**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z.Ú. ČESKÉ BUDĚJOVICE**

# BAKALÁŘSKÁ PRÁCE

**2017** **Václav Krejčí**

**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z.Ú. ČESKÉ BUDĚJOVICE**

# BAKALÁŘSKÁ PRÁCE

# POČÍTAČOVÁ KRIMINALITA V ČESKÉ REPUBLICE

**Autor práce:** Václav Krejčí
**Studijní obor:** Bezpečnostně právní činnost
**Forma studia:** Kombinovaná
**Vedoucí práce:** Mgr. Vladimír Čížek, DiS.
**Katedra:** Katedra právních oborů a bezpečnostních studií

**2017**

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

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

.....

Děkuji vedoucímu bakalářské práce Mgr. Vladimíru Čížkovi, DiS., za cenné rady, připomínky a metodické vedení práce.

# Abstrakt

KREJČÍ, V. *Počítačová kriminalita v České republice: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, z.ú., 2017. 74 s. Vedoucí bakalářské práce: Mgr. Čížek Vladimír, DiS.

**Klíčová slova:** Česká republika, kybernetická kriminalita, internet, malware, právo

Tato práce se zabývá počítačovou kriminalitou páchanou za pomoci informačních technologií v České republice. V první části práce je popisován vývoj a historie počítačové kriminality, prevence a současný boj, je zde popsána i problematika zabezpečení a zneužitelnosti internetu, který přímo souvisí s touto kriminalitou. Jsou zde rozděleny jednotlivé druhy počítačových kriminalit a zároveň vysvětleny jejich principy. Dále práce popisuje škodlivý software, který napadá dnešní koncové uživatele informačních technologií. Druhá část práce je věnována české legislativě a kvalifikaci jednotlivých skutkových podstat, definici počítačové kriminality a zároveň nejnovějším typům protiprávního jednání, které se objevují především v České republice.

# Abstract

KREJČÍ, V. *Computer crime in the Czech Republic: bachelor thesis.* České Budějovice: The College of European and Regional Studies, 2017. 74 p. Supervisor: Mgr. Čížek Vladimír, DiS.

**Keywords:** Czech republic, cyber-crime, Internet, malware, right

This work deals with computer crime committed using information technology in Czech Republic. In the first part there is described development and history of computer crime, prevention and current struggle with it, there are also described security issues and misuse of internet which is directly related to this kind of crime. There are divided particular types of computer crime and simultaneously there are explained their principles. Further on this work describes harmful software which attacks todays final users of information technology. The second part of the work is dedicated to Czech legislation and qualification of the particular factual essences, definition of computer crime and simultaneously the latest types of illegal negotiations which appear in Czech Republic.

# Obsah

# Úvod

Počítače a internet se staly od doby, kdy začal jejich obrovský rozmach, nedílnou součástí naší společnosti. Od doby jejich vzniku prošly tyto technologie takovým vývojem, že dnes nenajdeme zařízení, které by nedisponovalo připojením do internetové sítě a nevyužívalo jejích možností. Bohužel s tímto rozvojem se začala rozvíjet i trestná činnost, která se stala černou stranou této úžasné pokrokové technologie. Počítačová kriminalita se tak stala jednou z dalších hrozeb, které nelze podceňovat a které se bohužel nevyhnuly ani České republice.

Informační technologie v podobě počítačů a sítě Internet tedy přinesly postupem času společnosti mnoho usnadnění a výhod, kdy však postupně s narůstající počítačovou kriminalitou tato pozitiva začala a bohužel do dnešní doby jsou více a více nebezpečná. Lze říci, že dnes již pravděpodobně nenajdeme uživatele, který by se nesetkal s nějakým druhem počítačové kriminality.

Počítačová kriminalita je v dnešní době celosvětový problém. Každá země se s ní snaží bojovat jinak. V České republice stejně jako v jiných zemích je právní legislativa, která postihuje počítačovou kriminalitu, kdy však takový boj proti této činnosti nestačí. Základním problémem je nízká informovanost veřejnosti a tedy i prevence proti této kriminalitě.

Po přečtení této práce by měl koncový uživatel pochopit, co tedy vlastně počítačová kriminalita znamená, jaká je její historie, proč vznikla a jaké jsou především v České republice nejčastější hrozby a útoky. Zároveň by měl zjistit, zdali lze s počítačovou kriminalitou nějak bojovat, zdali jsou současná opatření dostatečná a jestli vůbec lze počítačovou kriminalitu zastavit.

# 1 Cíl a metodika bakalářské práce

Cílem práce bude pokusit se najít teoretické řešení, které by pomohlo najít způsob, jakým potlačit či zcela zastavit v současné době počítačovou kriminalitu, která je nedílnou součástí dnešního počítačového světa a to především se zaměřením na počítačovou kriminalitu páchanou v České republice.

V bakalářské práci jsem si stanovil následující části. V první teoretické části chci za pomoci dostupných literárních zdrojů vysvětlit vznik a historii počítačové kriminality a s tím i související vznik počítače a internetu, neboť za pomoci těchto prostředků právě počítačová kriminalita mohla vzniknout. Zároveň se pokusím důkladně vysvětlit v jednotlivé kapitole, proč se počítačové kriminalitě tak hojně daří a proč je tzv. boj s touto činností tak velice komplikovaný. První část zakončím popisem nejběžnějších počítačových útoků v České republice, kdy zároveň vysvětlím jejich princip, smysl a možný dopad.

Ve druhé části mé práce vyhodnotím a zanalyzuji dostupné legislativní a právní normy v České republice a vyčlením ty trestné činy, kterých se mohou jedinci páchající tyto činy na území České republiky dopustit. Dále se budu věnovat novým typům možných útoků a zároveň možnostem ochrany a trestním postihům dle trestního zákoníku.

Třetí a poslední část práce věnuji výzkumu, kdy za pomoci právě dostupných informací o nejběžnějších útocích, kde jsou jasně známy postupy a principy, se pokusím najít teoretické řešení, jak těmto útokům zcela předejít nebo je zcela potlačit, resp. až zastavit. Výsledky tohoto zkoumání vyhodnotím a pokusím se navrhnout obecné, případně konkrétní řešení daného problému.

# 2 Vývoj počítačové kriminality, prevence a boj proti počítačové kriminalitě

Díky rozvoji a rozšíření informačních a komunikačních technologií mohou dnes lidé komunikovat s lidmi na druhé straně planety. Mluvíme tedy o vzniku jakéhosi kyberprostoru neboli vytvoření virtuálního prostředí, kde se lidé střetávají, komunikují, uzavírají obchody atd. Přitom mezi nimi dochází ke vzájemnému styku, který nemá pouze aspekty sociální a ekonomické, ale i právní. Bohužel vznik virtuálního prostředí sebou přináší mimo jiné i vznik a rozvoj kriminality.

## 2.1 Zneužitelnost

Bezesporu největší nevýhodou internetu je jeho zneužitelnost. Dle posledních dostupných statistik z června 2016 provedených - Internet World Stats, je k síti internet připojeno přes 3,5 miliardy uživatelů, což je už skoro každý druhý obyvatel naší planety.[1] Vzhledem k tomu, že většina uživatelů si skrze tuto síť spravuje své finance v bance, objednává zboží, provádí platby, komunikuje, sdílí svá data, atd., stal se tak internet v této oblasti velmi zneužitelný pro neoprávněné zjištění citlivých dat jedinců a jejich zneužití.

Zcela jistě mezi nejrozšířenější útoky v síti internet patří právě zjištění přístupových hesel do internetových bankovnictví jednotlivých uživatelů, zjištění informací o platebních kartách při prováděných platbách, či vylákání peněz skrze podvodné inzeráty, pohledávky, exekuce, atd. Toto jsou nejběžnější pokusy obohacení, které provádějí pachatelé skrze síť internet a to i v České republice. Bohužel meze těchto osob neznají hranic, a tak se stále snaží vymyslet dokonalejší způsob, jak se obohatit na úkor druhých. Stále se snaží zdokonalovat své útoky a to jak za pomoci počítačových virů, které neustále vylepšují, tak i za pomoci emailů, které mají jen oklamat koncového uživatele. Jejich výzvy k provedení platby, které rozesílají emailem, jsou stále věrohodnější a i přes veškeré mediální varování, že se vždy v těchto případech jedná o podvody, se najde mnoho jedinců, kteří i přesto požadovanou platbu uhradí, aniž by si nejprve ověřili věrohodnost těchto zpráv.

[1] Internet live stats.com: *Internet statistic* [online].,[cit. 2017-03-01]. Dostupné z WWW: <http://www.internetlivestats.com/internet-users/>.

## 2.2 Zabezpečení

Při využívání sítě internet je velmi důležité zabezpečení. Tato síť sama o sobě nedisponuje jakýmsi velkým zabezpečovacím zařízením, které by nám zaručovalo bezpečný pohyb v této síti. Samotné zabezpečení je tedy na koncovém uživateli. Pohyb uživatele v síti je zaznamenán pomocí takzvané IP adresy (*IP adresa je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti. Zkratka IP znamená „Internet Protocol", což je protokol, pomocí kterého spolu komunikují všechna zařízení v internetu.*). Jedná se jednoduše řečeno o takové evidenční číslo uživatele, pod kterým vystupuje v síti. Pomocí této adresy lze až zjistit, kde uživatel sídlí, kde a kdy navštívil jaké webové stránky, co odeslal atd. [2]

Bohužel i tyto informace dokážou osoby zabývající se internetovou kriminalitou snadno zamaskovat, změnit, či dokonce zničit. Tyto osoby zpravidla disponují programy a znalostmi programování, které dokážou právě shora popisovaným způsobem jejich pohyb v síti zahladit. Často bývají využívány chyby v programech, v operačních systémech nebo v kódování stránek, kdy na základě těchto zjištěných chyb jsou poté vytvářeny různé programy (např. známé jako počítačové viry), kdy tyto jsou naprogramovány tak, že mají za úkol využít dané chyby a proniknout tak do celého programu, systému či webové stránky a napadnout ji. Napadením je myšleno získání, zpravidla skrytě, aniž by uživatel cokoliv zjistil, důležitých dat a jejich odeslání k cílovému zdroji. [3]

Koncový uživatel se proti všem těmto možným útokům může bránit několika způsoby. Nejdůležitější je bezpečný pohyb v síti, kdy jde zejména o to nenavštěvovat nedůvěryhodné webové stránky, neotevírat nevyžádanou poštu a jejich přílohy s neověřeným obsahem, nesdělovat a neuvádět svá citlivá data a platební informace jako čísla platebních karet, přístupová hesla a v případě, že je to nezbytně nutné (např. platba on-line kartou za objednané zboží), si vybírat pouze důvěryhodné a ověřené webové stránky nebo aplikace. Dále se uživatel brání používáním antivirových programů, které mají za účel včasné odhalení možných útoků, také prováděním pravidelných aktualizací

[2] ČERVEŇ, P. *Cracking a jak se proti němu bránit*. Praha : Computer Press, 2001. 90-91 s. ISBN 80-7226-382-X.

[3] MATĚJKA, M. *Počítačová kriminalita*. Praha : Computer Press, 2002. 24-27 s.

používaných programů, především operačního systému a nepoužívání neověřených sítí k připojení k síti internetu, jakou jsou veřejná místa nabízející zdarma připojení k internetu označována jako „WIFI FREE“.

Bohužel ne vždy lze tyto zásadní pravidla zcela dodržet a i v případě dodržení nám přesto nezaručují bezpečný pohyb v internetu. Lze tedy říci, že bezpečnost v síti internet je rovněž jeho slabší stránkou a tedy nevýhodou neboť kdyby byť jen tyto základní a zároveň nejdůležitější chyby v zabezpečení nebyly, byl by pohyb v této síti naprosto bezpečný a nedal by tak vůbec možnost vzniku internetové kriminalitě nebo by její rozmach eliminoval na minimum.

## 2.3 Vznik kybernetické kriminality

Za vznikem počítačové kriminality stojí velká jména osob, avšak za hlavní osobu a nejznámějšího počítačového kriminálníka lze označit osobu Kevin David Mitnick (nar. 6. srpna 1963). Tento „hacker“, jak později začala společnost nazývat osoby páchající počítačovou kriminalitu, měl na svědomí několik velkých skutků. Mezi ně patří např. získání administrátorských práv na počítačích IBM na Computer Learning Center v LA, nabourání se do zdrojového kódu VMS, což je operační systém, který využívají serverové stanice firmy Hewlett-Packard, dále pak nabourání do systémů firem Motorola, Nokia, Fujitsu Siemens, rovněž jsou mu přisuzovány i útoky do systémů Aplle Inc., FBI, Pentagon a další. Za své skutky poprvé v roce 1988 stanul před soudem, následně za pár let znovu, kdy byl následně odsouzen za napáchání škod ve výši 300 miliónů dolarů. Tímto se stal tak prvním odsouzeným hackerem na světě.[4]

Česká republika se rovněž nevyhnula počítačové kriminalitě. K nejzávažnějším počítačovým zločinům docházelo v oblasti bankovního sektoru, internetových podvodů, krádeží a zneužívání osobních dat. V 90. letech bylo v České republice zaznamenáno několik větších bankovních zločinů, které se zpravidla týkaly manipulace s bankovními údaji, kdy až na pár z nich byly všechny kvalifikovány jako podvody. Vznik hackerských skupin byl tak tedy jen otázkou času, kdy se v „českém kyberprostoru“ objevily první hackerské skupiny „Binary Division“ a „CzERT“. Obě tyto skupiny se zaměřovaly na

[4] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 58 s

pozměňování webů. Mezi jejich největší úspěchy můžeme zařadit např. nabourání webu Armády ČR nebo Ministerstva zdravotnictví. Informační zdroje v té době označily hackera za démona českého internetu. V této době bylo potvrzeno asi největší užívání nelegálního softwaru, kdy se hovořilo o zhruba 80% nelegálně používaného programového vybavení v České republice.[5]

K nelegálně užívanému softwaru stojí za zmínku i případ společnosti Mironet, kde bylo v minulosti zjištěno, že zde dochází k instalování nelegálního softwaru. Rovněž lze dále mezi známé počítačové útoky v České republice uvést phisingový útok na klienty Citibank nebo napadnutí webových stránek politické strany ODS skupinou „Hnutí Anonymous“, kdy se této skupině podařilo získat a zveřejnit osobní údaje tisíců členů strany, které následně rozeslali mnoha novinářským redakcím s připojenou zprávou pro politiky. Zpráva nebo spíše výzva se týkala obchodní dohody proti padělatelství ACTA, která v ČR zatím nebyla ratifikována. V posledních letech čelilo i mnoho dalších významných serverů útokům a i následným výpadkem, kdy byly postiženy např. servery jako Seznam, O2, T-Mobile, mimo jiné i některé zpravodajské a bankovní servery.

V dnešní době a to především vlivem technologického vývoje a změně smyslu útoků hackerů již takto obdobně velké útoky nebývají tak časté, resp. se dají označit za vzácné. Vše především kvůli několika faktorům a to především, že v minulosti šlo útočníkům více o prestiž, kdy chtěli dokázat napadeným cílům, že jejich znalosti jsou na daleko lepší úrovni a že oni jsou ti jedinci, kteří dokážou zničit nebo ohromit jejich velkou firmu. Zpravidla také platilo, že útočníci, jsou např. bývalí IT zaměstnanci dané společnosti nebo jiné konkurenční firmy, která tyto osoby např. nechtěla zaměstnat nebo s nimi spolupracovat. Získání nějakého zisku pro svoje obohacení tedy nebylo většinou pro tyto osoby prioritou. Naopak byli a jsou hackeři, kteří svoje znalosti využívají čistě pro svoje obohacení.

Z tohoto hlediska lze tedy hackery dělit na tyto skupiny:

- Hackery
- Crackery

[5] SMEJKAL, V., et al. *Právo informačních a telekomunikačních systémů*. Praha: C. H. Beck, 2001. 502-509 s.

Toto dělení je poněkud základní a lze jej ještě dále rozšířit. Další rozčlenění je tzv. kloboukové dělení, které zahrnuje i třetí alternativu, která je dle mého názoru i nejvýstižnější a nejčastější. Třetí varianta poukazuje na prolínání právě zmiňovaných jednotlivých skupin:

1. White hats česky „bílé klobouky“ jsou hackeři, kteří se sice dokáží nabourat do počítačové sítě a ukrást informace, nicméně tyto své znalosti používají jen k tomu, aby firmám a webovým stránkám pomohli lépe se zabezpečit.

2. Black hats v češtině „černé klobouky“, jsou hackeři, kteří využívají znalosti programování ke škodlivým účelům, například hanobení cizích webových stránek nebo kradení databází s osobními údaji uživatelů za účelem prodeje někomu dalšímu. Black hat hackerům se někdy říká i „crackeři“.[6]

3. „Grey hats“ se pohybují na pomezí obou skupin, jak již jejich název „šedé klobouky“ napovídá. Tato skupina byla zřejmě vytvořena proto, že předcházející skupiny spolu na mnoha místech interferují a rozdíl je jenom v přístupu k problému. Zároveň slouží jako doplňující prvek v taxonomii a obvykle je přechodným stadiem rodícího se hackera, který nemá ujasněn svůj budoucí úkol.

Toto dělení je odvozeno od klobouků hlavních hrdinů ve westernech. Obvykle kladný hrdina míval světlý nebo bílý klobouk, zatímco záporný hrdina se vyznačoval tmavou, nejčastěji černou barvou klobouku.[7]

Shrnutím předcházejících informací a základních charakteristik je možné vytvořit skupiny nejvýznamnějších hackerů:

- Kriminální hackeři neboli crackeři. Jejich motivací je zisk za každou cenu. Cíle zahrnují většinou servery velkých firem nebo institucí a často se jedná o organizované a izolované skupiny spojené s kriminálním podsvětím. Do této skupiny můžeme zařadit i individua zneužívající hackerské metody pro teroristické aktivity.

