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

BAKALÁŘSKÁ PRÁCE

TRESTNÉ ČINY V POČÍTAČOVÉM SVĚTĚ SE ZAMĚŘENÍM NA BĚŽNÉ UŽIVATELE

Autor práce: Vrbová Denisa

Studijní obor:Bezpečnostně právní činnost ve veřejné správě

Forma studia: Prezenční

Vedoucí práce:Mgr. Vladimír Čížek

Katedra:Katedra právních oborů a bezpečnostních studií

2017

Prohlašuji, že jsem bakalářskou práci vypracoval(a) 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, za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

VRBOVÁ, D. *Trestné činy v kybernetickém světě se zaměřením na běžného uživatele : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2017. 65 s. Vedoucí bakalářské práce : Mgr. Vladimír Čížek.

Klíčová slova: kybernetická kriminalita, internet, kybernetický prostor, kybernetický útok, uživatel

Informační technologie, jsou neodmyslitelnou součástí dnešní doby a každodenního života. Díky rychlému nástupu těchto technologií a stále rychlejšímu vývoji se také rychleji vyvíjí i trestná činnost jimi páchaná. Každý uživatel těchto technologií je přímo ohrožen, a proto je důležité chránit svůj počítač a data v něm uložená. V práci budou vyjmenovány a analyzovány nejčastější druhy a formy počítačové kriminality a za pomocí dat získaných dotazníkovým šetřením a polořízeným rozhovorem, navrhnuté řešení, jak se proti nim bránit a na co si má běžný uživatel dát pozor. Informace v této práci uvedené budou analyzovány z odborné literatury a důvěryhodných internetových zdrojů na toto téma.

ABSTRACT

VRBOVÁ, D. *Crimes in the Cyber World with a focus on common users :Bachelor thesis.* ČeskéBudějovice : The College of European and Regional Studies, 2017. 65 p. Supervisor : Mgr. Vladimír Čížek.

Key words: cybercrime, Internet, cyberspace, computer, cybber-attack, user

Information technology is an essential part of modern everyday life. Thanks to the rapid onset of these technologies and their fast development is also rapidly evolving crimes committed by them. Each user of these technologies is directly threatened, and therefore it is important to protect their computer and data stored in it. This bachelor thesis contains analysis of the most common types and forms of cybercrime. Based on data obtained with help of Interview Survey and semileaded interviews, will be suggested a solution how to defend against common cybercrimes and what is normal user beware. Information given in this work will be analyzed from literature and trusted internet sources on this topic.

Obsah

Úvod

Informační technologie jsou bezesporu nedílnou součástí moderní společnosti. Od druhé poloviny 20. století, se vývoj informačních technologií začal vyvíjet takovou rychlostí, že pokud v jednom roce vyjde publikace o nějakém softwaru, tak v dalším roce díky novým aktualizacím, může být publikace zastaralá. Dnes si život bez počítače a dalších informačních technologií většina lidí neumí představit. Informační technologie, jsou nedílnou součástí každodenního života a lze je nalézt téměř všude a všichni se s nimi již alespoň jednou setkali, ať se jedná o jakoukoli věkovou skupinu. Zkrátka je to fenomén dnešní doby, se kterým se lidé již nesetkají jen v práci, nebo ve školách, jak tomu bylo v minulosti, ale protože jsou informační technologie stále více finančně přístupné, tak je lze nalézt téměř v každé domácnosti.

Informační technologie, jak již bylo řečeno, lze nalézt všude, nejedná se jen o počítače jako takové, ale například i tablety, chytré telefony, mikrovlnné trouby, ledničky, auta, nebo letadla. Zkrátka vše, co obsahuje software, lze považovat za jakýsi stroj, který sbírá a ukládá nějaká data a informace. To ale ovšem také znamená, že vše, co obsahuje software, lze úmyslně napadnout, zneužít, nebo zničit. Informace hýbou světem a jsou mnohdy cennější než peníze samotné, a proto čím dál tím častěji dochází k trestné činnosti za použití informačních technologií.

Zaevidovaná kybernetická trestná činnost od roku 2011 do roku 2016 stoupla téměř čtyřnásobně.[1]To znamená, že ačkoli existuje mnoho odborných publikací a návodů, jak si uživatelé mohou zabezpečit svůj počítač. Ale běžní uživatelé je nevyužívají a vystavují tak svůj počítač zbytečně hrozbám, kterým by mohli sami předejít. Ale naopak, zručných pachatelů, kteří se ve světě informačních technologií vyznají a kteří za jejich použití páchají trestné činy, stále přibývá, a proto je důležité přesvědčit běžné uživatele informačních technologií, aby dodržovali alespoň základní bezpečnostní opatření.

[1]Kyberkriminalita. *Policie.cz*[online]. 2017 [cit. 2017-4-8]. Dostupné z WWW: <http://www.policie.cz/clanek/kyberkriminalita.aspx>.

1 Cíl a metodika bakalářské práce

Tato bakalářská práce je zaměřená na trestné činy v počítačovém světě a na běžné uživatele informačních technologií. Cílem práce je zjistit obecnou povědomost uživatelů o tomto tématu a následně navrhnout základní opatření, kterými by se měli uživatelé řídit, aby se co nejvíce ochránili proti tomuto druhu trestné činnosti.

První část bakalářské práce, je zaměřena na kybernetickou kriminalitu, její charakteristiku, druhy a základní dělení. Dále nástin základních zákonů, které se zabývají trestnou činností páchanou za pomoci počítačů, nebo na nich. Na závěr této části, jsou uvedené profesionální týmy, které se touto problematikou zabývají. V práci uvedené informace, jsou získány a analyzovány z odborných publikací v českém a anglickém jazyce a důvěryhodných internetových zdrojů.

