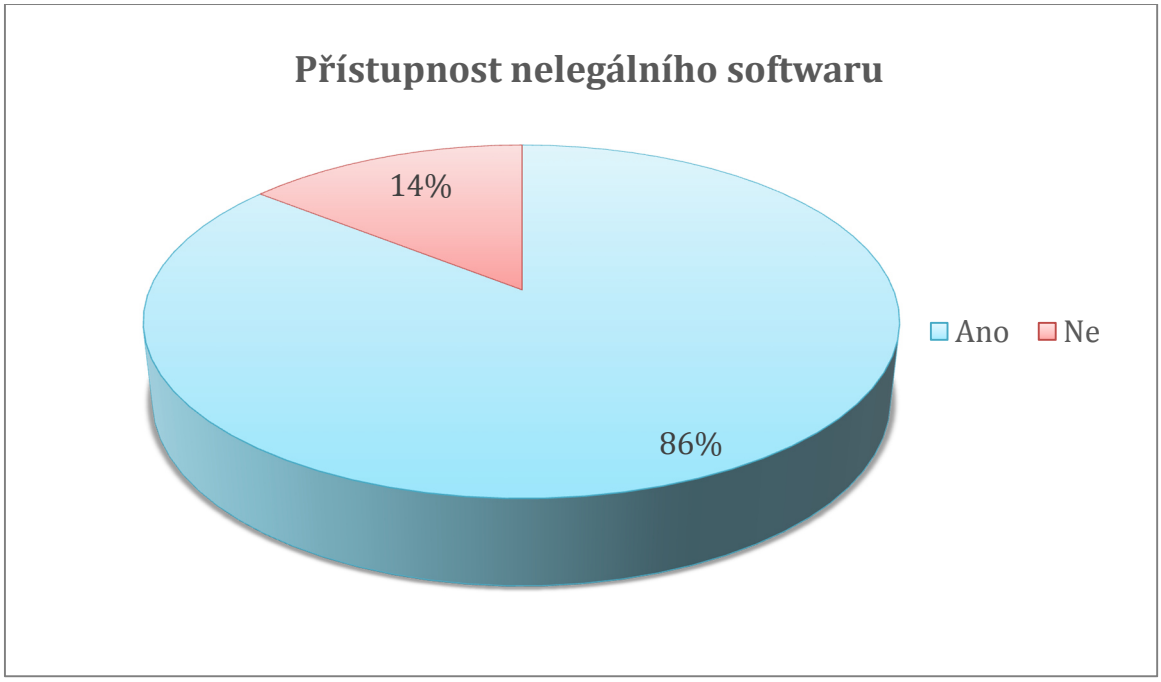
Otázka č. 12

Je pro Vás nelegální software snadno přístupný?

Dle dotazníkového šetření, 86 % respondentů odpovědělo, že je nelegální software pro ně a většinu lidí snadno přístupný, 14 % dotazovaných si myslí, že nikoliv.