---

[6] OLSON, P. *Jsme Anonymous: uvnitř hackerského světa Anonymous, LulzSec a globální internetové vzpoury*. Praha: Práh, 2012. 490-494 s.

[7] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 54-55 s.

- Profesionální hackeři, které je možné rozdělit podle předcházející kloboukové typologie na „White hats“, „Grey hats“ a „Black hats“.

- Nespokojení zaměstnanci, kteří tvoří jednu z nejnebezpečnějších skupin hackerských aktivit.

- Ideologičtí hackeři patří k fanaticky zaměřeným skupinám internetových aktivistů, kteří používají internetu k šíření a prosazování svých politických nebo ideologických cílů. Jejich aktivity obvykle souvisí s nějakou významnou událostí ve světové politice nebo ekonomice. Často se označují jako „haktivisté“ a bývají zahrnováni do kyberteroristických skupin.

- Skripťáčci (skript kiddies) je hanlivý termín označující někoho, kdo by se rád považoval za black hat hackera, ale kdo zatím k napadání počítačových sítí používá jen známé a volně dostupné webové nástroje nebo skripty. Skripťáčci si mnohdy prostřednictvím hackování chtějí vydobýt víc respektu mezi kamarády.[8]

## 2.4 Způsoby napadení – škodlivé programy (malware)

Malware neboli škodlivý software je počítačový program určený ke vniknutí do nebo poškození počítačového systému. Výraz malware vznikl složením anglických slov „malicious“ (zákeřný) a „software“ a označuje jakýkoli počítačový program, jehož cílem je provádět nežádoucí činnosti či poškozovat oprávněného uživatele počítače. Pod souhrnné označení malware se zahrnují počítačové viry, počítačoví červi, trojské koně, spyware a adware a další. Malware má nepředstavitelné množství podob. Nejznámějším typem malwaru jsou asi počítačové viry. Označení virus se pro tyto programy používá proto, že se šíří svým vlastním kopírováním. Podobně fungují i červi. Mnohé typy

[8] OLSON, P. *Jsme Anonymous: uvnitř hackerského světa Anonymous, LulzSec a globální internetové vzpoury*. Praha: Práh, 2012. 493 s

malwaru jsou pojmenovány podle toho, co dělají, například spyware vysílá uživatelovi osobní údaje, např. může jít o čísla platebních karet.[9]

Malware je podle Ministerstva vnitra ČR souhrnný pojem pro jakýkoli software, který při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány nebo reagovat na konkrétní naprogramovanou spouštěcí událost, např. na okamžik, kdy oprávněný uživatel otevře zprávu v rámci elektronické pošty. V následující části bude uveden stručný přehled škodlivého softwaru.[10]

Rozdělení malware na jednotlivé druhy dnes není jednoduché. Aby byly škodlivé programy účinné, musí se neustále velmi rychle vyvíjet (stejný trik nikdy neplatí dvakrát). Kvůli stále lepšímu vývoji počítačové ochrany dnes velmi rychle vznikají zcela nové druhy malware nebo hybridy kombinující několik vlastností z různých skupin malware. Tyto vlastnosti brání jejich snadnému rozřazení. Jedno z možných rozdělení škodlivého softwaru:

- **Virus** - Tímto pojmem se označuje kód, který sám sebe replikuje a vkládá do jiných programů. Často jsou tímto termínem nesprávně označovány všechny druhy malware. Samotných virů je celá řada a dají se dělit podle různých kritérií. Jde o jakousi podsložku malware. Vir se může nekontrolovatelně rozšiřovat nebo po svém spuštění zahájit destrukční proceduru (poškození, změnu či zničení dat, degradaci funkce operačního systému, stahování dalšího malware atd.). Existují viry, které mohou zároveň plnit funkci trojského koně a vytvářet backdoor do napadeného systému. Počátek šíření počítačového viru může být distribuován v prostoru ohnisek, vytvořených na již kompromitovaných (zavirovaných) počítačích, což nesmírně urychluje celý proces šíření infekce.[11]

[9] GLENNY, M., KLIMÁREK, O. Dark market (Temný trh). Praha: Dokořán, 2013. 135-136s.

[10] *Základní definice, vztahující se k tématu kybernetické bezpečnosti.* [online]. Praha, 2009, [cit. 2017-02-12]. Dostupné z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.

[11] *Základní definice, vztahující se k tématu kybernetické bezpečnosti.* [online]. Praha, 2009, [cit. 2017-02-12]. Dostupné z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.

Viry lze ještě tedy dle kritérií dělit:

A. Podle umístění do paměti
    - Rezidentní
    - Nerezidentní
B. Podle cíle infekce
    - Spustitelné soubory (COM, EXE, BIN)
    - Boot virus
    - Klastrové viry
C. Podle chování virů
    - Rozmnožující se vir (červ)
    - Stealth vir – neboli neviditelný, maskující se vir
    - Polymorfní vir (mutující vir)
    - Trojské koně (destruktivní viry)[12]

- **Červ (Worm)** - Tento termín označuje kód, který se také šiří mezi počítači, ale buď běží pouze v operační paměti počítače, nebo se ukládá na disk do samostatných souborů, jejichž spuštění při startu počítače si zajistí vhodnou modifikací souborů řídících start počítače. Červ bývá často zaměňován za virus. Zejména kvůli jeho vlastnosti kopírování sebe sama. Od viru se však liší tím, že se rozšiřuje pomocí počítačových sítí.

- **Trojský kůň (Trojan)** - Na rozdíl od virů nebo červů nejsou trojští koně schopni sebereplikace. Často bývají považováni za užitečné programy, nicméně jejich hlavní činností je provádění tajných akcí na pozadí. Mohou například do systému stahovat další škodlivý software nebo otevřít zadní vrátka (backdoor) hackerovi. V posledních letech bývají často kombinovány s jiným druhem malware a mají další přidané funkce. Jednou z funkcí je i odesílání citlivých údajů na určená sběrná místa. Existují velice povedené nástroje, které

[12] POŽÁR, J. *Informační bezpečnost*. Plzeň: Aleš Čeněk s.r.o., 2005, 216-218 s.

spojí kód trojského koně s nosným programem a přibalí k němu instrukce pro rozbalování.[13]

- **Spyware -** Výraz Spyware je složenina dvou anglických slov „spy“ tedy špeh nebo špehovat a „software“ tedy program. Jak už název napovídá hlavním cílem spyware je špehování uživatelů. Přesněji řečeno, jde o sbírání dat o uživatelích a jejich následné odeslání autorovi spyware. Může se jednat o legální software, pokud uživatel souhlasí s poskytováním dat o sobě a své činnosti. V jiných případech je většinou považován za ilegální. Některé spyware programy odesílají pouze základní data, jako verze používaných programů apod., jiné ovšem mohou sbírat i stlačení jednotlivých kláves a kliky myší a tak odesílat i uživatelova hesla, čísla kreditních karet a další velmi citlivé údaje.

- **Adware -** Celým názvem: Advertising supported software. Jedná se o programy, ve kterých je nějakým způsobem zobrazena reklama. Do této kategorie většinou spadají programy s bezplatnou licencí, za které zobrazováním této reklamy platíme. V některých případech se adware instaluje jako doplněk k některému jinému programu, většinou se dá instalace tohoto doplňku odmítnout. Existují i varianty hybridů se spyware, které mohou odesílat data o uživateli pro možnost cílenější reklamy.

- **Rootkit -** Jako rootkit je možné označit kterýkoli prostředek, který má za úkol skrýt činnost prováděnou na operačním systému. Uživatel není běžnými prostředky schopen rootkity najít a odstranit. Velmi mnoho jiných druhů škodlivých programů dnes využívá vlastností rootkitů. Rootkity byly odvozeny od účtu pro správu unixových operačních systémů, který se jmenuje „root“. To ovšem neznamená, že rootkit lze použít pouze pro operační systém Unix. Od roku 1999, kdy Greg Hoglund vytvořil první známý rootkit určený pro Windows NT, jsou tyto nástroje široce používány a žádný operační systém před nimi není v bezpečí. Rootkit se skládá ze dvou částí, a to přenašeče a nákladu. Přenašeč zneužije nějaké bezpečnostní chyby nebo nepozornosti uživatele a

[13] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 67 s.

spustí náklad. Ten má u většiny moderních rootkitů obvykle podobu jaderného modulu, takže se přidá do jádra systému a začne s úklidem stop.[14]

## 2.5 Prevence a boj proti počítačové kriminalitě

Prevence v oblasti kyberkriminality hraje stejně velice důležitou roli jako před každým jiným druhem kriminalit. V rámci České republiky vzniklo několik projektů, které mají za úkol právě pomoci uživatelům bezpečně se pohybovat v síti internet a varovat je před současnými možnými hrozbami. Za zmínku stojí zcela určitě stránky www.bezpecnyinternet.cz a www.e-bezpeci.cz. Tyto stránky spolupracují s několika dalšími velkými subjekty a úřady, mezi které např. patří Microsoft nebo Policie ČR. Mají tedy za úkol veškeré dnešní uživatele od dětí až po seniory poučit, jaké na ně může v síti internet číhat nebezpečí a jak tomuto mají předejít či takovéto jednání odhalit.

Základními body pro „bezpečný pohyb“ v síti internet jsou:

- Chránit svůj počítač pomocí softwaru zabezpečení.
- Udržovat počítač v aktuálním stavu pomocí nejnovějších oprav a aktualizací.
- Bezpečné nakonfigurování svého počítače.
- Zvolení si silných hesel, která si uchováváme v bezpečí.
- Dodržování základní zásad pro pohyb na internetu (nepřipojujeme se na nedůvěryhodné servery, nestahujeme neověřené soubory, apod.)

Tento seznam by zcela určitě šlo rozvést o několik dalších důležitých bodů, jako použití kvalitního firewallu, nepoužívat funkci automatického ukládání hesel, nebo automatického dokončování, či vyvarovat se odesílání citlivých dat skrze internet, nebo používání ověřených certifikátů. Zcela určitě by bylo možné dále pokračovat, kdy dle

[14] *Základní definice, vztahující se k tématu kybernetické bezpečnosti.* [online]. Praha, 2009, [cit. 2017-01-23]. Dostupné z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.

mého názoru pro základní bezpečný pohyb v síti internet lze považovat pět shora uvedených bodů.

V současné době se Česká republika snaží proti počítačové kriminalitě bojovat a to ve spolupráci s evropskou unií. Za zmínku stojí zcela určitě schválení zákona č. 181/2014 Sb., Zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), účinného od 1. 1. 2015 a jeho poslední novelizaci č. 104/2017 účinnou od 1.7.2017, který jasně stanovuje a určuje pravidla pro působení v síti internet v rámci České republiky.

V České republice působí skupina CERT (Computer Emergency Response Team). Jde o skupinu, která zveřejňuje velké množství bezpečnostních rad, k tomu dále zodpovídá za zprávy o internetových průlomech a velkém množství oznámení o zranitelných místech v různých systémech. Další činností skupiny CERT je 24 hodinová telefonická podpora, která poskytuje velmi důležité technické rady lidem, kteří se dostali do problémů související s narušením jejich zabezpečení. Na jejich webových stránkách jsou k dispozici důležité nové i starší informace o bezpečnosti. Navíc tato skupina vydává pravidelné roční zprávy, které poskytují vynikající statistický náhled na danou problematiku.[15]

Lze říci, že Česká republika se oproti jiným státům evropské unie a vůbec ostatním státům světa, snaží velice aktivně zapojit do boje proti počítačové kriminalitě, protože Česká republika stojí za názorem, že nelze počítačovou kriminalitu podceňovat a brát její současnou činnost na lehkou váhu.

[15] *Národní centrum kybernetické bezpečnosti*. [online]., [cit. 2017-05-26]. Dostupné z WWW: < https://www.govcert.cz/cs/vladni-cert/govcert-cz/>.

# 3 Legislativa

Současný stav české i evropské legislativy v oblasti informačních a komunikačních technologií není důkladně připraven na moderní nástroje kriminálního podsvětí. Jednotlivé trhliny jsou "záplatovány" případ od případu a celkové koncepční pojetí této oblasti se teprve rodí. O moc lépe na tom není ani legislativa zámořská, která však díky své odlišné právní metodice, spočívající na právních precedentech a dodatcích ústavy, má pro jednotlivé incidenty již své vzory a nekompromisní trestní taxy. [16]

Na přelomu století vedla potřeba harmonizovat právní úpravy na mezinárodní úrovni k vytvoření Úmluvy o počítačové kriminalitě. Jedinečnost této úmluvy se projevuje v její komplexnosti a v okruhu signatářů. Úmluva se zabývá nejen definicemi některých trestných činů v kyberprostoru, ale obsahuje též závazky k přijetí procesních opatření nezbytných k zajištění důkazů, odhalení a potrestání pachatelů, jakož i závazky v oblasti mezinárodní spolupráce. Poměrně dlouhou dobu trvalo, než vůbec došlo k ratifikaci této úmluvy i pro Českou republiku, neboť Česká republika nesplňovala některé právní normy této Úmluvy o počítačové kriminalitě. Až po zavedení příslušných právních úprav došlo v roce 2013 k ratifikaci této úmluvy, kdy se tak Česká republika zařadila mezi více jak 40 zemí, pro které je tato úmluva závazná. Jde především o evropské země, ale například i o USA či Japonsko.[17]

## 3.1 Legislativa v ČR

Nejčastěji uplatňované zákony z oblastí informatiky a telekomunikací jsou:

- Občanský zákoník - č. 89/2012 Sb.,[18] je hlavním předpisem pro vymezení vlastnického práva a zároveň upravuje a definuje právnickou a fyzickou osobu.

[16] GŘIVNA, T., POLČÁK, R., ed. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. 162 s.

[17] *Počítačová kriminalita: Mezinárodní úmluva je konečně závazná i pro Česko.* [online], [cit. 2017-01-23]. Dostupné z WWW: < https://www.patria.cz/pravo/2694193/pocitacova-kriminalita-mezinarodni-umluva-je-konecne-zavazna-i-pro-cesko.html>.

[18] AION CS. *Předpis č. 40/1964 Sb.: Občanský zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2017-02-12]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/1964-40>.

- Zákon o elektronických komunikacích č. 127/2005 Sb.,[19] obsahuje a upravuje dodržování telekomunikačního tajemství a zabývá se nezákonným chováním v prostředí počítačové sítě.
- Autorský zákon č. 121/2000 Sb.,[20] určuje, že dílo, tedy i program se stává duševním vlastnictvím a je tak i chráněn (např. jako literární dílo).
- Zákon o ochraně osobních údajů č. 101/2000 Sb.,[21]
- Trestní zákoník č. 40/2009 Sb.,[22] ve své poslední úpravě a s ním související předpisy by měly sloužit jako represivní nástroj v okamžiku prokázaného porušení některého zákonného předpisu, které spadá do sféry trestní odpovědnosti. Bohužel v těchto případech je mnohdy výklad zákona takový, že některé typické kriminální delikty v počítačovém prostředí se jenom velmi obtížně začleňují do stávající osnovy zákona. Rovněž dokazovací procedura je v těchto případech většinou složitá, neboť procesní dokazování je stavěno na klasických důkazních metodách.

### 3.2 Definice počítačové kriminality

Počítačová kriminalita (cyber-crime, kyberzločin): Je trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat) nebo pouze některá z jeho komponent, případně vetší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti. Často se pojem počítačová kriminalita používá i pro tradiční formy kriminality, u níž byly počítače nebo počítačové sítě použity, aby ji usnadnily. Určujícím operacionálním elementem je

---

[19] AION CS. *Předpis č. 127/2005 Sb.: Zákon o elektronických komunikacích.* [online]. AION CS, © 2010 - 2013, [2017-02-12]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/2005-127>

[20] AION CS. *Předpis č. 121/2000 Sb.: Autorský zákon.* [online]. AION CS, © 2010 - 2013, [cit 2017-02-12]. Dostupné z WWW: <http:// http://www.zakonyprolidi.cz/cs/2000-121 >.

[21] AION CS. *Předpis č. 101/2000 Sb.: Zákon o ochraně osobních údajů.* [online]. AION CS, © 2010 - 2013, [cit 2017-02-12]. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2000-101>.

[22] AION CS. *Předpis č. 40/2009 Sb.: Zákon trestní zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2017-02-12]. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2009-40>.

přitom vždy způsob zneužití výpočetní techniky, vzhledem k jejím specifickým vlastnostem a dominantnímu postavení mezi věcnými komponentami způsobu páchání konkrétního trestného činu. [23]

Definicí internetové kriminality jako je tato, je několik, avšak většina z nich vychází z podstaty, která je shora uvedená. Podle materiálu OSN, které se zabývá počítačovou kriminalitou, jsou jejím obsahem „*Tradiční zločinné aktivity jako krádež, podvod nebo padělání, tedy činy trestné ve většině zemí na světě. Počítač rovněž tvoří prostředí pro nové činy spočívající ve zneužití počítačů, které jsou nebo by měly být ve své podstatě trestné*“ Ve stejném materiálu se snaží OSN odlišit dva základní případy – náhodné a neúmyslné zneužití počítače, které vede ke vzniku škody, a úmyslné použití počítače jako nástroje nebo předmětu kriminálního deliktu.[24]

Internetovou kriminalitu lze rozdělit do dvou hlavních kategorií a to na majetkovou trestnou činnost, kde úmyslem pachatele je se obohatit, lze sem tedy zařadit především podvody, krádeže (podvodné emaily s falešnými výzvami, exekucemi, podvodné inzeráty, krádeže platebních informacích a následná krádež finančních prostředků) a ostatní trestnou činnost, kde jde hlavně o porušování autorských práv (softwarové pirátství), různé urážky, slovní napadání, které však může vyústit až v tzv. „stalking“, neboli nebezpečné pronásledování, rovněž sem, spadá i např. šíření pornografie.