Druhá poloviny práce je zaměřená na běžné uživatele, kde pomocí dotazníkového šetření je zjišťováno a následně analyzováno obecné povědomí o kybernetické kriminalitě a jejích druzích. Dále na základě položízeného rozhovoru s IT pracovníky jsou navržena základní opatření, kterými by se uživatelé měli řídit, aby se v co největší míře vyvarovali napadení jejich počítače a zamezili tak úniku svých citlivých dat.

2 Základní pojmy a jejich význam

2.1 Počítačový uživatel

Za uživatele v počítačovém světě se označují všichni lidé, kteří využívají počítačové systémy. K tomu, aby je využívali, potřebují svůj uživatelský účet, díky kterému do nich získávají přístup. Počítačový uživatel je s ohledem na počítačovou bezpečnost vždy tím nejslabším článkem. Důvod je prostý: člověk není stroj a tím pádem se může nedopatřením dopustit chyb. Proto se uživatelé musejí v průběhu života stále učit a zdokonalovat ve výpočetní technice, protože technologie jdou stále dopředu. A co se dnešní generace učí ve školách, tak příští to již bude považovat za historii. Počítačoví uživatelé se většinou dělí na:

1. Běžný uživatel – je jakýkoli uživatel, který využívá výpočetní techniku, anebo internetovou síť.

2. Administrátor – je ten, kdo spravuje síť, informační databáze, anebo má na starosti počítače jako takové.

2.2 Pachatel

Nejčastějšími pachateli v počítačovém světě jsou hackeři neboli počítačoví piráti. Hacker je člověk, který se baví tím, že se učí novým dovednostem, jako jsou počítačové jazyky, programování, anebo zkrátka na jakých principech počítač a internet funguje a jak lze tyto principy obejít či zneškodnit. Podle autorky Julie Mehan[2], lze hackery rozdělit na dva základní typy a to:

1. Vysoce sofistikované a technicky nadané lidi, kteří buď programy sami navrhují a píší, nebo je vyhledávají a využívají k prospěchu svému. Tito lidé jsou velice inteligentní a jejich útoky jsou nevypočitatelné a těžce zjistitelné, tedy ovšem pokud oni sami nechtějí.

2. Druhá skupina jsou lidé, kteří chtějí hlavně napáchat svým jednáním co největší škody.

[2]Mehan, J. E. *Cyberwar, cyberterror, cybercrime and cyberactivism*. Second Edition. United Kingdom: IT GovernancePublishing, 2014 s. 71-73.

Motivací k útoku může být mnoho, ale nejčastější druhy útoků jsou dva a to:

1. Krátkodobý aneb udeř a běž. Tyto útoky jsou většinou zaměřeny na přímé a rychlé poškození počítačového systému, nebo vyhledání a ukradení informací, které útočník dále využívá. Mezi krátkodobé útoky také patří krádež identity.

2. Dlouhodobý útok si útočník vybere například tehdy, když chce měnit informace a data v určitém informačním systému nějaké organizace za běhu a nechce být vystopován. Nebo si vybere dlouhodobý útok, kdy napadne uživatelský software a pomocí backdoorového programu dlouhodobě získává data a jiné citlivé údaje bez toho, aby ho oběť tohoto útoku odhalila.

2.3 Kybernetický prostor

Kybernetická kriminalita se nejčastěji odehrává v kyberprostoru. Kyberprostor můžeme přirovnat k virtuálnímu světu, který vznikl propojením počítačových sítí. Díky němu mohou uživatelé připojení na síť, snadněji komunikovat, nebo využívat další služby, které síť nabízí. Za kyberprostor tedy můžeme považovat celý internet. Kyberprostor je tvořen daty a informacemi, které tam uživatelé, kteří ho využívají, zanechávají. Podle Václava Jirovského[3] ke vzniku kyberprostoru došlo v roce 1968, kdy došlo k propojení čtyř univerzitních počítačů. Do té doby, byl počítač vždy jen samostatnou jednotkou. Při propojení počítačů, tedy při vzniku první sítě, nikdo nepředpovídal rychlý vzestup internetu, proto bezpečnostní prvky byly nedostačující. Díky rychle se rozrůstajícím sítím a stále více připojených uživatelů, bezpečnost, která neměla pevný základ již ze začátku, začala pokulhávat a nestačila se vyvíjet tak rychle jako výpočetní technika a jiné technologie, čehož využili hackeři pro páchání protiprávných činů. Tak vznikla kybernetická kriminalita.

2.4 Internet

Pojmem internet se myslí celosvětová počítačová síť, která spojuje ať už pomocí kabelu, nebo bezdrátově všechny počítače a jiná zařízení s možností přístupu na internet. Pomocí internetu mohou uživatelé sdílet data, posílat elektronickou poštu, vyhledávat informace či jen prohlížet webové stránky. Každý počítač, nebo zařízení, které je připojeno k internetu disponuje svojí IP adresou, podle které se mohou daná zařízení lokalizovat.

[3] Jirovský, V. *Kybernetická kriminalita*. Vyd. 1. Praha: GradaPublishing, a.s., 2008. s.15.

Informace, data, citlivé údaje

Informace a data[4]

Data jsou určité vjemy, které dokážeme zachytit lidskými smysly, ale sami osobě většinou nic neznamenají. Když se data spojí dohromady, vznikají informace.

Informace jsou vzácná komodita, kterou lze zneužít. Proto existuje zákon č. 106/1999 Sb. zákon o svobodném přístupu k informacím, který určuje, jaké informace a za jakých podmínek lze poskytovat a komu. Dále tento zákon říká, že pokud je požadovaná informace označena jako utajovaná informace, a žadatel k ní nemá oprávněný přístup, subjekt ji neposkytne. Stejně tak, pokud se jedná například o ochranu obchodního tajemství, nebo se jedná o informaci, která je předmětem ochrany autorského práva.[5]

Osobní a citlivé údaje[6]

Jsou to všechny údaje, které se nějak týkají člověka a jeho identity. Mohou to být například číslo mobilního telefonu, číslo občanského průkazu, záznamy o jeho zdraví, školní záznamy, údaje o jeho vyznání či jeho adresa.