Odpovědi	**n_i**	**p_i**
Ano	60	86 %
Ne	10	14 %
∑ (suma)	**70**	**100 %**

Tabulka 12 Přístupnost nelegálního softwaru
Zdroj: Vlastní zpracování



Graf 12 Přístupnost nelegálního softwaru
Zdroj: Vlastní zpracování

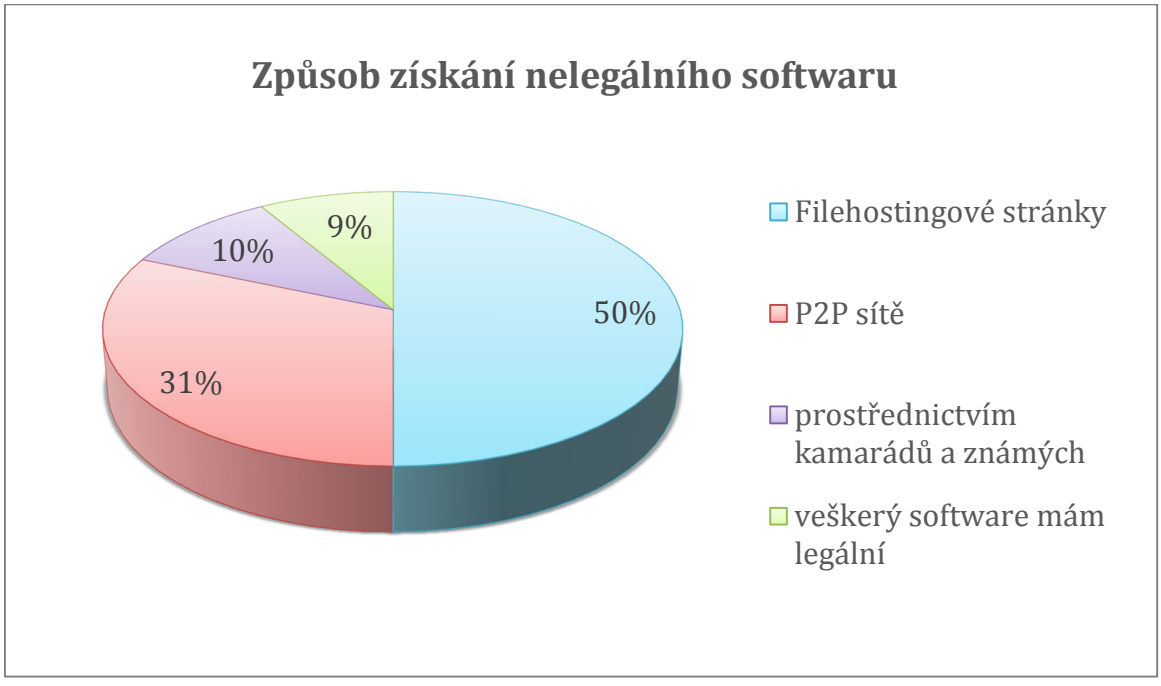
Otázka č. 13

Kde si nejčastěji opatřujete nelegální software?

Filehostingové stránky např. Rapidshare, Uložto používá ke stahování nelegálního softwaru polovina respondentů (50 %) a P2P sítě 31 % dotazovaných. Prostřednictvím kamarádů a známých získává nelegální software 10 % a zbylých 9 % respondentů vlastní pouze legální software.

Odpovědi	**n_i**	**p_i**
Filehostingové stránky (Rapidshare, Uložto, atd…)	35	50 %
P2P sítě (Torrent, DC++)	22	31 %
prostřednictvím kamarádů a známých	7	10 %
veškerý software mám legální	6	9 %
∑ (suma)	**70**	**100 %**

Tabulka 13 Způsob získání nelegálního softwaru
Zdroj: Vlastní zpracování



Graf 13 Způsob získání nelegálního softwaru
Zdroj: Vlastní zpracování

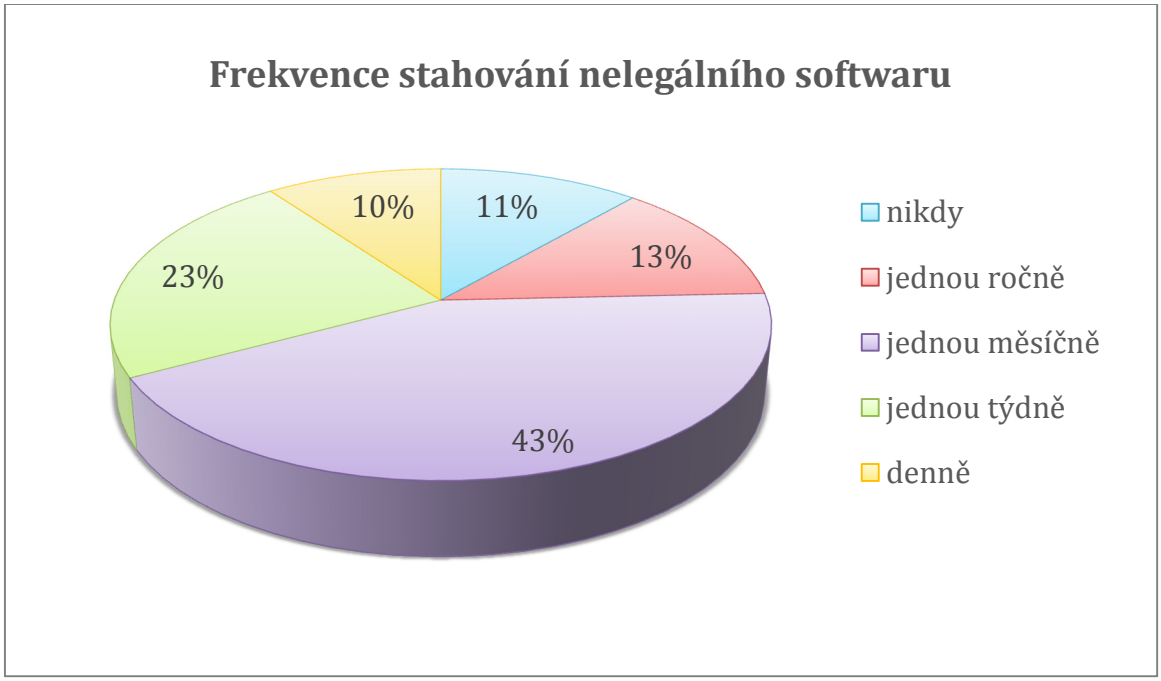
Otázka č. 14

Jak často stahujete nelegální software?