Prof. Smejkal a kolektiv rozděluje počítačovou kriminalitu při určitém zjednodušení do dvou základních skupin:

- Delikty, kde počítač, program, data, informační systém apod. jsou nástrojem trestné činnosti pachatele,
- delikty, kde počítač, program, data, informační systém atd. jsou cílem zločinného útoku, přičemž se může jednat o tyto trestné činy:
    - fyzický nebo logický útok na počítač nebo komunikační zařízení,

[23] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 269-274 s.

[24] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 91 s.

- neoprávněné užívání počítače nebo komunikačního zařízení,
- neoprávněné užívání nebo distribuci počítačových programů,
- změnu v programech a datech, okrajově i v technickém zapojení počítače nebo komunikačního zařízení,
- neoprávněný přístup k datům, získávání utajovaných informací (tzv. počítačová špionáž) nebo jiných informací o osobách (osobní údaje),
- trestné činy, předmětem jejichž útoku je počítač jako věc movitá.[25]

Rada Evropy dělí počítačovou kriminalitu do čtyř oblastí:

- Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů (neoprávněný přístup, neoprávněné odposlouchávání, narušování dat, narušování systémů, zneužívání zařízení).
- Trestné činy se vztahem k počítači (počítačový podvod, padělání počítačem).
- Trestné činy se vztahem k obsahu počítače (dětská pornografie).
- Trestné činy související s porušováním autorského práva a souvisejících práv.

Dále Rada Evropy v rozšířila tento okruh o čtyři skutkové podstaty xenofobních a rasově motivovaných deliktů. Tyto delikty přísluší pod "Trestné činy se vztahem k obsahu počítače".[26]

[25] SMEJKAL, V.,SOKOL, T.,VLČEK, M. *Počítačové právo.* Praha, C. H. Beck/SEVT 1995

[26] SMEJKAL, V.,SOKOL, T.,VLČEK, M. *Počítačové právo.* Praha, C. H. Beck/SEVT 1995

### 3.3 Majetková a ostatní trestná činnost

Do majetkové trestné činnost v rámci počítačové kriminality řadíme, jak již bylo poukázáno shora, především různé podvody a krádeže. Jde především o vylákávání peněz z uživatelů prostřednictvím podvodných emailů a inzerátů nebo napadení jejich počítače a získání tak přístupu k jejich elektronickým bankovním účtům. Majetková trestná činnost se tak stala bohužel nedílnou součástí internetu, neboť vzhledem k jeho vlivu, rozmachu a především možnostem umožnuje pachatelům takovéto jednání v této síti vykonávat i přes veškerou snahu společnosti tomu zamezit.

Do ostatní trestné činnosti páchané prostřednictvím sítě internet lze především zařadit porušování autorských práv, známé jako softwarové pirátství, nebezpečné pronásledování a šíření pornografie. Jedná se zcela jistě o ty nerozšířenější druhy kriminality páchané v této síti, které nejsou ve své povaze majetkově zaměřené.

# 4 Způsoby provedení počítačových kriminalit

Pachatelé si postupem času vytvořili několik způsobů, jak se prostřednictvím sítě internet mohou nelegálně obohacovat. Mezi nejčastější způsob, se kterým se můžeme setkat, lze zařadit různé podvodné nabídky a inzeráty. Tento druh podvodů se stal na internetu tím nejběžnějším, se kterým se může jedinec setkat. Na každé webové stránce zabývající se inzercí, narazí člověk na několik desítek až stovek inzerátů a nabídek, které mají podvodný charakter. Jedná se o typické znaky jako velmi nízká cena oproti konkurenčním nabídkám, nesrozumitelná nabídka (špatná čeština), platba předem, nemožnost osobní prohlídky a předání.

Dalším způsobem obohacení se staly s vývojem internetu podvodné emaily a viry. V podobě podvodných emailů se tyto buď snaží využít pochybností jedince a v podobě falešné pohledávky se tak snaží z uživatele vylákat peníze nebo přiloženým odkazem pod záštitou banky uživatele vylákat jeho přístupové údaje k jeho bankovnímu účtu.

Počítačové viry jsou tou nejzákeřnější formou. Uživatel často ani neví o jejich přítomnosti ve svém zařízení a mnohdy tedy ani netuší, že druhá strana získává důležité informace jako citlivá data, přístupové údaje a hesla.

## 4.1 Podvodné emaily

Dalším způsobem obohacení je rozesílání tzv. podvodných emailů. Ty mají různé podoby a obsahy. Mezi nejrozšířenější podvody touto cestou patří rozesílání různých výzev k uhrazení pohledávky nebo exekuce, kdy se pachatelé vydávají za nějaký exekutorský úřad nebo za nějakou společnost, která vymáhá pohledávky, a požadují uhrazení jimi požadované částky, čímž zaručují dotyčnému mimosoudní vyrovnání. Vše působí velmi věrohodně, hlavičky dokumentů, text, jména pracovníků bývají zkopírovány z originálních dokumentů, pouze jsou změněny údaje o dlužníkovi, případně společnost, které je dlužná částka dlužena. Opět zde působí u spousty lidí tzv. psychická stránka, kdy se spousta lidí zalekne a raději dlužnou částku okamžitě uhradí, aniž by si ověřovali, jestli skutečně něco někde dluží.

Dále se v současné době velmi rozšířily podvodné emaily, kde se pachatelé vydávají za banku uživatele a snaží se tak získat přístupové údaje k jejich elektronickému bankovnictví. Největší problém s tímto typem podvodů měla Česká spořitelna, a.s. Jejich zákazníci obdrželi email, který se vydával za servis České spořitelny, kdy vyzýval své majitele k jakési aktualizaci svého účtu, neboť jim údajně brzy vyprší platnost jejich přístupových údajů, a proto je zapotřebí je aktualizovat. Email obsahoval hlavičku České spořitelny a výzvu s těmito slovy, podepsáno vedoucí pracovnicí České spořitelny a odkazem k obnovení účtu. Po kliknutí na přiložený odkaz byl uživatel však přesměrován na zcela jiné stránky a to v posledním zjištěném případě na rodrigojucarep.com.br. a nikoli na servis24.cz, které využívá právě Česká spořitelna. Méně zkušený uživatel, který si tohoto nevšiml, vyplnil formulář, kam zadal veškeré přihlašovací údaje, včetně mob. čísla pro ověření a tím tak okamžitě zpřístupnil finanční účet pachatelům. (Viz obrázek 1,2)

*Obrázek č.1 Ukázka podvodného emailu České spořitelny*[27]


**From:** Česká spořitelna [mailto:oneillcm@slu.edu]
**Sent:** Monday, January 05, 2015
**To:** [redacted]
**Subject:** Aktualizace účtu - Česká spořitelna!!

ČESKÁ SPOŘITELNA

UKÁZKA PODVODNÉ ZPRÁVY

Aktualizace účtu - Česká spořitelna

Vážený zákazníku,

Chtěli bychom Vám zdůraznit, že přístup do Vašeho internetového bankovnictví již brzy vyprší. Aby bylo možné i nadále využívat on-line bankovnictví, žádáme Vás o potvrzení svých údajů pomocí odkazu níže.
Pro aktualizaci svého on-line bankovního účtu klikněte zde

Bankovní účet bude automaticky obnoven, poté Vás bude kontaktovat jeden z našich zaměstnanců.

S pozdravem,
Klára Pačesová,
Agentka zákaznického servisu.

[27] Novinky.cz: *Snaží se získat citlivé informace, podvod poznají jen pozorní* [online].,[cit. 2017-03-01]. Dostupné z WWW: <https://www.novinky.cz/internet-a-pc/bezpecnost/358664-snazi-se-ziskat-citlive-informace-podvod-poznaji-jen-pozorni.html/>.

*Obrázek č.2 Podvodné stránky po přesměrování*[28]


Banky svých klientů opakovaně provádějí medializaci těchto podvodů a upozorňují své klienty, že by nikdy od nich takovéto údaje nevyžadovali cestou emailu, a proto se vždy v takových případech jedná o podvod.

Tento typ útoku nazýváme „Phishing“. Jde o podvodný způsob, jak prostřednictvím internetu získat citlivé údaje (hesla, čísla kreditních karet, apod.). Jedná se o rozesílání e-mailových zpráv, které nabádají adresáta k zadání jeho osobních údajů na falešnou webovou stránku. Ta bývá téměř totožná s tou oficiální. Často zneužívána bývají zejména přihlašovací okénka internetového bankovnictví. Uživatel v dobrém úmyslu do okénka zadá své přihlašovací údaje (jméno a heslo) a tím nevědomky poskytne své údaje útočníkům, kteří následně z jeho účtu vykrádají peníze. Dále se může jednat například o zasílání různých zpráv o výhrách v loterii, apod.

[28] Novinky.cz: *Snaží se získat citlivé informace, podvod poznají jen pozorní* [online].,[cit. 2017-03-01]. Dostupné z WWW: <https://www.novinky.cz/internet-a-pc/bezpecnost/358664-snazi-se-ziskat-citlive-informace-podvod-poznaji-jen-pozorni.html/>.

Tyto internetové podvody bývají detailně promyšlené a mnohdy zahrnují též psychosociální aspekt – snahu o vyvolání důvěry, možnost získání významného profitu nebo naopak snadné vyvinění se z nastíněné nezákonné činnosti a často pak také časovou tíseň. Využívají například výhodné, časově omezené „nabídky".

Poškozený nemusí zprvu tušit, že se stal obětí trestného činu. Zjistí to, kupříkladu, až když se mu zablokuje počítač, dojde k neoprávněnému čerpání finančních prostředků z účtu a podobně. [29]

Pro bezpečný pohyb v rámci internetového bankovnictví lze stanovit několik hlavních faktorů, kdy při jejich dodržování lze brát transakce za bezpečné.

První bariérou proti zneužití je způsob, jakým se do internetového bankovnictví přihlašujeme. Jako základní prostředek přihlášení se většinou používá klientské ID (číslo) a heslo. Také při autorizaci pokynů bance, tzn. potvrzení platebních příkazů, zřízení trvalých příkazů, změnách v nastavení internetového bankovnictví, se používají různé způsoby zabezpečení. Další nabízenou metodou je také autorizace kódem z TAN (tabulka autorizačních čísel) nebo autorizace jednorázovým kódem zaslaným bankou klientovi v zabezpečené SMS. Některé banky nabízejí klientům také možnost autorizovat transakci do určitého limitu pouhým heslem. Naprosto kompletní zabezpečení pak poskytuje čipová karta s klientským certifikátem - prostřednictvím čtečky připojené k počítači tak lze jednoznačně rozpoznat uživatele.[30]

Dále může uživatel disponovat dalším druhem zabezpečení, jako je grafická klávesnice, možnost zablokování účtu, možnost kdykoli a jakkoli často měnit heslo, případně zasílání informací o transakcích přijatých bankou. K bezpečnosti internetového bankovnictví přispívá i fakt, že výše prostředků, které lze denně převést prostřednictvím internetu, je omezená určitým maximálním limitem, a pro vyšší částky je potřeba např. provést autorizaci klientským certifikátem.

Přestože všechna tato bezpečností opatření se důmyslně překrývají a jsou na první pohled neprolomitelná, zůstává tu rizikový faktor, a tím je sám uživatel. Na

---

[29] Počítačová kriminalita*: Pomoc obětem TČ*. [online], [cit. 2017-04-01]. Dostupné z WWW: < http://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx>.

[30] Bezpečný internet.cz: *Internetové bankovnictví* [online].,[cit. 2017-04-04]. Dostupné z WWW: < http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/bezpecnost.aspx>.

uživateli samotném je, aby dodržoval bezpečnostní doporučení daná bankou - to je zejména ochrana bezpečnostních údajů, ochrana účtu a dodržování bezpečnostních pravidel. Přihlašovací údaje se zásadně nikomu nesdělují a to ani rodinným příslušníkům. Další klíčovou zásadou je používat jen počítače, které známe. Není doporučováno obsluhovat své finance z veřejně dostupného počítače (ve škole nebo internetové kavárně), kde se střídají neznámí uživatelé. Takové počítače mohou obsahovat škodlivé programy, které umožní zkopírování přihlašovacích údajů včetně hesla.

K celkovému bezpečí patří i maximální ochrana osobního počítače používaného pro internetové bankovnictví. To znamená udržování aktuálních bezpečnostních oprav u operačního systému, zapnutí antivirové kontroly (včetně pravidelně aktualizovaných souborů) a v neposlední řadě i aktivování a správné nastavení brány firewall v operačním systému.[31]

## 4.2 Počítačový malware

Další kategorií nelegálního obohacování prostřednictvím internetové sítě je tzv. „malware“, ve společnosti spíše běžně označován laicky jako „viry“. Z odborného hlediska by se měl spíše užívat pojem malware. Výraz malware vznikl složením anglických slov „malicious“ (zákeřný) a „software“ (program) a popisuje záměr autora takového programu spíše než jeho specifické vlastnosti. Pod souhrnné označení malware se zahrnují především počítačové viry, trojské koně, spyware a adware. Přesto se mezi běžnými uživateli ujal spíše pojem vir, který se začal hojně užívat pro všeobecné napadení počítače, ať už se jedná o jakoukoliv modifikaci napadení. Za malware lze vlastně označit jakýkoliv program, který se dokáže sám šířit bez vědomí uživatele. Malware bývá naprogramován tak, aby využil zjištěné chyby v systému koncových uživatelů a pomocí sítě se dále šířil a napadal uživatele, kteří mají stejnou chybu v systému. Jde např. o systémy, kde uživatelé neprovádí pravidelné aktualizace nebo používají nelegální kopie

[31] Bezpečný internet.cz*: Internetové bankovnictví* [online].,[cit. 2017-04-04]. Dostupné z WWW: < http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/bezpecnost.aspx>.

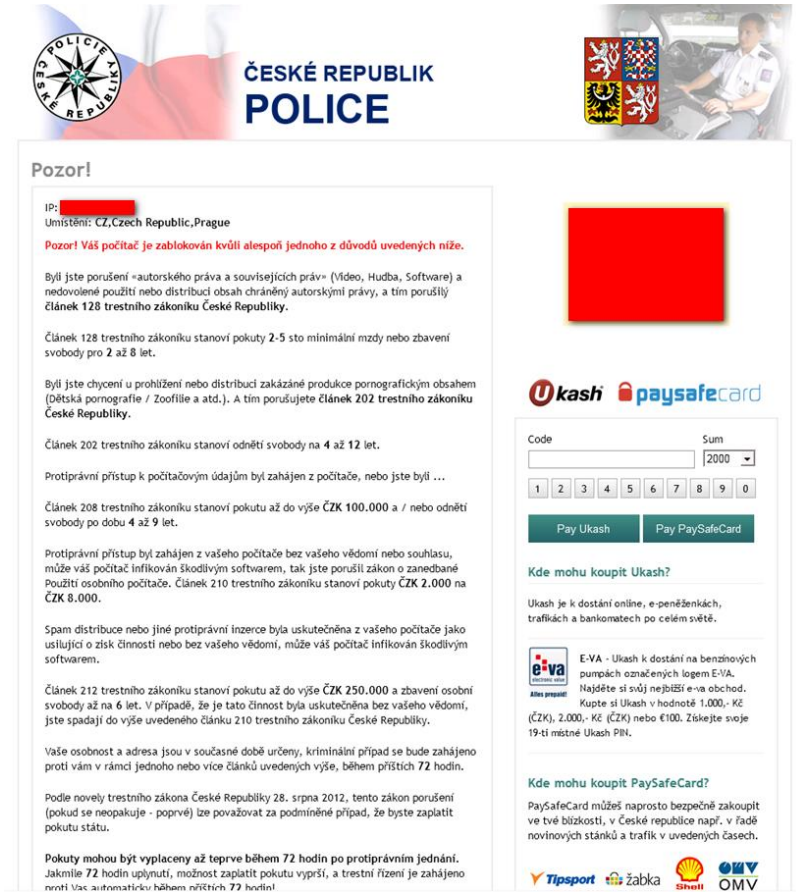
systému apod. Malware poté podle své povahy má za úkol napadnout cílový počítač a zjistit např. citlivé údaje, přihlašovací hesla, nebo zablokovat systém atd.[32]

Nejznámějším druhem malwaru je pravděpodobně ransomware - „Win32/Ransom“, který každý zná, neboť se tento škodlivý program vydává za Policii České republiky. Jedná se vlastně o trojského koně což je typ malwaru. Hlavním znakem trojského koně je, že nedokáže sám infikovat další počítače nebo programy svojí kopií. Existují však počítačoví červi, kteří na napadeném počítači instalují právě trojské koně nebo vytvářejí trojské koně z programů, které se v napadeném systému nacházejí.

Tento tedy tzv. „ransomware“ zablokuje koncový počítač a to tak, že znemožní přístup k osobním datům a zobrazí pouze úvodní obrazovku s výzvou, vydávající se za Policii České republiky, kdy sděluje, že počítač byl použit k nelegálním účelům, za což hrozí trestní sazba odnětí svobody nebo uložení pokuty. Dále je zde uvedeno, že v případě uhrazení stanovené pokuty (zpravidla jde o částku v rozmezí 1.000,-Kč až 2.000,- Kč) bude věc vyřešena touto cestou a počítač bude odblokován. Obrazovka nabízí zaplacení pokuty pomocí služeb „paysafecard“, což je jeden ze systému placení na internetu. Jak je vidět na obrázku č.3, výzva obsahuje spousty gramatických chyb. Odkazy na trestní zákoník a citované paragrafy jsou rovněž nepravdivé. V zabarvených červených polích je IP adresa uživatele a fotografie uživatele, je-li počítač vybaven web kamerou.