Ochranou osobních údajů se zabývá zákon č. 101/2000 Sb. Tento zákon chrání před neoprávněným zasahováním a zneužíváním osobních údajů. Dále určuje a ukládá dozorovou působnost úřadu pro ochranu osobních údajů. Tento zákon se především vztahuje na osobní údaje, které zpracovávají a nakládají s nimi státní úřady a orgány veřejné moci. Také určuje, že mohou shromažďovat a zpracovávat jen takové údaje, které jsou nezbytné pro naplnění jejich účelu nebo činnosti.

[4]Data, Informace, Znalosti. *is.bivs.cz.*[online]. 2014 [cit. 2017-8-4]. Dostupné z WWW: <https://is.bivs.cz/el/6110/zima2013/B101API/um/Data__Informace__Znalosti_v2014.pdf>.
[5] Zákon 106/1999 Sb., zákon o svobodném přístupu k informacím. Zákon pro lidi.cz [online]. 2017 [cit-2017-4-8]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/1999-106>.
[6] Zákon 101/2000 Sb., o ochraně osobních údajů. *uoou.cz*[online]. 2000 [cit-2017-4-8]. Dostupné z WWW: <https://www.uoou.cz/files/101_cz.pdf>.

3 Kybernetická kriminalita

3.1 Kybernetická kriminalita

Kybernetická kriminalita se díky rychlému rozvoji technologií a internetu stává čím dál tím větším problémem. Ale není to kyberprostor, nebo internet chcete-li, kdo je nebezpečný. Nebezpeční jsou právě jeho uživatelé, kteří ho využívají k protiprávnímu jednání, nebo uživatelé kteří, nevědomky narušují jeho bezpečnost a tím tak dávají prostor lidem, kteří toho zneužívají.

Jirovský[7]ve své knize vymezil pojem kybernetická kriminalita takto Kybernetická kriminalita je taková činnost, která porušuje zákon, nebo je v rozporu s morálními pravidly společnosti. Tato kriminalita může být namířena přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod., nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává.

Kybernetická kriminalita a trestné činy s ní spojené jsou trestné činy jako každé jiné a od běžné kriminality je odděluje jen to, že jsou páchány, jak již bylo řečeno, na počítačích a informačních technologiích, nebo s jejich pomocí. Pachatelé těchto činů se nazývají počítačoví piráti nebo hackeři. Tito lidé jsou ve většině případů velice chytří a dají se velmi těžce vystopovat, či chytit. Pokud je hacker odborník, dokáže se v kybernetickém prostoru pohybovat tak, že je téměř neviditelný. Proto nikdo neví, kdy a kde udeří. A když se tak stane, dokáže svou identitu změnit během několika minut hned několikrát. Ale počítačová kriminalita není jen o odbornících, tedy o zkušených počítačových pirátech. Jako každý jiný trestný čin i ten kybernetický, může být spáchán z nevědomosti či z nedbalosti. Z toho vyplývá, že ho může spáchat i běžný uživatel.

Pachatelé se tedy dají rozdělit do více skupin. [8]Na odborníky, kteří se v oboru informačních technologií vyznají, vědí, co dělají a vědí, že páchají protiprávní čin a označují se většinou za cílevědomé kriminogenní osobnosti. Vedle nich bychom mohli zařadit počítačové piráty amatéry. To jsou ti, kteří ačkoli něco málo o počítačích vědí, tak to není dostačující, dělají chyby, jsou snadněji vystopovatelní. Většinou dělají

[7] Jirovský, V. *Kybernetická kriminalita*. Vyd. 1. Praha: GradaPublishing, a.s., 2008. s. 19.
[8] Látal, I. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *scritub.com*[online]. 2017[cit. 2017-4-8]. Dostupné z WWW: <http://www.scritub.com/limba/ceha-slovaca/Potaov-informan-kriminalita-a-1513463.php>.

naschvály větším společnostem, nebo jiným uživatelům, například ze msty anebo pro pozornost, a trestné činy páchají spíše příležitostně. Mezi ně by se dali zařadit hackeři nebo crakeři. Dále jsou tu běžní uživatelé, ti o informatice vědí převážně jen základy. Protiprávní činy buď páchají z nevědomosti, nebo z nepozornosti, anebo páchají drobné činy, o kterých vědí, že jsou protiprávní, ale myslí si, že jsou natolik nicotné, že se na ně nepřijde.

3.2 Druhy počítačové kriminality

Jak již bylo řečeno, informační a telekomunikační technologie se vyvíjejí nadměrnou rychlostí, ale její bezpečnostní prvky jsou nedostačující. Daly tak prostor k naplnění hrozeb a k páchání trestných činů za pomocí výpočetní techniky. Počítačová kriminalita se ale nedá řešit podle dosavadních zákonů a právních předpisů, protože kybernetická kriminalita je nový fenomén, se kterým se v nich nepočítalo. Je těžké sjednotit názor na to, co počítačová kriminalita je a jaké jsou její druhy. Natož pak sjednotit návrhy na potlačování kybernetické kriminality a na její postihy. Roku 2001 ale byla Radou Evropy schválena Úmluva o kybernetické kriminalitě, ve které jsou vymezené pojmy, opatření, postihy a mezinárodní závazky pro členské státy, kterou Česká republika podepsala roku 2005 a následně roku 2013.

3.3 Struktura a dělení kybernetických činů, podle mezinárodní smlouvy (Úmluvy Rady Evropy)[9][10]

Oddíl 1. Trestné činy proti důvěryhodnosti, integritě a použitelnosti (dostupnosti) počítačových dat a systémů.