Každý den stáhne nelegální software 10 % dotazovaných, jednou týdně 23 %, skoro polovina respondentů (43 %) stahuje nelegální software jednou měsíčně, jednou ročně 13 % a ostatní (11 %) vlastní pouze legální software, proto nestahují vůbec.

Odpovědi	**n_i**	**p_i**
nikdy	8	11 %
jednou ročně	9	13 %
jednou měsíčně	30	43 %
jednou týdně	16	23 %
denně	7	10 %
∑ (suma)	**70**	**100 %**

Tabulka 14 Frekvence stahování nelegálního softwaru
Zdroj: Vlastní zpracování



Graf 14 Frekvence stahování nelegálního softwaru
Zdroj: Vlastní zpracování

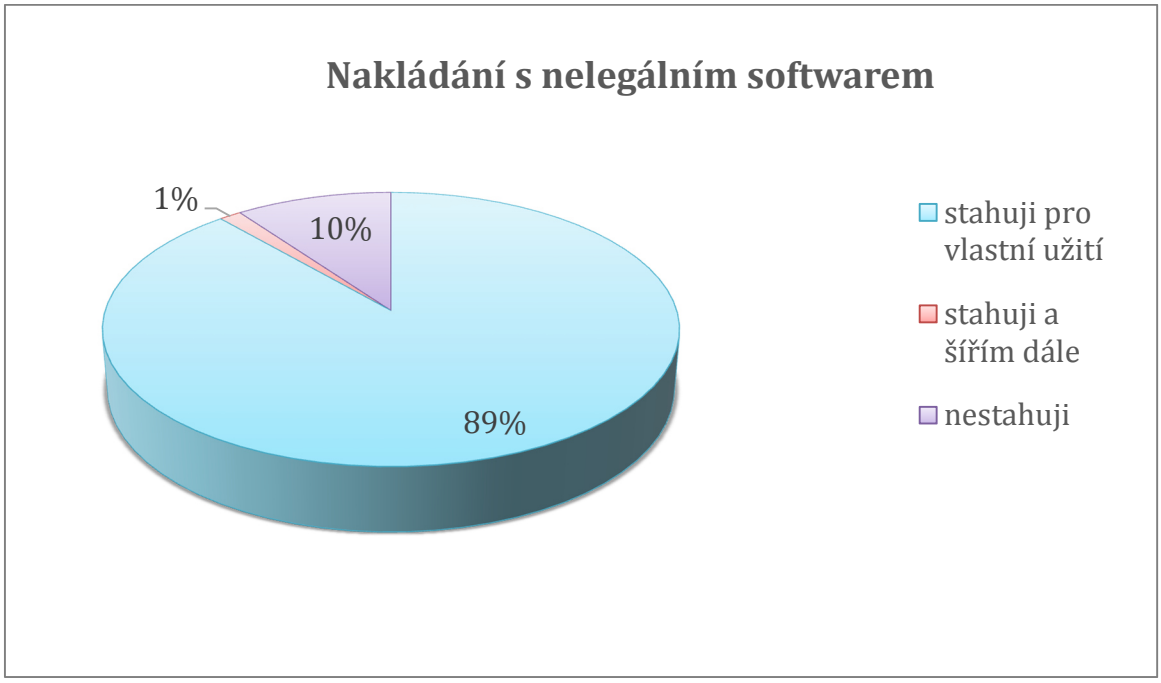
Otázka č. 15

Jak nakládáte s nelegálním softwarem?

Pouze pro vlastní užití vlastní většina respondentů (89 %) nelegální software, 1 % dále tento software šíří a ostatní (10 %) nestahují vůbec.

Odpovědi	**n_i**	**p_i**
stahuji pro vlastní užití	62	89 %
stahuji a šířím dále	1	1 %
nestahuji	7	10 %
∑ (suma)	**70**	**100 %**

Tabulka 15 Nakládání s nelegálním softwarem
Zdroj: Vlastní zpracování



Graf 15 Nakládání s nelegálním softwarem
Zdroj: Vlastní zpracování

4.4 Souhrn výsledků a návrh řešení

Vzhledem k výsledkům z dotazníkového šetření je možno říci, že se ho z větší části účastnili studenti, kteří s počítačem denně pracují, a zvládají některé pokročilé postupy při řešení různých problémů na počítači. Z toho vyplývají i následující výsledky.