[32] CRAIG, P., HONICK, R. *Softwarové pirátství bez záhad*. Přeložil Tomáš HLAVÁČ. Praha: Grada, 2008. 22-102 s.

*Obrázek č.3 Vzor úvodní stránky viru*[33]




Napadení tímto virem není postihnuta jen Česká republika. Tento trojský kůň má mnoho modifikací a jazykových verzí, kdy jím bylo napadeno mnoho počítačů po celém světě. I přesto, že již bylo na tento vir několikrát mediálně upozorňováno, Police ČR upozorňovala, že se jedná o vir „trojského koně“, kdy po aktivaci upozorní dotyčného uživatele, že byl jeho počítač Policií České republiky zablokován, kdy tedy zdůvodnění - je porušování autorských práv, nakládání s materiály s dětskou pornografií či šíření spamu. Součástí těchto upozornění je i nabídka uživateli o možnosti složení kauce v podobě zaplacení pokuty a uživateli bude poté počítač odblokován.

Jednání pachatelů tedy spočítá v šíření počítačového škodlivého kódu spolu s neoprávněným podvodným vylákáním finančních prostředků. Policie ČR uváděla, že nelze uvedeným způsobem realizovat zákonná opatření směřující k případným

[33] Novinky.cz: *Váš počítač zablokovala policie varuje virus a žádá peníze* [online].,[cit. 2017-03-01]. Dostupné z WWW: < https://www.novinky.cz/internet-a-pc/280892-vas-pocitac-zablokovala-policie-varuje-virus-a-zada-penize.html/>.

pachatelům trestných činů. Navíc neexistuje ani žádný právní titul, který by umožňoval deklarovaným způsobem po zaplacení tzv. pokuty, eliminovat úkony trestního řízení, i přesto se opět najde mnoho jedinců, kteří požadovanou částku uhradí.[34]

### 4.3 Porušování autorských práv (softwarové pirátství)

Porušování autorských práv, v internetové síti známé jako softwarové pirátství, neboli slangově „warez“, lze definovat jako nelegální nakládání s autorským dílem v rozporu s jeho autorským právem. Softwarové pirátství lze rozdělit podle druhu a to na počítačové hry, software, filmy a hudba. V době, kdy internet nebyl ještě takového rozmachu jako dnes, bylo šíření filmů, hudby a softwaru prováděno pomocí paměťových nosičů (CD, DVD). V dnešní době se již s takovým šířením moc nesetkáme, neboť roli šíření převzal internet.

Typickým způsobem šíření warezu je získání softwaru, filmu atd. před jeho oficiálním vydáním a to buď za využití nějakého kontaktu ve firmě, která očekávané dílo vydává, nebo např. odcizením skrze internet, napadení počítače vývojáře a stažením jeho díla. Posléze se takto získaného materiálu ujme programátor (cracker), který odstraní ochranu programu a umožní jeho spuštění. Následně již jen takto upravený software na sdílí na internetu, především na tzv. P2P sítí, kde dojde během několika hodin k masivnímu rozšíření po celém světě. P2P sítě (z ang. Peer to peer, čes. Rovný s rovným, neboli klient s klientem) je druh sítí, kde komunikují klienti sami přímo se sebou a nikoliv přes nějaký server. Jde tedy čistě o výměnné sítě, kde si uživatelé mezi sebou vyměňují různá data. Vzhledem k tomu se tyto sítě staly hlavním místem pro šíření nelegálního softwaru. Mezi nejznámější takovéto sítě patří např. Torrent, eDonkey, eMula, DC++ a další. Posléze se software dostane i na tzv. FTP úložiště známé jako uloz.to, edisk.cz, ze zahraničních např. rapidshare.com, megaupload.com a hellshare.com, kdy tyto stránky a obsah jsou uživatelům běžně dostupnější než z P2P sítí.[35]

---

[34] Policie.cz: *Varování před počítačovým virem* [online].,[cit. 2017-03-01]. Dostupné z WWW: < http://www.policie.cz/clanek/varovani-pred-pocitacovym-virem.aspx/>.

[35] CRAIG, P., HONICK, R. *Softwarové pirátství bez záhad*. Přeložil Tomáš HLAVÁČ. Praha: Grada, 2008. 35-37 s.

Softwarové pirátství je tedy synonymem pro neoprávněné užívání softwaru, které je chráněno autorskými právy. K pirátství může dojít jak např. při kopírování, stahování, sdílení či prodeji softwaru. Mezi formy pirátství patří i instalace více kopií softwaru, než umožňuje zakoupená licence. Většina lidí si neuvědomuje, že při nákupu softwaru si nekupují vlastní software (program), ale jen licenci na jeho užívání. Tato licence nám pak tedy určuje, jakým způsobem lze se softwarem nakládat - např. kolikrát jej lze nainstalovat, apod.[36]

S používáním nelegálního softwaru jsou spojena i tato rizika:

- **Riziko trestního postihu za používání nelegálního softwaru**: Používáním nelegálně nabytého softwaru se vystavujete možnosti stíhání za přestupek či trestný čin s následnými sankcemi, které mohou mít podobu peněžitého trestu, trestu propadnutí věci, trestu odnětí svobody až na 5 let podle rozsahu trestného činu. V případě podnikatelů a firem jsou neopomenutelné i doměrky příslušných daní od finančních úřadů, penále z daňových nedoplatků, pokuty, eventuálně pak sankce vyplývající ze živnostenského zákona.

- **Riziko ztráty dat**: V nelegálních programech, u nichž nemáte záruku jejich původu, se mohou vyskytovat chyby, které mohou vést k vymazání části nebo všech vašich dat. Představte si, že takto přijdete o důležité dokumenty, fotografie či videa.

- **Riziko virové nákazy počítače**: Instalací nelegálního programového vybavení z nedůvěryhodných zdrojů se vystavujete nebezpečí nákazy vašeho počítače počítačovým virem. Následné náklady související s jeho odstraněním mohou přesáhnout cenu originálního softwaru.

- **Riziko finanční ztráty**: Pokud máte v počítači uložené citlivé osobní informace nebo používáte počítač k přístupu na váš bankovní účet, hrozí v případě používání neověřeného nelegálního softwaru průnik do vašeho počítače a zneužití informací s možností přístupu cizí osoby na váš bankovní účet. Vzniklá ztráta může být mnohonásobně vyšší než cena legálního softwaru.

[36] Bezpečný internet.cz: *Softwarové pirátství* [online].,[cit. 2017-04-04]. Dostupné z WWW: < http://www.bezpecnyinternet.cz/pokrocily/stahovani-souboru-programu/softwarove-piratstvi.aspx/>.

- **Riziko ztráty soukromí**: Nelegální software může obsahovat zadní vrátka, která umožní cizí osobě přístup do vašeho počítače. Tato osoba může sledovat veškeré aktivity, jež vy nebo vaši rodinní příslušníci na počítači provádíte, a informace, které takto získá, může zneužít.

- **Riziko nemožnosti aplikovat bezpečnostní a funkční aktualizace**: Výrobci originálního softwaru uvolňují v pravidelných intervalech aktualizace, které zvyšují bezpečnost softwaru a zlepšují jeho funkčnost. V případě nelegálních programů je možnost aplikovat tyto aktualizace omezena nebo zcela znemožněna.[37]

V Česku a i ve většině západních zemích je jakákoliv tvorba, kopírování, či distribuce nelegální, zahrnuje tedy i běžné stahování autorských děl, ovšem výjimkou mohou být však softwary či nějaké databáze, které mají sloužit pro vlastní, tedy soukromou, osobní potřebu. V těchto případech by se jednalo o legální užívání. Nelegální je především šíření, což znamená další sdělování, distribuování pro veřejnost takových děl, kde nedošlo k povolení autora. Takové jednání je dle autorského zákona trestný čin, kdy se tedy může jednat o Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi, § 270 zák. č.40/2009Sb., trestní zákoník, který se trestá odnětím svobody až na dvě léta, nebo na šest měsíců až pět let, pokud tak pachatel konal ve značném rozsahu, nebo peněžitým trestem nebo propadnutím věci.[38]

Lze tedy říci, že v České republice je zákon nastaven tak, že samotné použití cizího autorského díla, bez jeho souhlasu je zcela legální, kdy hovoříme např. o stažení filmu a jeho zhlédnutí pro vlastní potřebu, kdy tedy tímto není zákon porušen, přestože třeba bylo dílo, resp. film volně šířen, což již je v rozporu s českými právními normami.

[37] Bezpečný internet.cz: *Softwarové pirátství* [online].,[cit. 2017-04-04]. Dostupné z WWW: < http://www.bezpecnyinternet.cz/pokrocily/stahovani-souboru-programu/softwarove-piratstvi.aspx/>.

[38] SMEJKAL, V., et al. *Právo informačních a telekomunikačních systémů*. Praha: C. H. Beck, 2004. 380-389 s.

## 4.4 Podvodné internetové inzerce

Podvodné nabídky, inzerce a prodeje jsou zcela jistě jednou z nejrozšířenějších majetkových trestných činností, které jsou v České republice prostřednictví sítě internet páchány. Pachatelé využívají masivních nabídek, které jsou na stránkách zabývající se inzercí a tím využívají i prostoru a možností anonymity, kterou jim do jisté míry internet přináší. V České republice tato kriminalita zcela jistě nejvíce postihuje internetové portály jako: www.bazos.cz, www.sbazar.cz a www.aukro.cz, které patří k největším stránkám zabývající se bazarovým prodejem.

Pachatelé se v inzercích zaměřují na zboží, které bývá často a velmi hodně žádané, takže se jedná především o elektroniku, kdy se nejčastěji setkáme s podvody s nabídkami mobilních telefonů, herních konzolí, počítačů, atd. Pachatelé vždy využívají psychologického nátlaku, kdy se nabídka vždy jeví jako velmi výhodná, oproti konkurenčním nabídkám je cena o poznání nižší, stav zboží je vždy prezentován jako „TOP“, dodání zboží obratem, zboží bývá zpravidla v záruce je v kompletním balení včetně příslušenství. I když kupující osoba má podezření, zpravidla se pokusí o kontaktování inzerujícího, kdy tento odpovídá obratem a vždy argumentuje nějakým logickým odůvodněním, proč zboží prodává. Tento krok však v kupujícím zvedne důvěru a přistoupí na koupi zboží. Vše bývá zpravidla podpořeno zprávami od prodávajícího ve stylu „ozvalo se mi již několik zájemců, prosím rychle se rozhodněte“ apod. Tyto všechny kroky vzbudí v jedinci snahu jednat rychle a právě bez uvážení, čehož využívá pachatel. Kupující aby nepropásl jedinečnou nabídku, přistupuje na zaslání peněz za zboží tzv. předem a to na předem domluvený účet. Do doby než požadovaná částka dorazí na účet, pachatel stále komunikuje a přesvědčuje kupujícího o odeslání prodávaného zboží. Po připsání částky na účet se stává pachatel obratem nekontaktní.

Podvodníci často a rychle mění nabídky, používají různé fotografie nabízeného zboží (zpravidla již někde na internetu prezentované), rovněž mění svá jména a kontaktní údaje jako je především email a telefonní spojení. Dále využívají toho, že cenu nabízeného zboží často uvádějí do hranice 5.000,-Kč a to ze dvou hlavních důvodů.

- Jsou srozuměni, že vzniklá škoda, která nepřesáhne 5.000,-Kč, není trestným činem, ale přestupkem a jejich postih je v případě odhalení minimální.
- Spoléhají na to, že poškozený vzhledem k často nižší částce, nebude chtít vůbec podvodné jednání řešit a oznamovat jej na Policii ČR a postupovat tak dlouhé úřední řízení.

Tímto jednáním tak pachatelé balancují nad trestně právní rovinou a to dle výše škody, kdy se zpravidla může jednat o přečin Podvod podle ust. § 209 tr. zákoníku a nebo o Přestupky proti majetku podle ust. § 50 přestupkového zákona.

Při této trestné činnosti bývá zpravidla hlavním vodítkem k pachateli číslo bankovního spojení, které uvádí pro úhradu zboží.

### 4.5 Podvodné zasílaní SMS zpráv

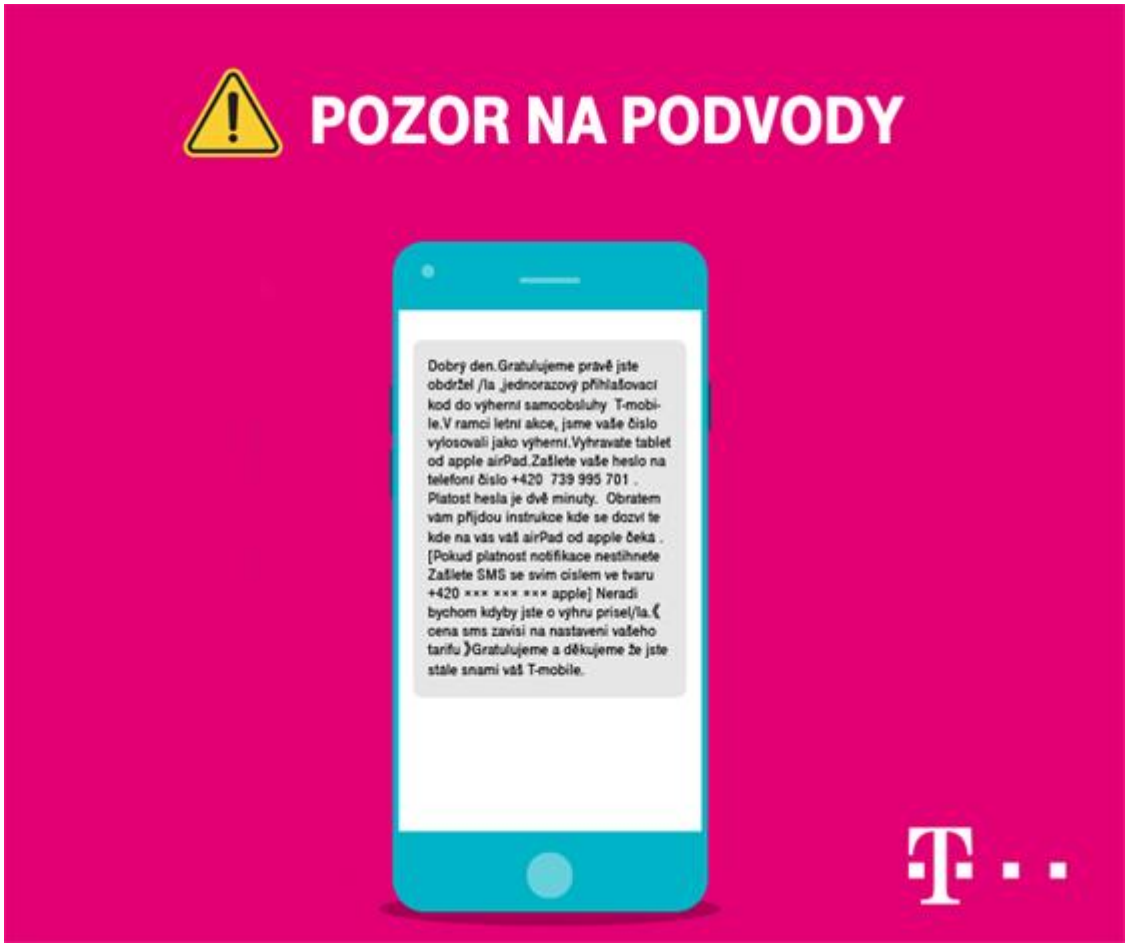
V poslední době a to především s rozvíjející se technologií komunikačních zařízení se podvodné útoky rozšířili z počítačového světa i do světa mobilních telefonů. V druhé polovině 2016 byl zaznamenán poměrně obrovský útok na uživatele tuzemských mobilních telefonů. Útočníci se pokoušeli vylákat peníze hned několika způsoby:

- Obdržením SMS zpráv od zdroje vydávajícího se za uživatelova operátora s možností získání nějaké slevy, či dokonce výhry v podobě nového mobilního telefonu apod. a to pouze za odeslání kódu, který uživatel chvíli před touto SMS zprávou obdržel.
- Obdržením SMS zprávy od nějakého důvěryhodného zdroje s odkazem ke stažení nějaké aktualizace nebo aplikace, která se jeví pro koncového uživatele jako důležitá, kdy však tato aplikace nebo aktualizace obsahuje malware, který po nainstalování má za úkol napadnout aplikaci mobilního bankovnictví uživatele a tak získat a odeslat pachateli přístupové údaje.

Tyto dva popisované způsoby byly v České republice za poslední dobu zaznamenány nejčastěji. Pachatelé zde opět využívají především nepozornosti samotného uživatele, kdy vše kryjí lákavou nabídkou soutěže a tím spojené výhry nebo důležité aktualizace. Útočnicí se nejprve pokusí (pravděpodobně za pomoci nějakého škodlivého programu) o zjištění přístupového hesla k uživatelskému emailu nebo telefonnímu číslu, které mají

k dispozici. Za pomoci pouze této jedné informace si zažádají za oprávněného uživatele o zaslání přístupového hesla k účtu. V této fázi začne uživateli přicházet několik SMS zpráv s přístupovým kódem k jeho účtu a to do doby než je využito maximální počet pokusů o zaslání. Neznalý koncový uživatel zpravidla nijak na zprávy nereaguje, považuje vše za nějako chybu systému, či omyl. Tyto SMS zprávy jsou odesílány operátorem a jsou tak i označeny. Následně však přichází SMS zpráva, která se již jen vydává za operátora a to s nabídkou slevy, či soutěže s možností lákavé výhry a to jen za odeslání kódu, který před chvíli uživatel obdržel. Koncový uživatel si však již zpravidla nevšimne, že zpráva již není ze stejného čísla, ale zcela z cizího mobilního telefonního čísla, kdy ve zprávě ještě dále je požadováno zaslání kódu na zcela jiné telefonní číslo, které je uvedeno v SMS zprávě.