2) Nezákonný přístup

Podle nařízení by měl stát, který smlouvu podepíše, přijmout taková legislativní opatření, aby byl neoprávněný přístup k počítačovému systému, nebo jeho části, pokud je spáchán úmyslně, protizákonný.

V trestním zákoně je uveden v § 230 a tohoto činu se ve většině případů dopouštějí hackeři, kteří prolamují bezpečnostní opatření systém.

3) Nezákonný odposlech

V této části Rada Evropy požaduje, aby jakýkoli nezákonný odposlech pomocí jakéhokoli zařízení, byl protizákonný.

Podle § 88 trestního řádu smí provádět odposlech jen policie s oprávněním od předsedy senátu v případě přípravného řízení na povolení od soudce. V jiných případech je odposlech protizákonný, tudíž je to trestní čin. Tohoto činu se dopouštějí nejen počítačový piráti, ale i běžní lidé, kteří tyto nahrávky většinou využívají k následnému vydírání, či je chtějí použít jako důkazní materiál.

4) Zasahování do dat

Stát by měl přijmout taková legislativní opatření, aby jakékoli úmyslné zasahování do dat, ať se jedná o neoprávněné poškození, vymazání, snížení kvality, pozměnění či potlačením počítačových dat, bylo protizákonné.

Tento protizákonný čin je poznamenán v § 232 trestního zákona. Tohoto činu se opět ve většině případů dopouštějí hackeři. Změna dat nemusí být jen v počítači, ale i v datových nosičích či informačních systémech.

[9] Sbírka mezinárodních smluv č. 104/2013. Praha 2004 [cit. 2017-4-8] s. 10812–10824
[10] Moštěk, M. Úplné znění, Trestní předpisy. *trestnizakonik.cz*[online] 2017 [cit. 2017-4-8] Dostupné z WWW: <http://www.trestnizakonik.cz/>.

5) Zasahování do systému

Stát by měl přijmout taková legislativní opatření, aby jakékoli úmyslné zasahování do systému, ať už se jedná o závažné omezení funkčnosti počítačového sytému vkládáním, přenášením, poškozením, vymazáním, snížením kvality, pozměněním, nebo potlačením počítačových dat, bylo nezákonné.

Tato část je v podstatě poznamenána v každém paragrafu, který souvisí s počítačem například v §230 nezákonný přístup, § 232 zasahování do dat a tak dále. Aby se hacker dostal k citlivým údajům a datům uloženým v počítači, které následně zneužívá, musí zasáhnout do systému.

6) Zneužívání zařízení

V tomto článku Úmluva ukládá, že se musí vytvořit taková legislativní opatření, která upravují úmyslnou a neoprávněnou výrobu, prodej, opatření za účelem použití, dovozu, distribuce, nebo jiné zpřístupnění

- zařízení včetně počítačového programu za účelem spáchání jakéhokoli spáchání trestného činu, které jsou sepsány výše;
- to samé se týká počítačových hesel, přístupových kódů, pomocí nichž lze získat přístup do celého počítačového systému, nebo jeho části;
- dále aby bylo také trestné jejich držení s úmyslem pozdějšího zneužití k protizákonnému činu.

Tento článek je v trestním zákoně poznamenán v § 231 o opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.

Oddíl 2. Trestné činy související s počítačem.

7) Počítačové padělání

V tomto článku se jedná o počítačové padělání. Ukládá se v něm, aby byla přijata taková legislativa, aby bylo každé úmyslné a neoprávněné vkládání, pozměnění, vymazání, nebo potlačení počítačových dat, které povede k nepravosti dat, a to

s úmyslem, aby byla tato data považována za pravá, anebo s nimi bylo jednáno tak, že jsou pravá, bez ohledu na to, zda jsou čitelná a srozumitelná.

8) Počítačový podvod

V tomto článku se ukládá, aby byla přijata taková legislativní opatření, aby bylo trestním činem jakékoli úmyslné a protiprávní jednání, které způsobí ztráty na majetku tím, že vkládáním, pozměňováním, vymazáním, nebo jakýmkoli jiným zásahem do fungování počítačového systému s nečestným úmyslem neoprávněně získat majetkový prospěch jiného.

Oddíl 3. Trestné činy související s obsahem.

9) Trestné činy související s dětskou pornografií

Článek číslo 9 se zabývá dětskou pornografií a vším, co se jí týká. Ukládá, aby státy přijaly taková opatření a legislativu, že všechny úmyslné a protiprávní činy jako jsou:

- výroba a distribuce dětské pornografie prostřednictvím počítačového systému, nabízení nebo zpřístupňování, distribuce nebo přenos, opatřování ať už pro sebe nebo pro jiného to vše pomocí počítačového systému anebo uchovávání dětské pornografie v počítači, nebo na datovém nosiči, byly trestnými činy;

- dále bude legislativní opatření zahrnovat pornografický materiál, který na první pohled, bude znázorňovat nezletilou osobu, která se jednoznačně účastní sexuálního jednání;

- anebo znázorňuje osobu, nebo realistické zobrazení osoby, která se zdá být nezletilou.

Tato trestná činnost je popsána v paragrafech č. § 191, § 192, § 193, § 193 a, § 193b. Na tuto trestnou činnost se kriminalisté, díky své škodlivosti, nejvíce zaměřují.

Oddíl 4. Trestné činy týkající se porušení autorského práva a práv související s autorským právem.

10) Trestné činy týkající se porušení autorského práva a práv souvisejí s autorským právem

Tento článek se zabývá porušením autorských práv a práv, která s nimi souvisejí. V tomto článku se ukládá, aby se zavedla legislativní opatření na základě

- Pařížské revize z 24. července 1971 Bernské Úmluvy o ochraně literárních a uměleckých děl;

- Dohody o obchodních aspektech práv k duševnímu vlastnictví a Smlouvy Světové organizace duševního vlastnictví (WIPO) o právu autorském;

- nebo na základě Mezinárodní úmluvy o ochraně výkonných umělců, výrobců zvukových snímků a rozhlasových organizací;

- Dohody o obchodních aspektech práv k duševnímu vlastnictví a Smlouvy WIPO o výkonech výkonných umělců a o zvukových záznamech, pokud jsou činy spáchány úmyslně, v komerčním měřítku a prostřednictvím počítačového systému.