ZABEZPEČENÍ

Protože 80 % respondentů běžně používá počítač a internet k práci s citlivými osobními daty, je tudíž velmi důležitá ochrana. Hlavní příčinou toho, že se různí hackeři a pachatelé trestných činností dostanou k velice citlivým údajům je také to, že uživatelé nesprávně zvolí přístupové heslo.

Jednou z otázek dotazníku byla, jestli respondenti volí dostatečně silná hesla, tedy kombinace číslic a písmen velkých i malých v dostatečné délce. Co se týče výsledků, jaké uvedli respondenti, je složitost a tím pádem bezpečnost jejich hesel pro přístup k osobním datům na celkem dobré úrovni. Téměř 90 % z nich uvedlo, že jejich heslo obsahuje kromě minimálního počtu šesti znaků i číslice a kombinace malých a velkých čísel. **Tento zajímavý a pozitivní fakt se neshoduje se stanovenou hypotézou.**

Pro zajímavost, heslo o 4 znacích dokáže hacker prolomit za 0.2 s, o 8 znacích za 2,5h, ale pokud se jedná o všechny symboly ASCII tabulky, tak heslo o délce 8 znaků hacker zlomí za 91 let.

Další otázka, která byla položena respondentům, se týkala bezpečnostních programů. Celkem 94 % studentů uvedlo, že na svém počítači používá nějaký druh bezpečnostního programu, z toho přes 64 % využívá volně dostupnou verzi antivirového programu, která je zdarma. **Tento fakt je potvrzen výsledkem dotazníkového šetření**. Necelých 14 % používá integrované nástroje systému, jako je například Firewall. Znepokojujícím údajem je, že 6% z dotazovaných nepoužívá žádný bezpečnostní program na svém počítači.

Z výsledků plyne, že za antivirovou ochranu si je ochotno zaplatit méně než šestina dotazovaných. Důvodem může být vysoká cena za kvalitní ochranu v souvislosti s nepřeberným množstvím bezplatných verzí těchto programů a do jisté míry možná i jistá nevzdělanost a apatie co se týká hrozeb a rizik na internetu.

NEBEZPEČÍ NA SOCIÁLNÍ SÍTI FACEBOOK

Protože všichni respondenti vlastní účet na sociální síti Facebook, další otázka, která byla položena respondentů, se týkala bezpečnosti na Facebooku. Bezpečně se zde cítí 67 % studentů, zbylých 33 % se snaží o ostražitost při pohybu na Facebooku.

Jaké procento studentů sdílí osobní informace prostřednictvím sociální sítě Facebook? Na tuto otázku odpovědělo 67 % respondentů, že o sobě nesdílí žádné osobní informace na sociální síti. Dalších 19 % studentů nemá přehled o tom, jaké informace přesně na Facebooku sdílí a neřeší to. Zbylých 14 % pak uvádí, že své osobní údaje sdílí prostřednictvím zpráv nebo statusů. Z tohoto šetření vyplývá to, že své osobní údaje na sociální síti sdílí zhruba *čtvrtina* respondentů. **Na základě tohoto tvrzení se POTVRZUJE stanovená hypotéza.**

Další otázka, která byla dotázaným položena, se týkala jejich názoru na bezpečnost internetu, tedy jestli si myslí, zdali je internet bezpečné místo, z hlediska zneužití údajů, fotografií, a nelegálního šíření dat.

Kontrolování a monitorování internetu by mohlo pomoci k větší bezpečnosti. O tomto faktu je přesvědčeno pouze 37 % respondentů. Zbylých 63 % respondentů nesouhlasí s důkladnějšími kontrolami Internetu. Výsledek dotazníkového šetření zřejmě koresponduje s následujícími fakty.

NELEGÁLNÍ ČINNOSTI

Jak bylo zmíněno na začátku, úroveň znalostí práce s PC respondentů, kteří se tohoto dotazníkového šetření zúčastnili, značně ovlivnila jeho výsledky.