*Obrázek č.4 Ukázka podvodné SMS zprávy T-Mobile*[39]




[39] Mobil.idnes.cz *[online].,[cit. 2017-03-01]. Dostupné z WWW:* < http://mobil.idnes.cz/t-mobile-podvodna-sms-vyhra-df6-/mobilni-operatori.aspx?c=A160913_124217_mobilni-operatori_LHR>.

Uživatel v domnění, že se účastní soutěže nebo žádá o slevu a kód odešle na požadované telefonní číslo, se však v okamžiku po odeslání dozví další obdrženou SMS zprávou, ve které je informován o tom, že z jeho telefonního účtu mu byla odečtena finanční částka, která v uvedených případech činila 5.000,-Kč. Částka byla zpravidla užita pro dobití jiného účtu. Potom co se úspěšně pachateli povede získat takto požadovanou částku ve svůj prospěch, tak obratem se stávají telefonní čísla, která byla užita pro podvodné jednání, nedostupná a nekontaktní.

### 4.6 Nebezpeční pronásledování, pornografie

Nebezpečné pronásledování, známé především pod pojmem „stalking“. Jedná se o trestný čin, který je definován ust. § 354 zák. č. 40/2009 Sb., trestní zákoník. Jde tedy o dlouhodobé pronásledování, které vzbuzuje u sledované osoby obavu o jeho zdraví nebo život a to i v případě jeho blízkých. Jednou z forem pronásledování může být i vytrvalá komunikace prostřednictvím elektronických prostředků, tedy prostřednictvím internetové sítě. Pachatel (v těchto případech „stalker“) tuto síť hojně využívá a to především pro její anonymitu, kdy může osobu kontaktovat jak pomocí mobilních zpráv, tak pomocí emailu, či sociálních sítí a to vždy s novým číslem, emailem a jménem, neboť síť umožnuje neomezené založení takových to účtů a zasílaní zpráv. Prokázání odesílání zpráv je pak proto velmi komplikované.

Pornografie a její šíření je a bude vždy celosvětovým problémem. Ve většině dnešních zemí jsou některé formy pornografie legální (dostupné v obchodech, ve vysílání, apod.). Naopak pornografie tvrdá, či dětská je zakázaná a ve většině zemí trestná. Český trestní zákoník postihuje některé tyto činy a to konkrétně: § 191 Šíření pornografie, § 192 Výroba a jiné nakládání s dětskou pornografií a § 193 Zneužití dítěte k výrobě pornografie. V tomto zákoně se vždy hovoří o tzv. pornografickém díle, které sice zákon zcela přesně nedefinuje a lze říci, že jde o obzvláště silné podněcování sexuálního pudu, které překračuje společností obecně uznávané hranice slušných pravidel a vyvolává pocit ostychu a studu. Podle obsahu dělíme pornografii na tvrdou, dětskou a prostou pornografii. Zvláště významně jsou českým trestním právem před pornografií chráněny děti. Šíření tvrdé pornografie je trestně postižitelné vždy, kdežto pokud dojde k šíření prosté pornografie, bude jedinec, který jí šíří trestně odpovědný jen tehdy, dostane-li se do kontaktu s dětmi. U tvrdé pornografie je kromě šíření také trestná pouze přímá

výroba, v případě dětské pornografie je však trestně stíhán i ten, kdo na její výrobě majetkově „kořistí“ (za úplatu vozí dítě na místo, pronajme prostory, na svých stránkách umístí odkaz apod.). Co se týče držení pornografie, tak všeobecně samotné držení trestné není, naopak od držení dětské pornografie, kde její přechovávání již trestné je.[40]

[40] AION CS. *Předpis č. 40/2009 Sb.: Zákon trestní zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2017-02-12]. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2009-40>.

# 5 Výzkum

Cílem výzkumu je stanovit znalosti a zkušenosti respondentů v oblasti počítačové kriminality a také reakce na určité typy útoku. Pro dosažení optimálních výsledků byla zvolena metoda kvantitativního výzkumu.

Pro svůj kvantitativní výzkum si stanovuji tyto hypotézy:

1. Počítačová kriminalita není veřejností brána jako hrozba, ale pouze jako negativní část dnešního počítačového světa, kdy je do jisté míry tolerována a není proti ní potřeba zvyšovat opatření a eliminovat ji.

2. Dnešní koncoví PC uživatelé nejsou dostatečně informování o možných hrozbách počítačové kriminality a neumějí se před ní bránit.

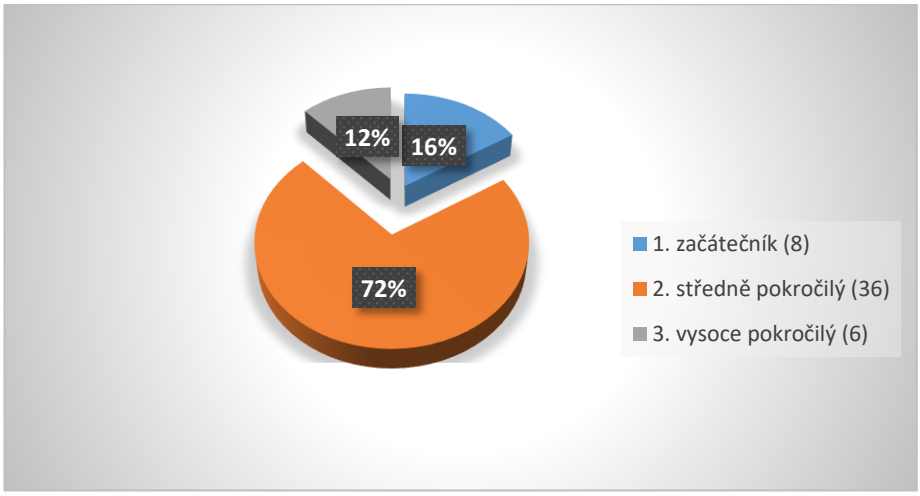
Při sestavování dotazníku jsem se soustředil na zodpovězení otázek v oblasti dnes nejběžnějších druhů počítačových kriminalit, se kterými se uživatel PC může setkat a snažil jsem se vystihnout to nejdůležitější a nejzákladnější, s čím by se uživatel PC mohl setkat, resp. se již setkal. Zároveň jsem několik otázek věnoval běžné informovanosti o možných hrozbách. Zvolil jsem i základní otázky určující věk, pohlaví a postavení v zaměstnání, což ve výsledku umožňuje více možností posouzení odpovědí.

Takto sestavený dotazník o 20 otázkách byl zacílen na běžnou skupinu lidí, menších až středně velkých pracovišť ve státním i soukromém sektoru (firmě), respektive tedy na jejich zaměstnance a pracovníky. Dotazníkové šetření bylo rozšířeno anonymním uživatelům službou Google forms a získané odpovědi byly protříděny na 50 použitelných odpovědí pro tento výzkum.

## 5.1 Výsledky a popis výsledků dotazníkového šetření

Otázka č. 1 : Jak hodnotíte Vaše znalosti v IT?

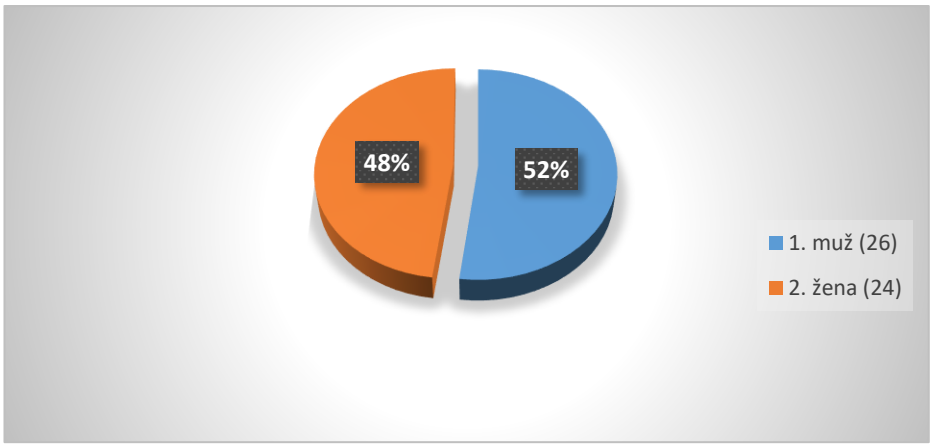
*Graf č. 1 Četnost respondentů z hlediska znalostí*[41]




Jak je vidět, většina respondentů se hodnotí jako „středně pokročilí“ jedná se o tedy 72% dotazovaných, jako „začátečníci“ se označilo 16% dotazovaných a zbylých 12% se označilo jako „vysoce pokročilí“ uživatelé.

Otázka č. 2 : Jakého jste pohlaví?

*Graf č. 2 Četnost respondentů z hlediska pohlaví*[42]



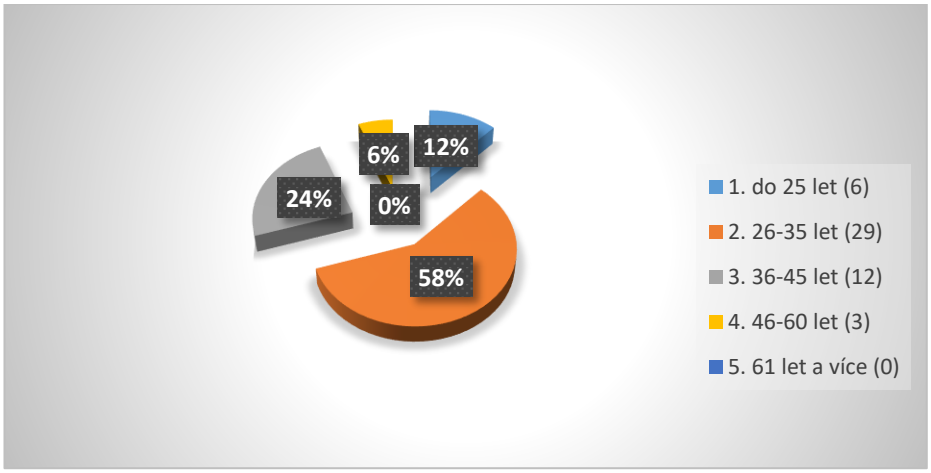

[41] Vlastní tvorba

[42] Vlastní tvorba

Z obdržených hodnot je patrné, že poměr mužů (52%) je poměrně vyrovnaný vůči ženám (48%). Dotazovaní, co se týče pohlaví, byli takřka na stejné úrovni.

Otázka č. 3 : Kolik je Vám let?

*Graf č. 3 Četnost respondentů z věku*[43]

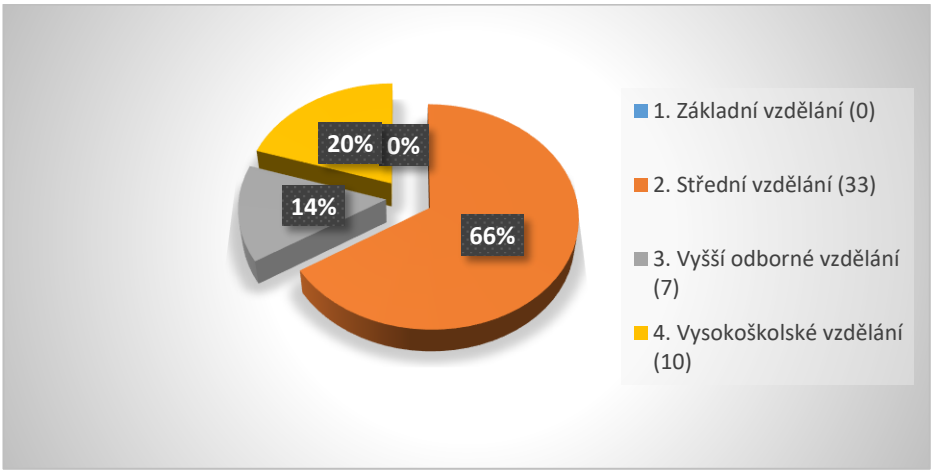



Souhrn odpovědí od respondentů ukazuje, že nejvíce odpovědí je od lidí ve věku 26 – 35 let (58%), jde tedy o více než polovinu respondentů. Na druhou stranu nejméně odpověděli respondenti ve věku 46 – 60 let (6%), když pomineme skupinu 61 let a více, tuto odpověď žádný respondent nezvolil. Necelou čtvrtinu odpovědí získala věková skupina ve věku 36-45 let (24%). Ve skupině do 25 let bylo zaznamenáno (12%) odpovědí.

[43] Vlastní tvorba

Otázka č. 4 : Jaké je Vaše nejvyšší dosažené vzdělání?

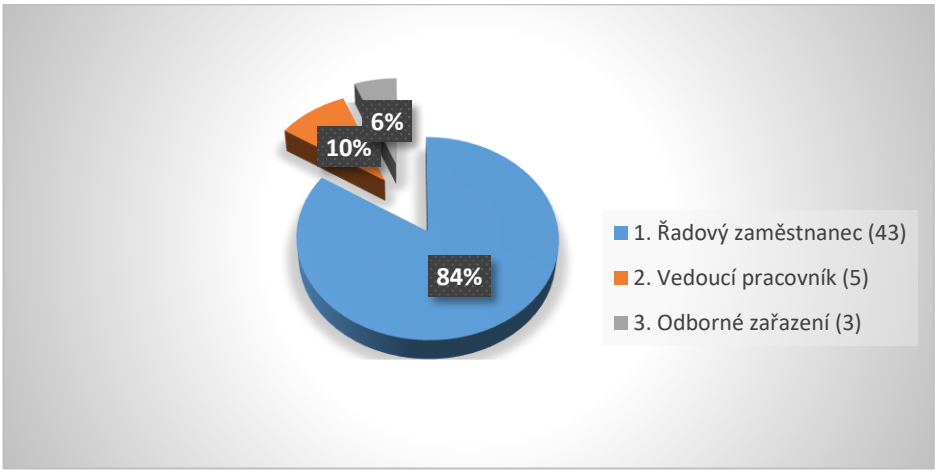
*Graf č. 4 Četnost respondentů z hlediska vzdělání*[44]




Největší zastoupení odpovědí, co se týče vzdělání respondentů, obdržela varianta středoškolského vzdělání (66%), Vyšší odborné zvolilo pak (14%) a Vysokoškolské (20%). Základní vzdělání nezvolil žádný z dotazovaných (0%).

Otázka č. 5 : Jaké je Vaše oblast pracovní pozice?

*Graf č. 5 Četnost respondentů z hlediska pracovní pozice*[45]



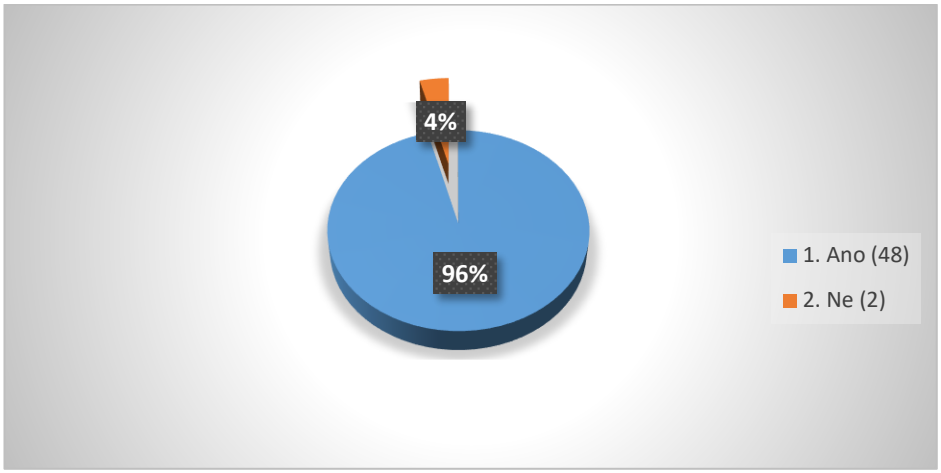

Mezi respondenty jak šlo předpokládat je nejvíce řadových zaměstnanců (86%), vedoucích pracovníků (10%) a odborně zařazených respondentů pouze (6%).

[44] Vlastní tvorba

[45] Vlastní tvorba

Otázka č. 6 : Je Váš počítač připojen k internetu?

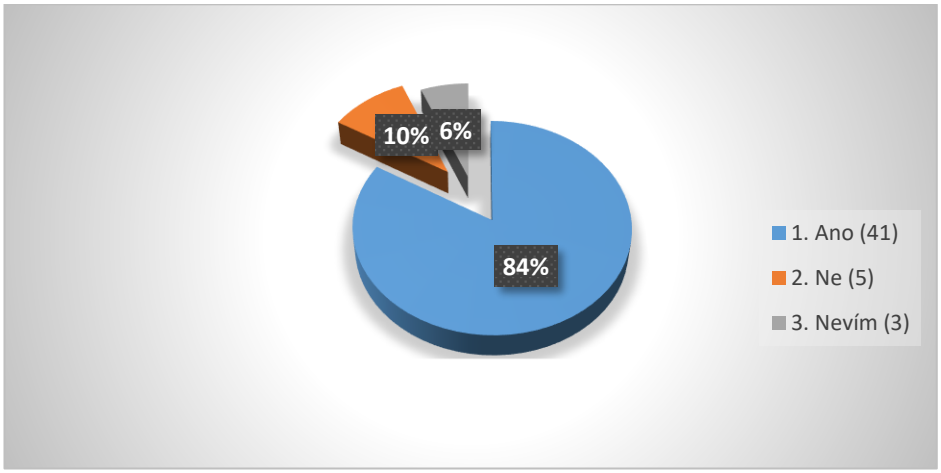
*Graf č. 6 Četnost respondentů z hlediska připojení k internetu*[46]




Dle odpovědí lze usoudit, že většina respondentů má připojený počítač k internetu. Pouze 2 respondenti uvedli, že nemají PC připojené k této síti.