Trestné činy zabývající se autorskými právy jsou popsány v trestním zákoníku a to v § 270 a v § 271.

Oddíl 5. Další formy odpovědnosti a trestů.

11) Pokus trestného činu a účastenství

V tomto článku Úmluva ukládá, aby se přijala taková legislativní opatření, aby jakákoli forma účastenství, anebo pokusu o trestný čin, který byl zmiňován v článcích 2 až 10, byla považována za trestný čin.

12) Odpovědnost právnických osob

Článek 12 pojednává o právnických osobách a jejich odpovědnosti, která souvisí s trestnými činy, které byly vyjmenovány v předchozích článcích. Ukládá, že právnická osoba může být odpovědná, za trestný čin, který je spáchán jakoukoli fyzickou osobou, v prospěch právnické osoby, ve výkonném postavení, nebo jako člen orgánu na základě pravomoci:

- jednat jménem právnické osoby;
- přijímat rozhodnutí jménem právnické osoby;
- a vykonávat rozhodnutí v rámci právnické osoby.

Dále článek ukládá, že právnická osoba může být uznána odpovědnou v případě, kdy nedostatek její kontroly či dohledu umožnil fyzické osobě spáchat tyto trestné činy v jejím jménu a prospěchu.

13) Tresty a opatření

Článek číslo 13 se zabývá tresty a opatřeními za trestné činy, které byly vyjmenovány ve výše vypsaných článcích. Ukládá, aby bylo možné potrestat fyzické osoby účinnými, přiměřenými a odrazujícími tresty, a to i trestu odnětí svobody.

Dále ukládá, aby bylo možné potrestat právnické osoby přiměřenými, účinnými a odrazujícími trestními a netrestnými sankcemi či opatřeními, a to i včetně peněžitých sankcí.

3.4 Dělení hrozeb (trestných činů) podle Jirovského[11]

Porušení autorizace

Osoba, která je autorizována k použití zdroje pro jistý účel jej použije k jinému, neautorizovanému účelu. Získané informace může například za poplatek nabídnout konkurenci.

[11] Jirovský, V. *kybernetická kriminalita.* Vyd. 1. Praha: GradaPublishing, a.s., 2008. s. 21-24.

Obejití řízení

Útočník využije bezpečnostních mezer v systému, nebo jeho slabin. Tento způsob napadení systému používají hackeři k získání důvěrných informací, nebo naopak systém napadnou, aby ho mohly zevnitř poškodit.

Potlačení služby

Omezení legitimního přístupu k informacím, nebo jiným zdrojům v síti. K tomuto může dojít, pokud útočník nechce, aby byl daný uživatel schopen reagovat na určitý stav v síti a tím, že mu odepře přístup, ho zdrží na potřebnou dobu, které využije k páchání své činnosti.

Nezákonný odposlech

Informace je získávána monitorováním přenosového kanálu. Tento způsob protiprávní činnosti je přímo poznamenán v zákoně č. 141/1961 Sb. Trestní řád v sedmém oddílu v § 88 a § 88a. Nezákonný odposlech je jedna z nejčastěji používaných forem trestné činnosti k získávání informací. Bohužel, je to i jedna z nejjednodušších variant, jak dané informace získat. Útočník se může pomocí WiFi sítě napojit na počítač a na webkameru u notebooku, pomocí níž pak může nejen získávat osobní informace z uživatelova počítače, ale může získávat i uživatelovy fotografie pomocí webkamery, fotografie části jeho pokoje, kanceláře či jiné části domu. Stejně tak se útočník může takzvaně napíchnout i na telefon. Díky dnešnímu technologickému pokroku mají chytrý telefon téměř všichni a díky tomu, že je téměř každý telefon připojen na síť, útočník se na něj může připojit a odposlouchávat nejen hovory, ale může získat přístup i ke správám, či jiným aplikacím, které se využívají ke komunikaci.

Emisní nebo VF odposlech

Informace je extrahována z vysokofrekvenčního vyzařování, nebo emisí či jiných elektromagnetických jevů, ke kterým dochází při provozu elektronického zařízení. S touto formou odposlechu se většina běžných uživatelů nesetká, jedná se většinou o takzvané štěnice.

Nelegitimní použití

Zdroj je používán neautorizovanou osobou, nebo neautorizovaným způsobem. Tuto formu si útočník většinou vybere k tomu, když se chce dostat například do databází s důvěrnými informacemi, anebo například při vniknutí do internetového bankovnictví, kde už ale nejde o informace jako komoditu, ale o peníze jako takové.

Indiskrece

Autorizovaná osoba prozradí důvěrnou informaci neautorizované osobě z neopatrnosti, nebo za úplatu. S touto formou se uživatel nemusí setkat jen přes útočníka, ale spáchat ji může i on sám. A jak již bylo řečeno, může ji spáchat jak úmyslně, tak i neúmyslně.

Únik informace

Získání důvěrné informace neautorizovanou osobou nebo systémem. S únikem informací, se většinou potýkají firmy, ale jednat se může například i o policii, nebo jiné orgány státu. Útočník může získat informace odposlechem a monitorováním dat, anebo k získání informací může využít program k tomu navržený. Program může být v podobě viru, který se do systému dostane například pomocí infikovaného e-mailu.

Narušení integrity

Konzistence dat je narušena jejich neautorizovaným vytvořením, úpravou nebo vymazáním. Tato hrozba je většinou spojována opět převážně s uživatelem jako takovým a k narušení může dojít nejen úmyslným činem, ale i neopatrností uživatele, který nesprávně nakládá s informacemi a informačním systémem.