Více jak 90 % respondentů odpovědělo, že vlastní nějakou nelegální kopii her, hudby, filmů. A co se týče dalšího sdílení, jeden z dotazovaných odpověděl, že data podléhající autorskému právu sdílí, což je protizákonné. Pouze pro vlastní užití, vlastní tento nelegální software skoro 90% respondentů. Jeho používání je podle výsledků šetření celkem dost rozšířené. Hlavním důvodem jeho používání je vysoká cena. Nejvíce si uživatelé tento software opatřují prostřednictvím Filehostingových stránkem např. Rapidshare, Uložto, pomocí, P2P sítě nebo od přátel a známých. Není divu, že tolik lidí používá nelegální software, když většina nepovažuje jeho užívaní za krádež srovnatelnou s movitou věcí. **Na základně těchto výsledků se potvrzuje další stanovená hypotéza**

SPAM

Každý snad ví co je to spam, proto se další otázka v dotazníku týkala této nevyžádané pošty, a jak často respondentům chodí na své emailové adresy.

Výsledky nejsou nikterak překvapující, dle statistik 81 % studentů nachází ve své schránce spam. **Na základě tohoto šetření se stanovená hypotéza potvrdila.** Převážná většina nevyžádanou poštu neotevírá a ti co ano, postupují při jejich prohlížení velmi obezřetně.

Maximálně 5 spamů měsíčně má ve své schránce 26 % respondentů, 5 – 10 spamů zakroužkovalo 23 % respondentů, 10 - 30 nevyžádaných zpráv ve schránce nachází 24 % - **což se mi potvrdilo**, a 30 – 50 spamů dostává 11 % a více než 50 spamů měsíčně obdrží 16 % respondentů.

NÁVRHY MOŽNÝCH ŘEŠENÍ

Jak již bylo v práci uvedeno, boj proti počítačové kriminalitě musíme rozdělit na dvě základní složky, **prevence a represe**. Pokud například poškozený ve svém počítači nemá žádný druh preventivní ochrany, je zde vysoká pravděpodobnost, že se mu do jeho počítače někdo “naboura“, a on o tom nebude vůbec vědět. Samozřejmě pak nebude mít ani on, ani policie, či další orgány, zabývající se touto kriminalitou, důvod ani snahu takovou kriminální činnost řešit.

Co se vzájemného poměru těchto složek týká, je jasné, že právě prevence zaujímá imaginární vůdčí postavení, jelikož působení represe je kvůli velkému množství komplikací při vyšetřování těchto počítačových zločinu velmi omezené.

Prevence, která představuje různá zabezpečení, komplikující činnost útočníka, jako je prolomení přístupu do cizího počítače a jeho dat, se nazývá „technologická prevence“. V tomto případě ochrany svých dat je nutné mít zapnuté bezpečnostní prvky, jako jsou antivirové programy, antispyware, firewall, zapnutý rezidentní štít a další takto zaměřené preventivní programy. Zde nestačí pouze mít tyto programy, ale důležitým prvkem je zde také udržovat tyto programy s aktualizované spolu s jejich nejnovější databází škodlivého softwaru. Pokud jsou tyto programy na počítači takto udržované, pravděpodobnost ochrany před nebezpečným vlivem vnějšího prostředí se výrazně zvýší.

Další možnou hrozbou na internetu jsou e-mailové zprávy obsahující spam. Je velmi důležité neotevírat poštu s neznámou přílohou a stejně tak e-maily, které nám nedávají smysl. Lepší je takové e-maily rovnou vymazat. Jedním ze základních preventivních prvků je filtrování emailové pošty. Pokud je filtr správně nastaven, nepronikne ním až 100% spamu.

Důležitým prvkem ochrany našeho počítače, je nejen stahování aktualizací antivirového programu, ale i stahování pravidelných aktualizací systémů od autorizovaného výrobce.

Kromě ochrany počítače pomocí programů a jejich aktualizací je dalším velice důležitým prvkem prevence dostatečné povědomí uživatelů pohybujících se na internetu. Toto povědomí by se mělo týkat především bezpečnostních rizik na internetu.

Často diskutovaným problémem jsou nedostatečně silná hesla některých uživatelů. Doporučuje se mít heslo o minimální délce 6 - 8 znaků složené ze všech znaku ASCII tabulky. Takto zvolené heslo výrazně prodlouží čas, který musí hacker vynaložit, než ho dokáže prolomit, navíc když bude uživatel své heslo pravidelně měnit, je velice obtížné, aby k jeho datům kdokoliv získal přístup.