Otázka č. 7 : Je Váš počítač nebo mob. telefon nějak chráněn? Např. pomocí antivirového programu?

*Graf č. 7 Četnost respondentů z hlediska zabezpečení zařízení*[47]




Cílem této otázky bylo zjistit, zda jsou respondenti obezřetní, co se týká chránění jejich zařízení (PC, mobilních zařízení, apod.) pomocí např. antivirového programu.

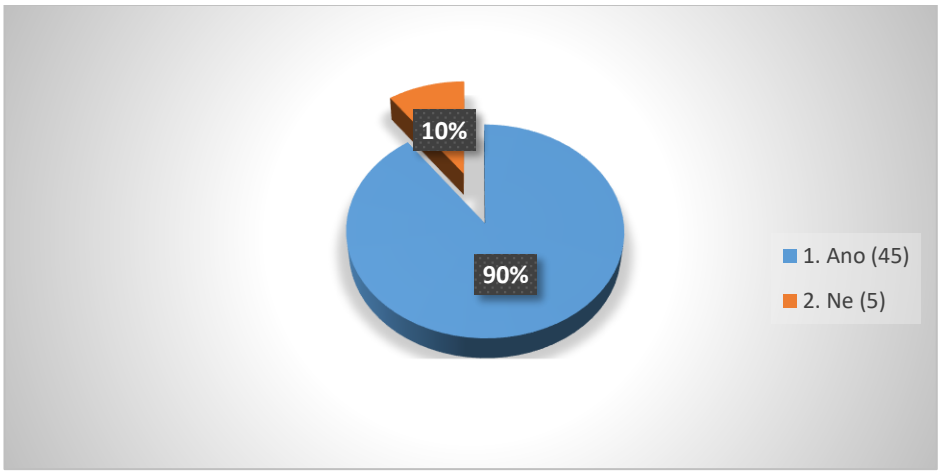
[46] Vlastní tvorba

[47] Vlastní tvorba

Překvapivě většina respondentů (82%) odpověděla, že ano, poměrně velmi malá část (10%) odpověděla, že žádné zabezpečující programy neužívá a zbylé 3% neví.

Otázka č. 8 : Máte internetové bankovnictví?

*Graf č. 8 Četnost respondentů z hlediska vlastnictví internetového bankovnictví*[48]

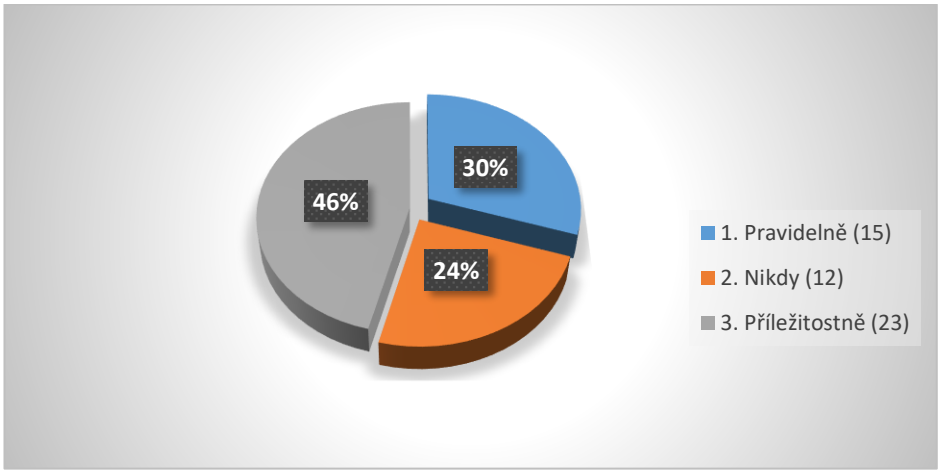



Z toho počtu odpovědí, opět jasně převahuje většina respondentů pro variantu „Ano“, tedy že vlastní internetové bankovnictví (90%), to vypovídá o tom, že většina dnešních uživatelů plně využívá a pracuje se sítí internet.

[48] Vlastní tvorba

Otázka č. 9 : Nakupujete přes internet přes bazarové stránky?

*Graf č. 9 Četnost respondentů z hlediska nákupů přes bazarové stránky na internetu*[49]

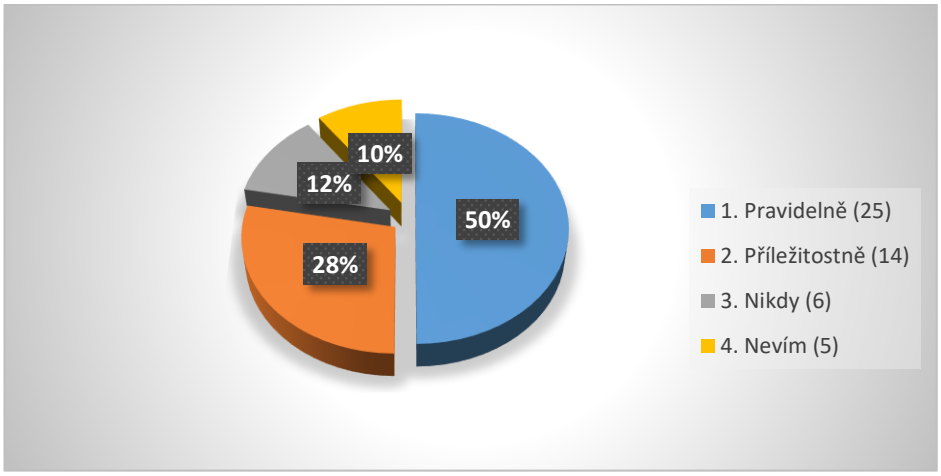



Co se týče bazarových nákupů přes internet, jsou již odpovědi nesjednocené, dá se říci, že možné varianty jsou poměrně vyrovnané. I tak lze uvést, že 30% respondentů nakupuje pravidelně a 46% příležitostně, tedy z pohledu, že více jak ¾ dotazovaných již nakupovali přes bazarové stránky přes internet, je pravděpodobné, že tato část dotazovaných se již i setkala s nějakým druhem počítačové kriminality, tedy např. s podvodnými nabídkami.

[49] Vlastní tvorba

Otázka č. 10 : Užíváte nebo jste užíval(a) někdy nějaký nelegální software?

*Graf č. 10 Četnost respondentů z hlediska užívání nelegálního softwaru* [50]

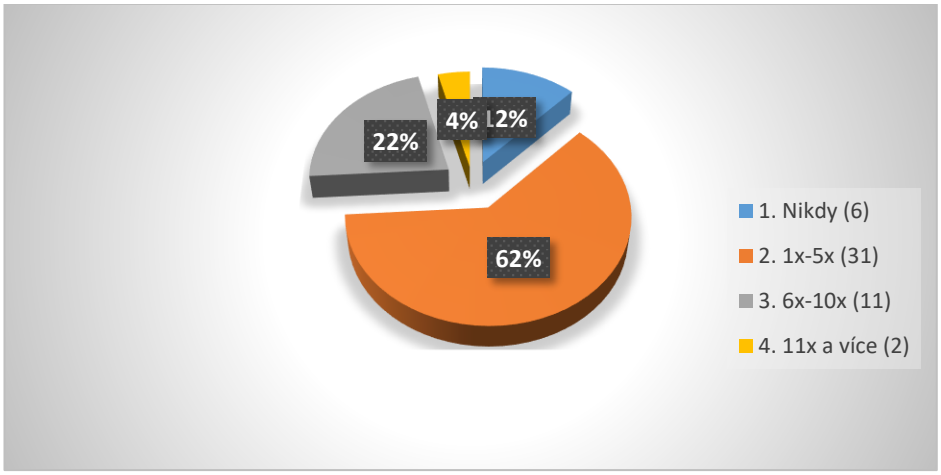



Tento výsledek je z běžného pohledu očekáváný, ale přesto je alarmující. 50% respondentů uvedla, že pravidelně užívá nelegální software. Dále 28% dotazovaných přiznalo, že příležitostně takovýto software užije. Tedy více jak ¾ respondentů užívá, nebo někdy užilo nelegální software. Jen 12% respondentů uvedlo, že nikdy a zbylých 10% neví.

[50] Vlastní tvorba

Otázka č. 11 : Setkal(a) jste se někdy s počítačovou kriminalitou? (počítačový vir, nelegální software, vyhrožování přes internet, podvody, napadení Vaše bankovního účtu, pornografií, apod.)

*Graf č. 11 Četnost respondentů z hlediska setkání se s počítačovou kriminalitou*[51]

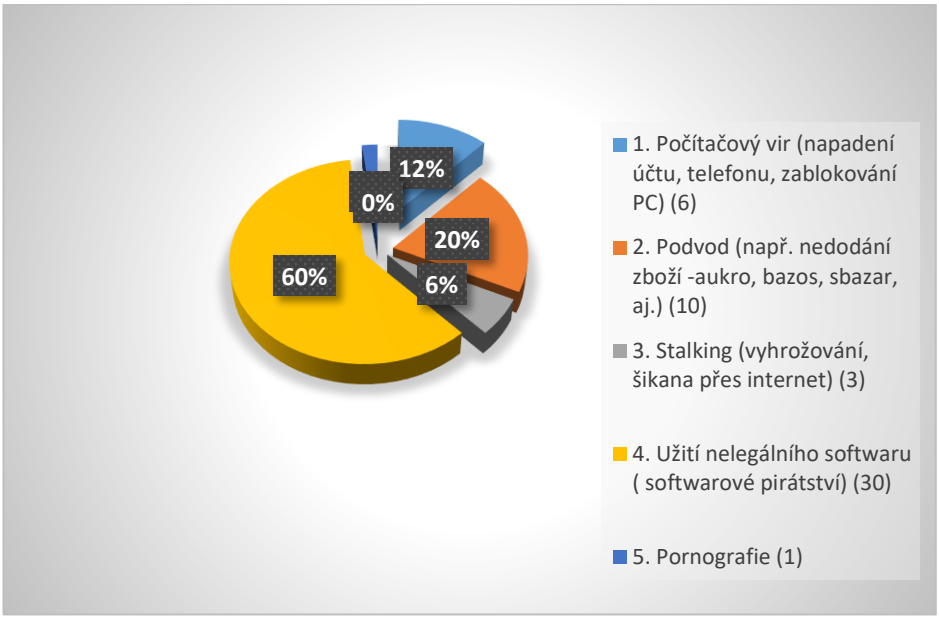



Podle odpovědí respondentů je patrné, že většina se již setkala s nějakým druhem počítačové kriminality, což není dobrá zpráva. Ze všech dotazovaných pouze 12% uvedlo, že se nikdy s počítačovou kriminalitou nesetkalo.

[51] Vlastní tvorba

Otázka č. 12 : Pokud ano, s jakým druhem?

*Graf č. 12 Četnost respondentů z hlediska setkání se s počítačovou kriminalitou a konkrétním druhem*[52]




Co se týče druhu kriminality na tuto otázku odpovídalo pouze 44 respondentů, vzhledem k předchozí otázce, kde 6 dotazovaných uvedlo, že se s žádným druhem počítačové kriminality dosud nesetkali. Ze zbylých dotazovaných někteří uváděli i více možností najednou, tedy setkali se s více druhy počítačových kriminalit.

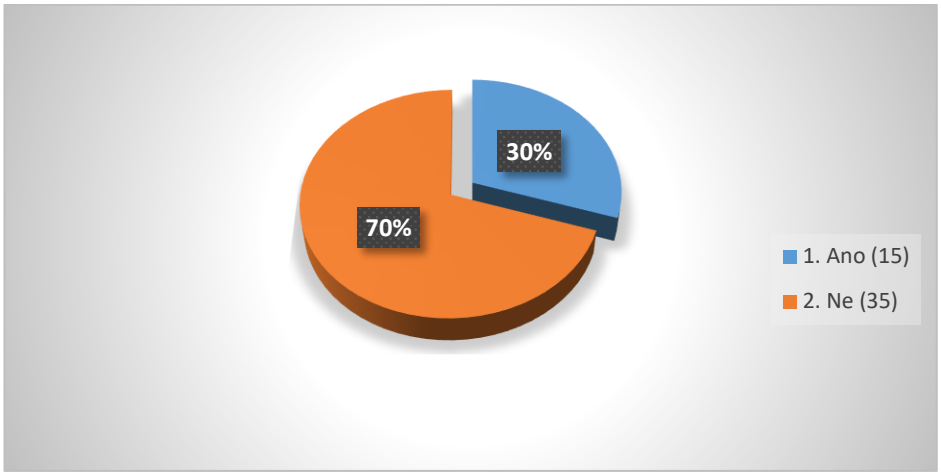
Jednoznačně se respondenti shodli, že nejčastěji se setkali s nějakým druhem nelegálního softwaru, programu. Jednalo se o 30 označení této možnosti, poté lze jako nejčastější kriminalitu v ČR označit podvody, tedy např. nedodání zboží přes inzerce a počítačové viry (zablokování PC a požadovaní zaplacení pokuty, apod.)

Ostatní uvedené možnosti byli voleny minimálně, stalking ve formě vyhrožování uvedli pouze 3 dotazovaní, s pornografií se setkal pouze jeden respondent a nikdo nezvolil a neuvedl jiný druh.

[52] Vlastní tvorba

Otázka č. 13 : Myslíte si, že jste dostatečně informován(a) o nových hrozbách, které Vás mohou potkat v při práci s počítačem a internetem?

*Graf č. 13 Četnost respondentů z hlediska informovanosti o nových hrozbách*[53]



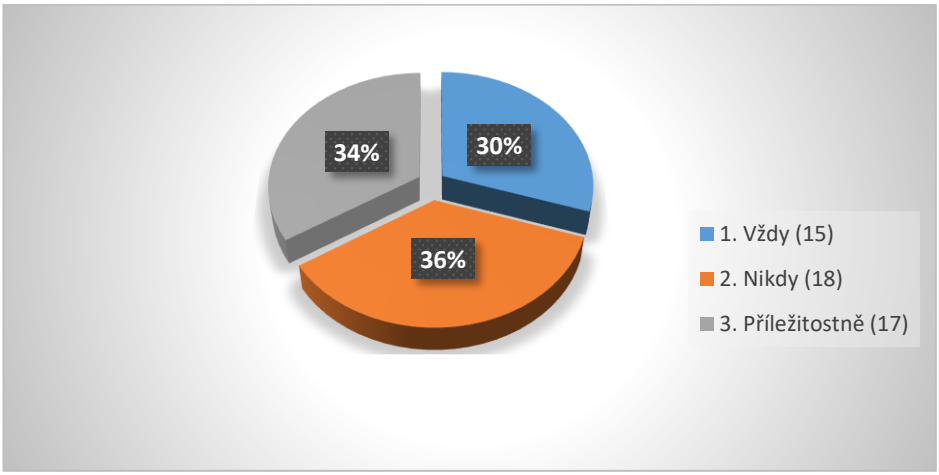

Zde více jak 2/3 dotazovaných uvedli, že nejsou spokojeni se současným stavem informovanosti veřejnosti ohledně nových možnostech počítačových kriminalit a tím spojených možnostech útoků a hrozeb. Zároveň uvedli, že ani neví, kde se dají tyto informace získat nebo nalézt. Zbylých 30% respondentů uvedlo, že jim současná informovanost o současných hrozbách připadá dostačující.

Získané odpovědi na tuto otázku ukázali, že jedním s problémů který má vést k potlačení počítačové kriminality je nedostatečná prevence, která spočívá i především v informovanosti veřejnosti.

[53] Vlastní tvorba

Otázka č. 14 : V případě, že obdržíte email nebo SMS zprávu s nějakou lákavou nabídkou (sleva na zboží, nabídka výhry, apod.), reagujete na ní?

*Graf č. 14 Četnost respondentů z hlediska reakce na lákavou nabídku*[54]



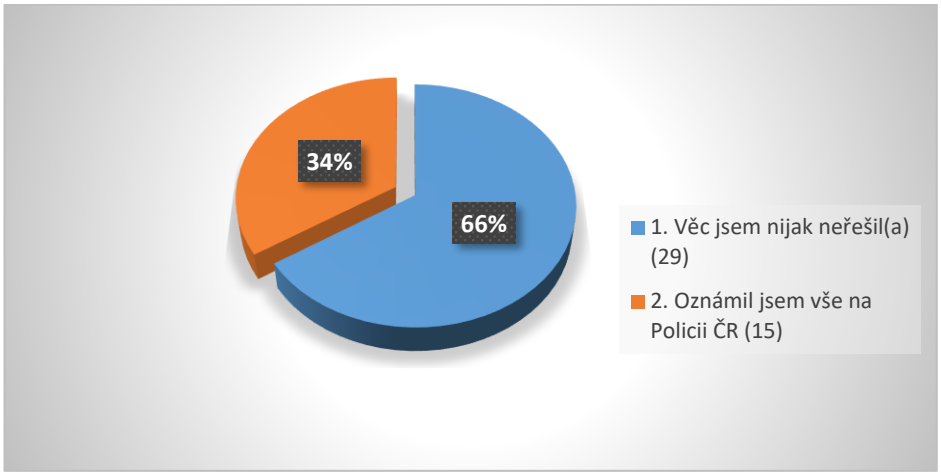

Touto otázkou jsem chtěl zjistit, jak se nechávají lidé „zlákat“ různými „výhodnými nabídkami“, „akcemi“, „slevami“, apod.

Z výsledku, kde 30% dotazovaných uvedlo, že na tyto nabídky reagují vždy, je patrné, proč se i těmto druhům počítačové kriminality (ve formě podvodů) tak hojně daří. Představa, že dalších 34% respondentů uvedlo, že na tyto zprávy reagují příležitostně, lze říci, že více jak 60% dotazovaných je vystaveno tomuto druhu kriminality, která bohužel poslední dobou proto hojně využívá těchto možností k finančním podvodům.