Změna dat při přenosu

Přenášená data jsou během přenosu informačním kanálem změněna, odstraněna, nebo zcela vyměněna. Jelikož jsou data při přenosu rozložena do takzvaných paketů a následně zase složena, může se stát, že dojde k jejich poškození například ztrátou jednoho nebo více paketů. Taková informace je poškozená, nebo přímo ztracená z důvodu toho, že již nelze otevřít, nebo přečíst. Stát se to může, například když je výpadek elektrické energie, zakolísá signál připojení k síti, nebo je síť přehlcená informacemi. Ke změně dat při přenosu také může dojít úmyslně, kdy útočník uměle

pozmění jeden či více paketů, nebo k informaci přimkne jeden paket, který může obsahovat například vir.

Maškaráda

Jedna entita (osoba, nebo systém) se představuje jako jiná entita. Tuto formu útoku většinou útočník využívá k získání autorizace do informačního systému, do internetového bankovnictví, nebo například k získání přístupu do uživatelského účtu na sociální síti.

Vytěžení odpadových médií

Informace je získávána z magnetických, nebo papírových médií, vyhozených do odpadu. Tato forma získávání informací se opět váže spíše na uživatele, než na útočníka. Získané informace nemusejí být úplné. To ale neznamená, že nejsou důležité. V papírové formě se může jednat například o faktury, kde jsou vytištěny bankovní účty, adresy a tak dále. Pokud se ale jedná o magnetická média, o nich už musí uživatel mít jisté znalosti a zkušenosti, aby z nich dokázal získat nějaká data.

Fyzický průnik

Útočník získá kontrolu nad systémem proniknutím k jeho ovládacím prvkům. K fyzickému průniku tedy dojde tehdy, když útočník může kdykoli převzít kontrolu nad systémem, ať už se jedná o počítač, nebo jiné zařízení a může v něm dělat trvalé změny.

Replay

Zachycená kopie legitimní transakce je využita pro opětovný přenos s nelegitimním úmyslem. S touto formou se může uživatel setkat například, když on využije klíč například k programu či hře, který byl již použit jiným uživatelem, který si ho zakoupil anebo naopak.

Popření skutečnosti

Strana zúčastněná ve vzájemné komunikaci později popře, že k takové komunikaci došlo. Tato forma hrozby je všudypřítomná. Ať už se jedná o komunikaci mezi uživateli tedy pracovníky jedné firmy nebo mezi zákazníkem a prodejcem. Proto

je dobré si vždy důležitou konverzaci uložit, zálohovat na přenosný disk, nebo vytisknout a tím předejít pozdějším rozepřím.

Vyčerpání zdrojů

Jistý zdroj, např. port, je úmyslně natolik zatížen, že je znemožněno používání služby, která je na něj vázána řádnými uživateli. Tato situace může nastat úmyslně i neúmyslně. Neúmyslně může nastat při zahlcení internetové databáze například registru vozidel. Znamená to, že spousta uživatelů začne využívat jednu službu v ten samý čas a síť, protože je zahlcená informacemi, v tomto případě žádostmi, spadne. Úmyslné zahlcení může nastat tehdy, když útočník chce naschvál shodit nějaký portál či službu a posílá obrovské množství dat. Tím opět dojde k zahlcení sítě.

Podvržení služby

Podvržený systém nebo systémová komponenta, která se vůči uživateli chová jako běžná součást systému, slouží k získání citlivých informací od důvěřivého uživatele.

Krádež

Kritický prvek bezpečnostního systému (např. přístupová karta nebo veškeré citlivé informace) jsou zcizeny. S touto formou hrozby se může uživatel setkat fyzicky tím, že mu pachatel ukradne čipovou kartu, nebo pachatel vnikne do počítače a přímo z něho odcizí důvěrné informace. Dále se s touto formou může uživatel setkat tím způsobem, že on sám odcizí důležité informace (například z firemních disků).

Zadní vrátka

Do systému je zabudována vlastnost nebo vložena součást, která při jisté konstelaci vstupních dat umožní obejít bezpečnostní mechanismy. Zadní vrátka jsou velmi častou formou získávání informací, ať už se jedná o firemní citlivé informace, nebo citlivé informace ze soukromých zařízení (počítačů, mobilů atd..). Pachatelem může být přímo uživatel, například když program určený k získávání informací vědomě nainstaluje v práci, který si předem uložil na flash disk. Nebo si uživatel neúmyslně otevře infikovaný e-mail, ke kterému je přidaný vir, který má za úkol posílat citlivé údaje do útočníkova zařízení.

Trojský kůň

Software obsahuje zdánlivě nevinnou, nebo neviditelnou část kódu, který – pakliže je spuštěn – ohrozí bezpečnost uživatele. Trojský kůň je škodlivý program, vir, který se tak nazývá, protože se většinou uživateli jeví jako program jiný, s jinou funkcí, nebo je částí jiného programu. Uživatel se s ním většinou setká tím, že si stáhne program, nebo dokument z neprověřených internetových stránek. Proti tomuto škodlivému programu se uživatel může bránit pomocí antivirového programu, který pravidelně aktualizuje, nebo když si všimne, že dokument, který si stáhl, má příponu .exe, okamžitě ho odstraní ze svého počítače, či jiného zařízení.

3.5 Formy počítačové kriminality

Hacking[12]

Pojem hacking znamená neoprávněný přístup k počítačovému systému či nosiči. Hackerství je díky tomu, že hackeři překonávají bezpečnostní opatření a přístupová práva, trestným činem a provádí ho takzvaní hackeři. Hackeři využívají chyb v systému a slabostí k tomu, aby do daného systému pronikli a dále získali přístup k citlivým údajům či jiným soukromým informacím v uživatelském počítači či jiném elektronickém zařízení (například mobilu).