Povědomí uživatelů by se nemělo týkat jen toho, jakým způsobem svá data zabezpečit vůči útokům zvenčí, ale mělo by se týkat také etikety, tedy chování na internetu, což se vztahuje na celou společnost. Pokud bude mít společnost povědomí například o tom, jaká rizika obnáší mít na svém počítači nelegální software, může to ve vztahu k legalitě pozitivně ovlivnit způsob, jak budou, nebo nebudou s tímto druhem softwaru dále nakládat. Problémům, spojeným s prošetřováním legálnosti firemního softwaru lze předejít pomocí tzv. „softwarového auditu“. Ten firmám zaručí legálnost jejich softwaru.

Dalším důležitým prvkem prevence, je tzv. „psychologická prevence“. Ta souvisí s šířením povědomí o společenské nepřijatelnosti a nemorálnosti protiprávních činů, které souvisí s počítačovou kriminalitou. Někteří lidé jsou přesvědčeni o dostatečné míře anonymity na internetu a myslí si, že na ně nemůže nikdo přijít, když stahují a sdílí audiovizuální díla, hudbu a software, podléhající autorskému zákonu. Neuvědomují si, že se mohou dopouštět trestného činu, který je srovnatelný s krádeží. Důvodem, proč se tato díla dále šíří, může být cena, která je nad uživatelovy finanční možnosti. Tento problém by se dal částečně řešit snížením cen produktů výrobců softwaru, stejně jako hudby a filmů. Tím by se jistě snížil i počet nelegálně šířených dat.

Častým terčem internetových podvodů bývají různé společnosti, které na internetu nabízí své služby k ochraně svých aplikací. Jsou jimi například bankovní instituce. Jejich klienti jsou někdy oběťmi podvodných emailů. Když už se ale obětí stanou, je důležité pachateli, který získá jejich přihlašovací údaje, pomocí zvýšení zabezpečení zkomplikovat transakce na účtech. Toho se dá dosáhnout například certifikátem, který vlastní pouze uživatel na svém počítači nebo pomocí zasílání autorizačních SMS.

5 Závěr

Počítačová kriminalita si bezesporu zaslouží jistou dávku pozornosti, jednak ze strany laické či odborné veřejnosti, ale i ze strany orgánů činných v trestním řízení.

Cílem práce je stručně nastínit historický vývoj a současné formy počítačové kriminality, použitím literatury zmapovat problémy počítačové kriminality a nastínit možné způsoby k její regulaci. Vymýtit tuto kriminalitu ze světa úplně je totiž nereálné.

Na základě dotazníkového šetření bylo zjištěno, že s internetovou kriminalitou se může potýkat každý uživatel a to bez rozdílů věku či pohlaví. Uživatelé stále nedostatečně zabezpečují svá data vhodným antivirovým programem. Upřednostňují bezplatnou verzi Antivirového programu před placenou. Zabezpečení hesel jednotlivých uživatelů je však celkem na dobré úrovni.

Pozitivním zjištěním je přístup uživatelů k nevyžádané poště. Většině z dotazovaných přichází na email minimálně 5 spamů měsíčně, z toho převážná část spamy neotevírá a pokud ano, postupují velice obezřetně.

Fenoménem současné doby se stala veřejná sociální síť Facebook. Z celkového počtu respondentů, všech 70 dotazovaných má založený účet na této sociální síti. Z toho vyplývá následující riziko – riziko sdílení osobních informací. I když 67 % uživatelů osobní informace prostřednictví sociální sítě nesdílí, jsou tu i ti, kteří tuto hrozbu neřeší a nebojí se o sobě prozrazovat citlivější osobní údaje široké veřejnosti.

Díky anonymitě, kterou internet svým uživatelům nabízí, s počítačovou kriminalitou přicházejí do styku i méně pokročilí uživatelé, ať už cíleně či nevědomě. Tito uživatelé se dopouštějí převážně nelegálního stahování hudby, filmů či her prostřednictvím Filehostingových stránek, které jsou pro veřejnost snadno přístupné.

6 Seznam použité literatury

Knižní zdroje

[1] ADÁMEK, Martin. *Spam: jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu*. 1. vyd. Praha: Grada, 2009, 166 s. Průvodce (Grada). ISBN 978-80-247-2638-0.

[2] CRAIG, Paul P a Ron HONICK. *Softwarové pirátství bez záhad*. 1. vyd. Praha: Grada, 2008, 212 s. ISBN 978-80-247-1765-4.

[3] GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

[4] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247- 1561-2.

[5] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-7226-419-2.

[6] MC CARTHY. Linda, WELDON-SIVIY. Denise. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ. NIC, [2013], 316 s. ISBN 978-80-904248-6-9.