[54] Vlastní tvorba

Otázka č. 15 : Pokud jste se někdy setkal(a) s nějakým druhem počítačové kriminality, jak jste se zachoval(a)?

*Graf č. 15 Četnost respondentů z hlediska reakce na počítačovou kriminalitu*[55]




Na tuto otázku opět odpovídalo pouze 44 respondentů, vzhledem k předešlé otázce, kde 6 respondentů uvedlo, že se doposud s žádnou počítačovou kriminalitou nesetkalo.

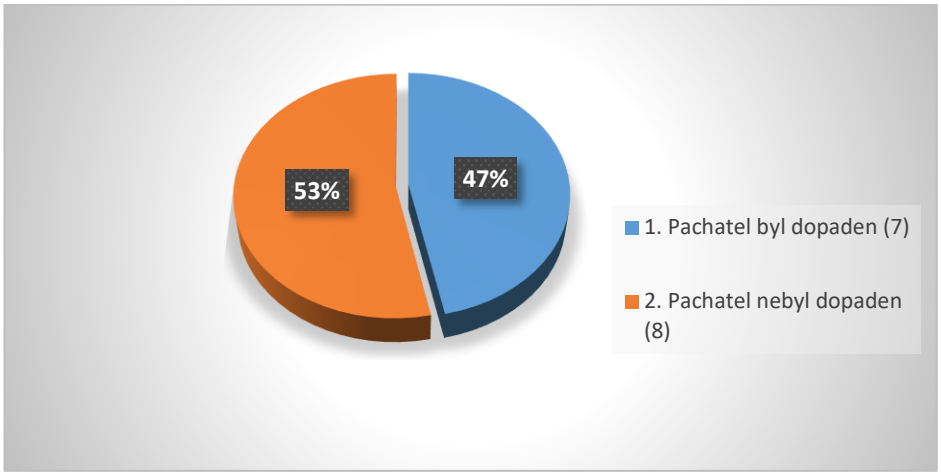
Jak je ze získaných hodnot vidět, většina poškozených nikdy počítačovou kriminalitu dále neřešila. Pouze třetina z poškozených touto kriminalitou uvedla, že se po zjištění obrátila na Policii ČR.

Je otázkou, zdali dotazovaní, kteří se na Policii ČR neobrátili, nemají pouze důvěru v tzv. úřední systém nebo tuto kriminalitu nevnímají tak nebezpečnou jako např. jiné činy, a proto se ani z těchto důvodů neobracejí na orgány činné v trestním řízení.

[55] Vlastní tvorba

Otázka č. 16 : Pokud jste řešil(a) nějaký druh počítačové kriminality přes Policii ČR s jakým výsledkem vše dopadlo?

*Graf č. 16 Četnost respondentů z hlediska výsledku řešení skrze Policii ČR*[56]



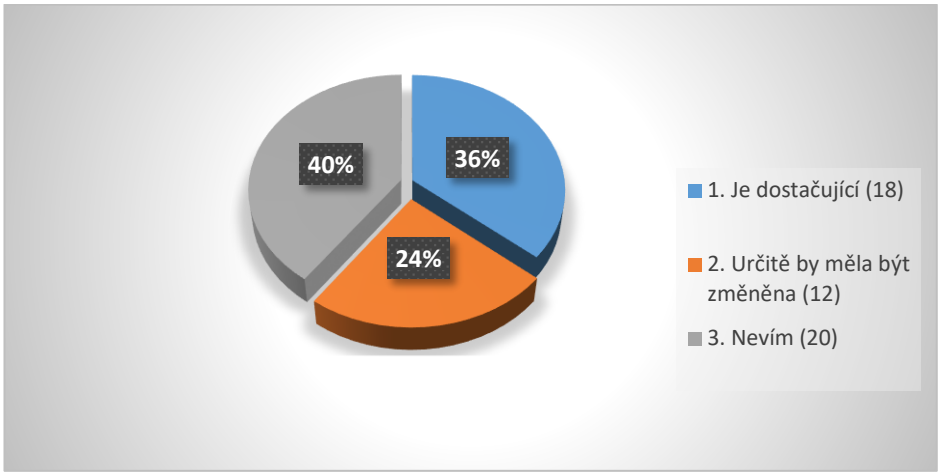

Na tuto otázku dle předchozí otázky odpovídalo pouze 15 respondentů.

Výsledek není bohužel zcela pozitivní. Necelá polovina zbylých respondentů, kteří řešili počítačovou kriminalitu cestou Policie ČR, označila, že byl v jejich případě zjištěn pachatel jejich činu. Pravděpodobně i tato poměrně malá objasněnost přispívá tomu, že poškození často své poškození touto kriminalitou těmto úřadům ani neoznamují.

[56] Vlastní tvorba

Otázka č. 17 Myslíte, že je současná právní úprava pro počítačovou kriminalitu v ČR dostačující (postihy, postup řízení, atd.)?

*Graf č. 17 Četnost respondentů z hlediska dostatečné právní úpravy v ČR*[57]

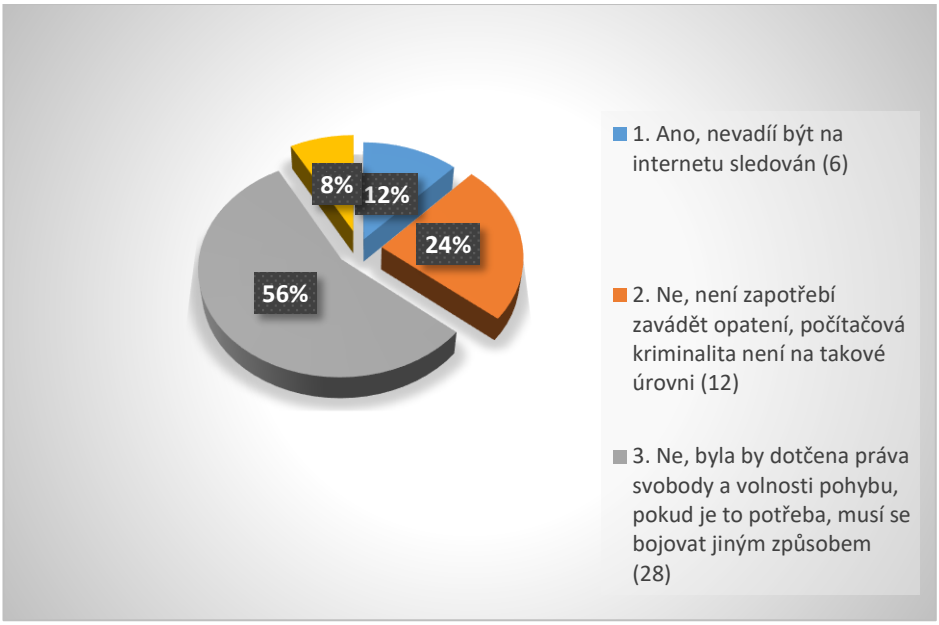



Jak lze vidět, zde se dotazovaní respondenti v žádné možné odpovědi nesjednotili. Naopak odpovědi jsou značně vyrovnané. I přesto je zajímavé, že největší část respondentů (40%) odpověděla, že neví, jestli je současná právní úprava dostačující. Pro upřesnění 24% by byla pro úpravu právních norem a 36% ji považuje za dostačující.

[57] Vlastní tvorba

Otázka č. 18 : Souhlasili byste se zavedením nějakého opatření v rámci sítě internet se záměrem zvýšení bezpečnosti a však na úkor ztracení svobody pohybu po této síti (cenzura internetu, kontrola, apod.)?

*Graf č. 18 Četnost respondentů z hlediska reakce na zavedení opatření*[58]



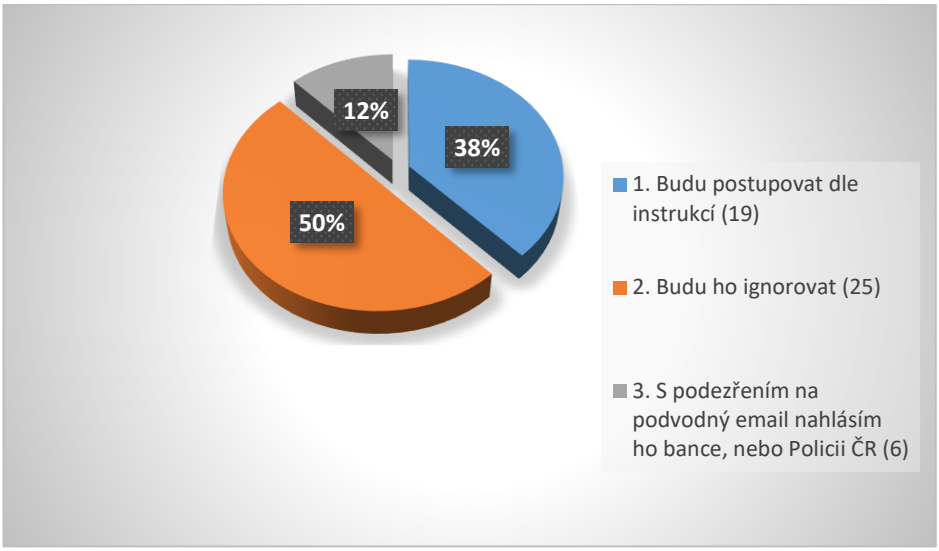

Zde je velmi zajímavé, že nadpoloviční většina respondentů (56%) uvedla, že jakákoliv omezující opatření v síti internet v rámci potlačení kriminality by nepřijala, ale uvedla, že pokud je to zapotřebí, musí se proti této kriminalitě najít jiný způsob boje. 24% dotazovaných uvedlo, že počítačová kriminalita není na takové úrovni, aby se museli zavádět taková to opatření. 12% by zavedená opatření nevadila a 8 % by to bylo jedno.

[58] Vlastní tvorba

Otázka č. 19 : Obdržíte email, kde bude zpráva, jak se zachováte?

Vazeni klienti, radi bychom Vas upozornili na novou verzi podvodneho e-mailu (tzv. phishingu). Nova verze e-mailu ma jako ty predesle vzbudit dojem, ze byla odeslana z e-mailove adresy Ceske sporitelny, tentokrat vsak z oficialni e-mailove adresy banky csas@csas.cz. Obsahuje odkaz v tele na udajne webove stranky internetoveho bankovnictvi banky a uzivatel je vyzvan k prihlaseni, tedy zadani osobnich bankovnich udaju. Prosim, verifikujte tuto emailovou adresu kliknutim na spojeni nize: http://www.csas.cz/banka/appmanager/portal/banka Verifikovaci spojeni je platne do 24 hodin.

*Graf č. 19 Četnost respondentů z hlediska reakce na uvedenou zprávu*[59]

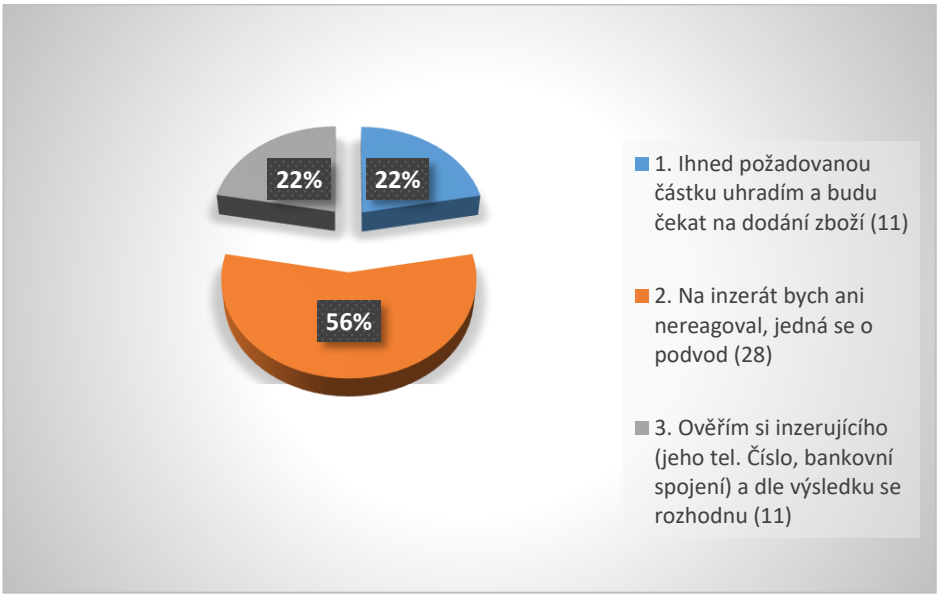



Na tomto příkladu útoku je vidět, že více jak 50% respondentů by poznala počítačový útok, cílený na získání přístupových údajů do internetového bankovnictví. Dokonce 12 % by tento email, či zprávu ihned oznámila na svojí banku či Policii ČR. Z grafu je i tak patrné, že 38% dotazovaných zvolilo odpověď, že by instrukce ihned splnili a tedy by podlehli možnému útoku. I přesto, že většina by útok rozeznala, stále je číslo osob, které by útoku podlehly dosti vysoké.

[59] Vlastní tvorba

Otázka č. 20 : Na inzerci bazos.cz najdete skvělou nabídku na nový mob. telefon Samsung S8 za cenu, která se oproti jiným nabídkám pohybuje o 30-50% níže než konkurenční nabídky. Inzerce je stručná, ale lákavá, občas narazíte na chybu v textu, je požadována platba předem, odeslání zboží obratem po zaplacení. Inzerent s Vámi komunikuje a slibuje okamžité odeslání zboží. Jak se zachováte?

*Graf č. 20 Četnost respondentů z hlediska reakce na uvedenou inzerci*[60]




Je chvályhodné, že nadpoloviční většina respondentů by opětovně poznala podvodný inzerát a na tento by vůbec nereagovala. Rovněž lze vyzdvihnout 22% respondentů, kteří by nejprve si inzerujícího prověřili a to možnými prostředky, tedy ověření tel. čísla, ověření bankovního účtu, atd. Bohužel stále velká část dotazujících, tedy 22%, což je skoro ¼, by ihned zareagovala tím, že by požadovanou částku uhradila a vyčkávala by na dodání zboží.

Na tomto příkladu se projevu psychologická stránka podvodu, kdy stále někteří lidé doufají, že jim seto stát nemůže, a s vidinou výhodné koupě reagují rychleji než by bylo vhodné.

[60] Vlastní tvorba

## Vyhodnocení hypotéz

První hypotéza potvrdila, že veřejnost nebere počítačovou kriminalitu jako hrozbu, ale pouze jako negativní část dnešního počítačového světa, která je do jisté míry tolerována a není tak proti ní potřeba bojovat a zvyšovat opatření.

Dle zjištění, kdy většina dotazovaných (56%) by žádná omezující opatření v síti internet v rámci potlačení kriminality nepřijala a 24% dotazovaných dokonce označilo možnost, že současná počítačová kriminalita není na takové úrovni, aby se proti ní muselo bojovat, lze tedy první hypotézu vyhodnotit tak, že dnešní společnost vnímá současnou počítačovou kriminalitu spíše jako negativní část počítačového světa, nikoliv jako hrozbu.

Druhá hypotéza rovněž potvrdila, že současní koncoví uživatelé nejsou dostatečně informování o současných hrozbách a neumějí se proti těmto zcela bránit.

Na otázku, zdali si myslí, že jsou dostatečně informování o současných hrozbách, odpovědělo více jak 70% respondentů negativně, tedy že nejsou dostatečně informování. Je však zajímavé, že otázky, na které dále respondenti odpovídali, které měly prověřit jejich znalosti a reakce na možné počítačové útoky, převažovaly ve vyhodnocení v kladných číslech. To znamená, že většinou více jak 50% dotazovaných by na možný útok zareagovalo správně a případný podvod by tak včas rozpoznali. Bohužel i přesto se zde odráží první hypotéza, tedy nízká informovanost veřejnosti, kdy číslo osob, které by případnému útoku podlehlo, je stále velmi obrovské.

### 5.2 Porovnávání příkladů počítačové kriminality

Jako nejběžnější příklady počítačové kriminality jsem zvolil ty, které se dle statistiky Policie ČR nejvíce vyskytují v České republice a se kterými se tedy zároveň můžeme nejčastěji setkat.[61] Jedná se tedy o:

- **Podvodné emaily:** vydávající se za nějaké instituce, úřady, banky atd. s vymáháním nějaké fiktivní pohledávky a tedy uhrazení požadované částky,

[61] Policie.cz *[online].,[cit. 2017-05-16]. Dostupné z WWW:* <http://www.policie.cz/clanek/zpravodajstvi-uo-jihlava-mezinarodni-konference.aspx>.

nebo vylákání přihlašovacích údajů k internetovému bankovnictví se zasíláním podvodných odkazů.

- **Malwere:** konr. „Trojský kůň Win32/Ransom“ který se hojně rozšířil po celém světě, tak i v České republice, který zablokuje uživateli koncové zařízení a vyžaduje zaplacení pokuty pomocí „paysafecard kódu“, kdy až po zmiňované úhradě dojde opět k jeho odblokování.
- **Porušování autorských práv**: neboli softwarové pirátství, kdy jde o nelegální získání nějakého díla, ať už jde o film, program, či hudbu apod. a jeho další šíření v rámci sítě internet i mimo něj bez svolení autora.
- **Podvodné internetové inzerce**: nabízení zboží, které není po uhrazení dodáno. Je podmíněné zasláním požadované částky za zboží předem na konkrétní účet.
- **Podvodné zasílaní SMS zpráv**: pachatelé se vydávají za operátory koncových uživatelů, kdy pod záminkou výhry nebo zvýhodnění stáváních služeb vylákají od uživatelů přístupové hesla, či kódy k jejich účtům v rámci telekomunikačních účtu, kdy se posléze takto obohacují na dobíjení kreditu k telefonování, apod.
- **Nebezpeční pronásledování, pornografie**: jedná se o trestnou činnost, kdy pouze moderní doba a síť internet hojně posloužila jako nástroj pro lepší páchání této činnosti.