Hacker může pomocí svých vědomostí a pomocných programů získat plnohodnotný přístup k cizímu počítači a dále ho zneužívat. Zneužití může být jednorázové, například vykradení dat z uživatelova účtu na sociální síti, nebo dlouhodobé, kdy při jeho útoku vloží do počítače škodlivý program, takzvaný backdoor, anebo keylogger, a dlouhodobě čerpá informace z obětního počítače a následně je zneužívá.

Craking[13]

Craking je prolamování nebo obcházení ochranných prvků elektronických nebo programových produktů s cílem jejich neoprávněného použití. Craking používá celou řadu metod od prostého debutování spuštěného programu, až po tzv. reverse engineering (to znamená zkoumání daného programu a vytvoření jeho kopie, která je ovšem většinou neúplná, to znamená, že chybí ta část kódu, kam se například k puštění programu zadával uživatelský klíč). Cracking je často používaná metoda při průniku do systému, kde cílem crackingu není „zprovoznění“programu chráněného softwarovým nebo hardwarovým klíčem, ale zjištění informací důležitých pro umožnění neoprávněného přístupu do cílového systému. Nejčastěji se jedná o tzv. „pasword cracking“ což znamená zjišťování hesla pro přístup do systému. Password cracking má širokou škálu metod od snahy uhodnout heslo pomocí slovníku nejčastěji používaných hesel, použití hrubě síly při zkoušení všech možných kombinací znaků přicházející v úvahu, až po sofistikované algoritmy snažící se o zpětnou rekonstrukci odpovídající kombinace znaků ze zakódovaného řetězce hesla, uloženého v systémovém souboru s hesly.

[12]Kyberkriminalita. *Policie.cz.*[online]. 2017 [cit. 2017-4-8]. Dostupné z WWW: <http://www.policie.cz/clanek/kyberkriminalita.aspx?q=Y2hudW09Mw%3d%3d>.
[13] Jirovský, V. *Kybernetická kriminalita*. Vyd. 1. Praha: GradaPublishing, a.s., 2008. s. 106.

Spamming[14]

Pojem spam, znamená nevyžádanou či nechtěnou poštu, která má komerční obsah. Což znamená, že prostřednictvím spamových zpráv, či e-mailů spammer (ten kdo tyto zprávy rozesílá) hromadně rozesílá e-maily, které uživatelům zahlcují emailové schránky. Ale nemusí to být jen o bezvýznamných komerčních zprávách, které nabízejí to či ono, ať už se jedná o podvodné nabídky nebo ne, prostřednictvím spammingu se mohou rozesílat například i hoaxové zprávy, nebo zprávy, které jsou infikované škodlivými viry, kterými si uživatel může poškodit počítač.

Další možnost, kde se uživatel může setkat se sparingem, je například v diskusních fórech, na sociálních sítích ve formě komentářů, atd. Zkrátka spam je určen k propagaci ať už nějakého zboží, určité situace, nebo k propagaci autora, služby, nebo firmy.

Proti spammům se lze částečně bránit tím, že si uživatel zapne anti-spamové filtry ve své emailové schránce, které si sám může nastavit a sám si koriguje, jaké zprávy do spamového seznamu přidá.

Hoax[15]

Anglické slovo HOAX v překladu znamená falešnou zprávu, mystifikaci, novinářskou kachnu, podvod, poplašnou zprávu, výmysl, žert či kanadský žertík. V počítačovém světě slovem HOAX nejčastěji označujeme poplašnou zprávu, která varuje před neexistujícím nebezpečím. Hoax většinou obsahuje i výzvu žádající další rozeslání hoaxu mezi přátele, příp. na co největší množství dalších adres. Proto se někdy označuje také jako řetězový e-mail.

Hoax operuje s efektivním využíváním jazyka s využitím základních principů mediální komunikace v kombinaci s efektivním působením na city příjemce. Stejně jako běžné mediální produkty, jako například různé reklamy, pracují s hoaxy, které poukazují a pracují s různými problémy. Obsahovou konstrukci pak doprovázejí „osobními důkazy“ a „logickými argumenty“. Často je tvrzení pisatele doprovázeno

[14] Spam. *It-slovnik.cz*. [online]. 2017 [cit. 2017-4-8]. Dostupné z WWW: <http://it-slovnik.cz/pojem/spam>.
[15]Kopecký, K. Co je hoax. *E-bezpeci.cz*. [online]. 2008 [cit. 2017-4-8]. Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25>.

velmi expresivními obrázky (nádory, tělesná postižení, oběti autonehody, nebezpečná zvířata…) tak, aby co nejefektivněji zaujali příjemce těchto zpráv.

Hoaxy, kromě toho, že jsou nepravdivé a mohou rozšířit zbytečnou paniku, obtěžují příjemce, mohou poskytovat nebezpečné rady, zbytečně zatěžují servery, touto formou také může dojít k cílenému přetěžování konkrétní e-mailové schránky, může dojít k poškození dobrého jména konkrétní instituce a na konec může dojít i k prozrazení důvěrných informací například osobního emailu.

Phishing[16]

Každý ví, co znamená rybařit, nebo chytat ryby. Na rybářský prut se připevní návnada, která se poté hodí do rybníka či řeky a čeká se, jestli se nechytne nějaká ryba. Termín phishing v českém překladu rhybaření pracuje na obdobném principu tedy na digitální návnadě, která se místo do rybníku umístí na Internet. Počítačoví piráti používají tuto formu počítačové kriminality k tomu, aby z nic netušících a naivních uživatelů získaly jejich citlivé osobní údaje, hesla, jejich uživatelská přihlášení například k emailu, nebo přístupy k jejich bankovním účtům. Phishing jako forma kyber kriminality vznikla asi v polovině 90. let, kdy mezi rokem 1995 a 1996 byly pravidelné phishing útoky na poskytovatele internetových služeb v americe, American Online, kdy hackeři podvedli uživatele k získání jejich citlivých údajů o jejich kreditních kartách pomocí podvodných emailů s falešnou zprávou o problémech s jejich financemi.