[7] MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking bez záhad*. 1. vyd. Praha: Grada, 2007, 520 s. ISBN 978-80-247-1502-5.

[8] POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, 388 s. Téma (Auditorium). ISBN 978-80-87284-22-3.

[9] POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP*. Vyd. 1. Brno: Computer Press, 2007, v, 150 s. Právo a IT. ISBN 978-80-251-1777-4.

[10] STEBE, Matthew a Charles PERKINS. *Firewally a proxy-servery: praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, xiv, 450 s. ISBN 80-7226-9836.

Internetové zdroje

[1] BSA THE SOFTWARE ALLIANCE. *O BSA a členech.* [online]. 2014, cit. 2015-04-01] Dostupné z: http://ww2.bsa.org/country/BSA%20and%20Members.aspx

[2] ČESKÁ PROTIPIRÁTSKÁ UNIE. *Kdo jsme a čím se zabýváme.* [online]. 2015, [cit. 2015-04-01] Dostupné z: http://www.cpufilm.cz/kdo_jsme.html

[3] DOČEKAL, Daniel - LUPA CZ. *Facebook mění pravidla* [online]. 2014, [cit. 2015-04-01] Dostupné z: http://www.lupa.cz/clanky/facebook-meni-pravidla-chcete-vedet-co-se-skutecne-zmeni/

[4] HYNČICOVÁ, Kateřina - PRAVNI RADCE *Česká republika po osmi letech ratifikovala Úmluvu o počítačové kriminalitě* [online]. 2013, [cit. 2015-04-01] Dostupné z: http://pravniradce.ihned.cz/c1-60516560-ceska-republika-po-osmi-letech-ratifikovala-umluvu-o-pocitacove-kriminalite

[5] IBN LIVE. *Technologie* [online]. 2014, [cit. 2015-04-01] Dostupné z: http://ibnlive.in.com/news/facebook-messenger-app-loaded-with-spyware-security-specialist/500258-11.html

[6] KURZY CZ. *Zákony* [online]. 2015, [cit. 2015-04-01] Dostupné z: http://zakony.kurzy.cz/140-1961-trestni-zakon/paragraf-257a/

[7] MALIŠ, - PRÁVO IT *Významná změna v právní úpravě SPAMu* [online]. 2012, [cit. 2015-04-01] http://www.pravoit.cz/article/vyznamna-zmena-v-pravni-uprave-spamu-od-1-1-2012

[8] MICROSOFT. *Ochrana práv* [online]. 2015, [cit. 2015-04-01] Dostupné z: http://www.microsoft.com/cze/legalnisoftware/ochrana-prav/souvisejici-zakony.aspx

[9] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Dokumenty – kybernetické hrozby* [online]. 2009, [cit. 2015-04-01] Dostupné z: http://www.mvcr.cz/soubor/informacni-pdf.aspx

[10] PORTÁL VEŘEJNÉ SPRÁVY. *Zákony* [online]. 2015, [cit. 2015-04-01] Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=58329&recShow=1&nr=480~2F2004&rpp=15#parCnt

[11] PORTÁL VEŘEJNÉ SPRÁVY. *Zákony* [online]. 2015, [cit. 2015-04-01] Dostupné z http://portal.gov.cz/app/zakony/zakonPar.jsp?page=2&idBiblio=68040&recShow=235&nr=40~2F2009&rpp=100#parCnt

[13] PORTÁL VEŘEJNÉ SPRÁVY. *Zákony.* [online]. 2015, [cit. 2015-04-01] Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?page=2&idBiblio=68040&recShow=234&nr=40~2F2009&rpp=100#parCnt

[14] SOKOL, Tomáš - PRAVNI RADCE *Postih počítačové kriminality podle nového trestního zákona* [online]. 2009, [cit. 2015-04-01] Dostupné z: http://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona

[15] ZAHRADNÍČEK, Jaroslav - PATRIA ONLINE *Zákony.* [online]. 2014, [cit. 2015-04-01] Dostupné z: https://www.patria.cz/pravo/2694193/pocitacova-kriminalita-mezinarodni-umluva-je-konecne-zavazna-i-pro-cesko.html

Seznam tabulek

Seznam grafů

7 Přílohy

1) Příloha č. 1 – Dotazník

Dobrý den,

jmenuji se Vojtěch Hartman a jsem studentem 3. ročníku oboru Informační management na Univerzitě v Hradci Králové. Chtěl bych Vás požádat o vyplnění tohoto dotazníku, který je součástí mé bakalářské práce na téma: ***„počítačová kriminalita“.*** Dotazník obsahuje 16 otázek. Odpovězte na každou otázku co nejpřesněji. **Prosím, u každé otázky označte vždy jen jednu odpověď.**

Předem děkuji za Vaši ochotu spolupracovat.