V případech podvodných emailů, virů, podvodného zasílání SMS zpráv se pouze pachatelé snaží využívat co největší věrohodnosti. Ve svých zprávách (které se neustále mění, právě za účelem zvýšení věrohodnosti) neustále vylepšují záměr zprávy, který má koncového uživatele zmást a oklamat.

V případě těchto útoků se tedy vždy jedná o kombinaci psychologického a softwarového útoku. Pachatelé musí použít co nejdůvěryhodnější zprávu, která musí vzbudit dojem originality, tak aby koncový uživatel na ni zareagoval, tak jak pachatel potřebuje. Poté pouze za pomoci potřebného „viru“ ve formě např. falešného internetového odkazu nebo stažení falešné aktualizace dojde k dokončení požadované podvodné akce a poškození koncového uživatel. Ve své podstatě jde pouze neustálou inovaci nápadu a použitého programu, kdy použití a účel virů je popsán např. v použité

literatuře - JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.[62]

Jako možným opatřením proti těmto druhům útoků se jeví především dostatečná softwarová ochrana koncového uživatel (antiviry, apod.) a dostačená informovanost koncového uživatele před aktuálními způsoby útoků.

U dalších druhů počítačových kriminalit jako podvodné inzerce, nebezpečné pronásledování, pornografie lze říci, že internet pouze posloužil jako nástroj pro lepší páchání těchto druhů trestné činnosti. Pachatelé zde především využívají do jisté míry své anonymity a možnosti masivního šíření své činnosti. (podvodný inzerát je nabízen na několika portálech najednou, možnost reakce je oproti jiným způsobům nabízení několikanásobně vyšší, pornografický materiál je šířen obrovskou rychlostí po celém světě – případný zisk je několikanásobně vyšší než šíření jiným způsobem, nebezpečné pronásledování – anonymita tzv. „stalkera“). Tento druh útoků je značně popsán v použité literatuře - MATĚJKA, M. Počítačová kriminalita.[63]

Proti těmto druhům kriminality se jeví jako jediné možné řešení zavedení nějakého opatření v rámci sítě internet (např. ověření identity prodávajícího, cenzura, možná kontrola odesílaných a sdílených dat.)

Porušování autorských práv neboli také softwarové pirátství. Jedná se o specifickou trestnou činnost, kdy jde především o prolomení softwarové ochrany nějakého programu a následné volné šíření veřejnosti. Rovněž se dále jedná o šíření video a audio souborů podléhající autorskému právu. Svým způsobem jde o jakýsi způsob boje proti marketingu (vysoké ceny softwaru) a zviditelnění (dokázání schopností útočníka). Samotné softwarové pirátství rovněž hojně popisuje použitá literatura - MATĚJKA, M. Počítačová kriminalita. [64]

---

[62] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 59-67 s

[63] MATĚJKA, M. *Počítačová kriminalita*. Praha: Computer Press, 2002. 47-60 s.

[64] MATĚJKA, M. *Počítačová kriminalita*. Praha: Computer Press, 2002. 41-42 s.

Jako vhodné opatření proti tomuto druhu kriminality se jeví zlepšení softwarové ochrany programů (resp. znemožnění jejich „cracknutí“), snížení cen programů, zavedení kontroly sdílených dat, kontrola P2P sítí, atd.)

Jak lze vidět porovnáním základních příkladů zvolených počítačových kriminalit je hlavním problémem této kriminality nízká informovanost o útocích, určitá anonymita pachatele a volnost a možnosti „svobody a pohybu“ v síti internet.

Porovnáním s výsledky dotazníkového šetření je však patrné, že uživatelé budou raději do jisté míry tento druh kriminality tolerovat, než aby přišli právě o zmiňovanou „svobodu“ v síti internet.

# Závěr

Cílem této bakalářské práce bylo pokusit se najít teoretické řešení, které by pomohlo najít způsob jakým potlačit, či zcela zastavit v současné době počítačovou kriminalitu, která je nedílnou součástí dnešního počítačového světa a to především se zaměřením na počítačovou kriminalitu páchanou v České republice. V práci jsem charakterizoval počátky počítačové kriminality a to jak světově, tak se zaměřením na Českou republiku. Zároveň jsem popsal, jaká je současná prevence v ČR a jak probíhá boj proti této kriminalitě. Byla zde rozdělena a popsána hlavní trestná činnost, která je prostřednictvím této sítě páchána a vyčleněna ta počítačová trestná činnost se kterou se v České republice nejvíce setkáváme.

Závěrem lze říci, že vznik internetové sítě obrovskou mírou ovlivnil společnost světa. Síť, která měla být na svém počátku pouze technologickým vojenským vylepšením se stala o několik desítek let později nejužívanějším místem neboli prostorem na světě. Přínos této sítě pro společnost se stal tak markantní, že se na ni stal svět závislý. Lze si jen těžko představit, jaký by byl dopad pro společnost v případě celosvětového ochromení internetové sítě. Bohužel internetová síť dala zároveň prostor vzniku nové kriminality, počítačové kriminality. Jedná se o zcela nový druh páchání trestné činnosti a to v neznámém prostoru, kde dokazování a objasňování těchto činů dostává zcela jiný směr.

V poslední době se proto tímto stále více zaobírá Organizace spojených národů a některé světové velmoci, jako např. USA ve spolupráci s ostatními státy zabývající se stejnou problematikou, kdy se snaží navrhnout prosazení nových zákonů a opatření, které by zpřísnily a umožnily lepší boj s počítačovou kriminalitou.

Dle provedeného dotazníkového průzkumu lze usoudit, že lidé v České republice nejsou zcela dostatečně informovaní, co se týká nebezpečí a možných hrozeb při používání počítače v síti internet. Při pohybu po této síti a při provádění dnes již běžně standartních operací jsou často neobezřetní a lehkomyslní. Pro většinu lidí znamená počítač a připojení k internetu samozřejmost, ale ochrana dat a svého soukromí, která by měla být prioritní, je velmi zanedbána a podceňována. Proto se mnoho lidí stává obětí nějakého škodlivého softwaru nebo jiných útoků. Je velice zajímavé, že mnoho respondentů uvedlo, že používá nebo používalo vědomě nelegální software, přičemž

právě ten bývá zdrojem škodlivého softwaru, který může mít následky dalších mnohdy i hrozivějších útoků.

A však je potřeba zmínit, že v důležitých otázkách se většina respondentů zachovala dle zdravého rozumu a nepodlehla by možným počítačovým podvodným útokům.

Dle mých zjištění jsem dospěl názoru, že proti počítačové kriminalitě páchané nejen v České republice lze bojovat a dokonce ji v rámci možností za určitých reálných opatření, především zvýšení prevence a informovanosti potlačit, avšak její zastavení se jeví jako zcela nereálné, neboť opatření, která by musela být přijata, jsou značně teoretická a v dnešní době nepřijatelná.

# Seznam použitých zdrojů

TIŠTĚNÉ ZDROJE


1. CRAIG, P., HONICK, R. Softwarové pirátství bez záhad. Přeložil Tomáš HLAVÁČ. Praha: Grada, 2008. 212 s. ISBN 978-80-247-1765-4.
2. ČERVEŇ, P. Cracking a jak se proti němu bránit. Praha: Computer Press, 2001. 205 s. ISBN 80-7226-382-X.
3. GLENNY, M., KLIMÁREK, O. *Dark market ( Temný trh* ). Praha : Dokořán, 2013. 272 s. ISBN 978-80-7363-522-0
4. GŘIVNA, T., POLČÁK, R., ed. Kyberkriminalita a právo. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
5. JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 284 s. ISBN 978-80-247-1561-2.
6. MATĚJKA, M. Počítačová kriminalita. Praha: Computer Press, 2002. 106 s. ISBN 80-7226-419-2.
7. OLSON, P. Jsme Anonymous: uvnitř hackerského světa Anonymous, LulzSec a globální internetové vzpoury. Praha: Práh, 2012. 494 s. ISBN 978-80-7252-400-6.
8. POŽÁR, J. Informační bezpečnost. Plzeň: Aleš Čeněk s.r.o., 2005. 309 s. ISBN 80-868-9838-5.
9. ZELENÝ, J.,MANNOVÁ B. Historie výpočetní techniky. Praha: Scientia, 2006. 183 s. ISBN 80-86960-04-8
10. SMEJKAL, V., et al. *Právo informačních a telekomunikačních systémů, 2. rozšířené vydání*. Praha: C. H. Beck, 2004. 770 s. ISBN 80-717-976-50.
11. SMEJKAL, V.,SOKOL, T.,VLČEK, M. *Počítačové právo.* Praha, C. H. Beck/SEVT 1995

ELEKTRONICKÉ ZDROJE


1. *Základní definice, vztahující se k tématu kybernetické bezpečnosti.* [online]. Praha, 2009, [cit. 2017-01-23]. Dostupné z WWW: <http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.
2. PAUKERTOVÁ, V. *Elektronická informační kriminalita*. [online]. Ikaros. 2006, roč. 10, č. 8 [cit. 2017-02-12]. Dostupné z WWW: <http://www.ikaros.cz/node/3554>.
3. AION CS. *Předpis č. 127/2005 Sb.: Zákon o elektronických komunikacích.* [online]. AION CS, © 2010 - 2013, [cit 2017-02-12]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/2005-127>.
4. AION CS. *Předpis č. 121/2000 Sb.: Autorský zákon.* [online]. AION CS, © 2010 - 2013, [cit 2017-02-12]. Dostupné z WWW: <http:// http://www.zakonyprolidi.cz/cs/2000-121 >.
5. AION CS. *Předpis č. 101/2000 Sb.: Zákon o ochraně osobních údajů.* [online]. AION CS, © 2010 - 2013, [cit 2017-02-12]. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2000-101>.
6. AION CS. *Předpis č. 40/2009 Sb.: Zákon trestní zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2017-02-12]. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2009-40>.
7. AION CS. *Předpis č. 89/2012 Sb.: Občanský zákoník.* [online]. AION CS, © 2010 - 2013, [cit 2017-02-12]. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/1964-40>.
8. Počítačová kriminalita: *Mezinárodní úmluva je konečně závazná i pro Česko.* [online], [cit. 2017-01-23]. Dostupné z WWW: < https://www.patria.cz/pravo/2694193/pocitacova-kriminalita-mezinarodni-umluva-je-konecne-zavazna-i-pro-cesko.html>
9. Počítačová kriminalita*: Pomoc obětem TČ.* [online], [cit. 2017-04-01]. Dostupné z WWW: <http://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx>
10. Internet live stats.*: Internet statistic* [online].,[cit. 2017-03-01]. Dostupné z WWW: <http://www.internetlivestats.com/internet-users/>.

11. CESNET má 20 let*: historie české akademické sítě. [online]*. Praha, 2016, [cit. 2017-03-10]. Dostupné z WWW: <http://www.root.cz/clanky/cesnet-ma-20-let-historie-ceske-akademicke-site>.
12. Bezpečný internet.cz: *Softwarové pirátství* [online].,[cit. 2017-04-04]. Dostupné z WWW: < http://www.bezpecnyinternet.cz/pokrocily/stahovani-souboru-programu/softwarove-piratstvi.aspx/>.
13. Bezpečný internet.cz: *Internetové bankovnictví* [online].,[cit. 2017-04-04]. Dostupné z WWW: < http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/bezpecnost.aspx>.
14. Policie.cz: *Varování před počítačovým virem* [online].,[cit. 2017-03-01]. Dostupné z WWW: < http://www.policie.cz/clanek/varovani-pred-pocitacovym-virem.aspx/>.
15. GOVCERT.CZ: Národní centrum kybernetické bezpečnosti. [online].,[cit. 2017-05-26]. Dostupné z WWW: < https://www.govcert.cz/cs/vladni-cert/govcert-cz
16. Policie.cz: Mezinárodní konference, řešení elektronického násilí a kyberkriminality. *[online].,[cit. 2017-05-16]. Dostupné z WWW:* <http://www.policie.cz/clanek/zpravodajstvi-uo-jihlava-mezinarodni-konference.aspx

# Seznam obrázků

# Seznam tabulek a grafů

# Přílohy

Příloha č. 1 Použitý dotazník

## Umíte se bránit před počítačovou kriminalitou?

***Jak hodnotíte Vaše znalosti v IT?***

- ☐ začátečník
- ☐ středně pokročilé
- ☐ velmi pokročilé

***Jakého jste pohlaví?***

- ☐ Žena
- ☐ Muž

***Kolik Vám je let?***

- ☐ do 25 let
- ☐ 26 - 35 let
- ☐ 36 - 45 let
- ☐ 46 - 60 let
- ☐ 61 let a více

***Jaké je Vaše nejvyšší dosažené vzdělání?***

- ☐ Základní vzdělání
- ☐ Střední vzdělání
- ☐ Vyšší odborné vzdělání
- ☐ Vysokoškolské vzdělání

***Jaké je Vaše oblast pracovní pozice?***

- řadový zaměstnanec
- vedoucí pracovník
- odborné zařazení (např. IT specialista)

***Je Váš počítač připojen k internetu?***

- Ano
- Ne

***Je Váš počítač, nebo mob. telefon nějak chráněn? Např. pomocí antivirového programu?***

- Ano
- Ne
- Nevím

***Máte internetové bankovnictví?***

- Ano
- Ne

***Nakupujete přes internet přes bazarové stránky?***

- Pravidelně
- Nikdy
- Příležitostně

***Užíváte, nebo jste užíval(a) někdy nějaký nelegální software?***

- Používám pravidelně, tento software je „zadarmo“
- Příležitostně, pouze pokud potřebuji software, který je moc fin. nákladný
- Nikdy, nelegální software může obsahovat viry, nemá podporu aktualizací
- Nevím

***Setkal(a) jste se někdy s počítačovou kriminalitou? (počítačový vir, nelegální software, vyhrožování přes internet, podvody, napadení Vaše bankovního účtu, pornografií, apod.)***

 Nikdy

 1x-5x

 6x-10x

 11x a více

***Pokud ano, s jakým druhem?***

 Počítačový vir (napadení bankovního účtu, telefonu, zablokování PC virem, zaplacení pokuty aj.)

 Podvod (nedodání zboží) skrze inzerci (bazos, sbazar, aukro, aj.)

 „Stalking“, vyhrožování, šikana skrze internet

 Užití nelegálního software (softwarové pirátství)

 Pornografií

 Jinou……

***Myslíte si, že jste dostatečně informován(a) o nových hrozbách, které Vás mohou potkat v při práci s počítačem a internetem?***

 Ano, informace jsou dostačující

 Ne, nikdy jsem o hrozbách informován nebyl(a) a ani nevím kde se tyto informace nacházejí

***V případě, že obdržíte email nebo SMS zprávu s nějakou lákavou nabídkou (sleva na zboží, nabídka výhry, apod.), reagujete na ní?***

 Vždy

 Nikdy

 Příležitostně

***Pokud jste se někdy setkal(a) s nějakým druhem počítačové kriminality, jak jste se zachoval(a)?***

 Věc jsem nijak dále neřešil(a)

 Oznámila jsem vše na Policii ČR

***Pokud jste řešil(a) nějaký druh počítačové kriminality přes Policii ČR s jakým výsledkem vše dopadlo?***

 Pachatel byl dopaden

 Pachatel nebyl dopaden

***Myslíte, že je současná právní úprava pro počítačovou kriminalitu v ČR dostačující (postihy, postup řízení, atd.)?***

 Je dostačující

 Určitě by měla být změněna

 Nevím

***Souhlasili byste se zavedením nějakého opatření v rámci sítě internet se záměrem zvýšení bezpečnosti a však na úkor ztracení svobody pohybu po této síti (cenzura internetu, kontrola, apod.)?***

 Ano, nevadí mi být na internetu sledován, je za

 Ne, počítačová kriminalita není na takové úrovni, aby bylo zapotřebí zavádět taková opatření

 Ne, byla by tím dotčena práva svobody a volnosti pohybu, která na internetu jsou, pokud je to potřeba, musí se proti počítačové kriminalitě bojovat jiným způsobem

 Je mi to jedno

***Obdržíte email, kde bude zpráva, jak se zachováte?***

***Vazeni klienti, radi bychom Vas upozornili na novou verzi podvodneho e-mailu (tzv. phishingu). Nova verze e-mailu ma jako ty predesle vzbudit dojem, ze byla odeslana z e-mailove adresy Ceske sporitelny, tentokrat vsak z oficialni e-mailove adresy banky csas@csas.cz. Obsahuje odkaz v tele na udajne webove stranky internetoveho bankovnictvi banky a uzivatel je vyzvan k prihlaseni, tedy zadani osobnich bankovnich udaju. Prosim, verifikujte tuto emailovou adresu kliknutim na spojeni nize: http://www.csas.cz/banka/appmanager/portal/banka Verifikovaci spojeni je platne do 24 hodin.***

 Budu postupovat dle instrukcí

 Budu ho ignorovat

 S podezřením na podvodný email nahlásím bance, nebo Policii ČR

***Na inzerci bazos.cz najdete skvělou nabídku na nový mob. telefon Samsung S8 za cenu, která se oproti jiným nabídkám pohybuje o 30-50% níže než konkurenční nabídky. Inzerce je stručná, ale lákavá, občas narazíte na chybu v textu, je požadována platba předem, odeslání zboží obratem po zaplacení. Inzerent s Vámi komunikuje a slibuje okamžité odeslání zboží. Jak se zachováte?***

 Ihned požadovanou částku uhradím a budu čekat na dodání zboží

 Na inzerát bych ani nereagoval, jedná se o podvodný inzerát

 Ověřím si inzerujícího (jeho tel. Číslo, bankovní spojení), např. přes jiné stránky a až podle výsledku se rozhodnu