1. Uveďte prosím Váš věk ……

2. Jaká je Vaše znalost v oblasti IT?
a) základní (práce s programy, Office, základní používání internetu)
b) pokročilá (reinstalace op. systému, řešení problému, základy programování)
c) profesionální (PC jako zdroj obživy, programátor, IT specialista)

3. Používáte internet pro práci s citlivými osobními daty? (internetové bankovnictví, účetnictví, atd…)
a) ano
b) ano, jen když nemám jinou možnost
c) ne

<u>Zabezpečení</u>

4. Zaškrtněte, jaký bezpečnostní program na vašem počítači používáte.
a) Antivir - placená verze
b) Antivir – freeware (zdarma)
c) Integrované nástroje systému (Firewall)
d) jiné
e) žádný

5. Jak vypadá Vaše heslo, jež používáte pro přístup k Vašim citlivým údajům?

a) obsahuje min. 6 znaků, číslice, kombinace malých a velkých písmen

b) obsahuje pouze číslice

c) obsahuje pouze písmena

d) jiné

Nebezpečí na sociálních sítích

6. Máte účet na sociální síti Facebook? Pokud ano, cítíte se zde bezpečně?

a) ano, nevidím důvod k obavám

b) ano, ale jsem ostražitý/á

c) nemám založený účet na Facebooku

7. Sdílíte prostřednictvím Facebooku svoje osobní údaje?

a) ano, obvykle je sdílím prostřednictvím zpráv nebo statusů

b) v žádném případě, dávám si pozor na to, co o sobě sdílím

c) nevím, sdílím, co chci a myslím, že je to v pořádku

d) nemám založený účet na Facebooku

8. Jste pro to, aby byl internet více monitorován a kontrolován?

a) Ne, na internetu by se měl člověk pohybovat svobodně

b) Spíše ano, průběžná kontrola by mohla pomoci k větší bezpečnosti

Spam

9. Přichází Vám na emailovou stránku nevyžádaná pošta (spamy), pokud ano, otevíráte je?

a) ano, ale neotevírám

b) ano, občas otevírám

c) ne

10. Pokud ano, kolik spamu (nevyžádané pošty) ve Vaší emailové schránce nacházíte?

a) 0 - 5 za měsíc napsat třeba

b) 5-10 za měsíc

c) 10-30 za měsíc

d) 30-50 za měsíc

e) více než 50 za měsíc

Nelegální činnosti

11. Vlastníte nějakou kopii hudby, filmů, her, které jste nelegálně stáhli z internetu?

a) ano

b) ne

12. Je pro Vás nelegální software snadnopřístupný?

a) ano

b) ne

13. Kde si opatřujete nelegální software?

a) Filehostingové stránky (Rapidshare, Uložto, atd…)

b) P2P sítě (Torrent, DC++)

c) prostřednictvím kamarádů a známých

d) veškerý software mám legální

14. Jak často stahujete nelegální software?

a) nikdy

b) jednou ročně

c) jednou měsíčně

d) jednou týdně

e) denně

15. Jak nakládáte s nelegálním softwarem?

a) stahuji pro vlastní užití

b) stahuji a šířím dále

c) nestahuji

FIM UHK
UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Rokitanského 62, 500 03 Hradec Králové, tel: 493 331 111, fax: 493 332 235

Zadání k závěrečné práci

Jméno a příjmení studenta: **Vojtěch Hartman**

Obor studia: Informační management (3)
Jméno a příjmení vedoucího práce: **Jan Janeček**

Název práce:
Počítačová kriminalita

Název práce v AJ:
Cybercrime

Podtitul práce:

Podtitul práce v AJ:

Cíl práce: Vymezení pojmu počítačové kriminality, provedení stručného rozboru jejího historického vývoje se zaměřením na analýzu jejích současných forem dotýkajících se především mládeže a návrh možných řešení.

Osnova práce:
1. Vymezení cílů a metod práce.
2. Vymezení pojmů.
3. Analýza historického vývoje počítačové kriminality.
4. Analýza současného stavu.
5. Dotazníkový průzkum.
6. Zhodnocení a návrh řešení.

Projednáno dne: 14. 10. 2014

Podpis studenta

Podpis vedoucího práce