Od té doby se tato forma kybernetické kriminality zlepšila natolik, že je těžce rozeznatelný pravdivý email od toho zfalšovaného. Většinou hackeři posílají email, který působí, jako by byl zaslán z velice důvěryhodného zdroje, například přímo z jejich banky. Přitom je celý zfalšovaný, nebo jen jeho část, kdy je ke zdrojovému kódu připojen další, který zaznamenává všechny informace od uživatele, kterému byl phishingový email zaslán. Funguje to tak, že když se uživatel proklikne pomocí odkazu v zaslaném emailu, místo na originální stránky jejich internetového bankovnictví je to nasměruje na podvodně stránky, které vypadají téměř stejně až na drobné odchylky, které ale běžný uživatel většinou nerozpozná. Dále když uživatel vyplní svoje přihlašovací údaje tak, je hacker může snadno zneužít ke svému prospěchu.

[16]McQuade, S.C. *EncyclopediaofCyberCrime*. Firstedition. 2009. USA: GreenwoodPublishing Group, Inc. S. 139-141.

Pharming[17]

Pharming je modernější forma phisingu, která ke svému šíření nevyužívá e-maily, ale počítačoví piráti pracují rovnou s internetovou doménou. Například, když uživatel zadá internetovou adresu svého internetového bankovnictví, tak místo na originální stránky banky se jim zobrazí falešná stránka, ze které získávají citlivé informace poté, kdy je uživatel zadá do příslušných okének.

Spamming, Hoax, Phishing a Pharming, jsou nejčastější formy kybernetické kriminality, se kterou se běžní uživatelé můžou nejčastěji setkat. Tyto formy nejen že používají podobné nástroje k jejich šíření, ale také spolu úzce spolupracují a hackeři toho využívají. Proto je velice nebezpečné otevírat e-mail, který je původem nejasný, je díky svému obsahu podezřelý, nebo v nejhorším případě obsahuje přílohu, většinou ve formě .exe souboru.

Identity theft[18]

Doslovný překlad je krádež či odcizení identity běžných uživatelů. Tato technika je oblíbená především v USA. Využívá toho, že při prokazování identity po internetu je vyžadováno ověření zpravidla jedním způsobem. Stačí tedy získat například číslo sociálního pojištění (v USA něco jako rodné číslo u nás, což není veřejný údaj, ale také není tajný) nebo číslo kreditní karty. Všechny popsané metody se stávají obyčejným uživatelům velmi nebezpečné a v poslední době i časté. I v ČR bylo zaznamenáno několik případů odčerpání nemalých částek z účtů klientů bank. Bohužel v současné době banky u nás někdy přesouvají zodpovědnost za úniky informací a finanční ztráty na koncové uživatele bez dostatečné informační kampaně. Zavedení doplňkových bezpečnostních prvků je pomalé nebo nedostatečné. Bankovní konto však není jediným cílem hackerů. Lákavé jsou jakékoliv zpeněžitelné či jinak využitelné informace. Od lékařských záznamů přes osobní nebo ekonomická data až po například právní informace a různé smlouvy.

Běžní uživatelé se s touto formou mohou také často setkat, když jim druhá strana „ukradne“ jejich identitu na sociální síti například na facebooku, nebo na instagramu,

[17]McQuade, S.C. *EncyclopediaofCyberCrime*. Firstedition. 2009. USA: GreenwoodPublishing Group, Inc. s. 140.
[18]Macháček, M. Počítačová kriminalita a bezpečnost. *Internetprosvechny.cz.*[online]. 2013. [cit. 2017-4-8]. Dostupné z WWW: <http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/>.

kde se poté druhá strana vydává za originálního uživatele, kde poté může například žádat peníze od přátel a rodiny původního uživatele.

Warez[19]

V počítačovém slangu se softwarový piráti označují pojmem warez. Jedná se o jednu z nejrozšířenějších forem počítačové kriminality, která se ovšem velmi těžce potlačuje. Jedná se o trestnou činnost, kdy softwaroví piráti šíří prostředky k odstranění ochranných prvků, které slouží k ochraně autorských děl, nebo je rovnou sami odstraní a takhle pozměněný software dále šíří. Ovšem spolu s ním se většinou také šíří počítačové viry, které pak dovolují další páchání trestné činnosti jako například phishing, nebo ukradení identity.

Druhy warez

- **Aplikace** = různé kancelářské balíky bez potřeby zadat koupený uživatelský klíč
- **Cracky** = takzvané záplaty, určené ke změnění zkušební verze softwaru na plnou verzi, nebo k obejití softwarové ochrany například není nutné originálního instalačního CD
- **Keyloggers**= balíček registračních a instalačních klíčů, či jejich generace.
- **Hry** = různé pirátské kopie her.
- **Filmy** = různé neoprávněně pořízené kopie filmů.
- **MP3/Music** = různé pirátské kopie hudby.
- **Knihy** = pirátské kopie knih v podobě epub formátů.

Kyberšikana[20]

Kyberšikana, má v podstatě ten samý význam jako šikana jako taková a není trestným činem, nýbrž přestupkem anebo jiným správním deliktem. Rozdíl je ale v tom, že kyberšikany se dopouští ten, kdo šikanuje druhého pomocí elektronických prostředků. V dnešní době se nejvíce využívají ke kyberšikaně sociální sítě.

[19]Warez. *Pocitacova-kriminalita.webnode.sk*. [online]. 2014. [cit. 2017-4-8]. Dostupné z WWW: <http://pocitacova-kriminalita.webnode.sk/nieco-k-teme/warez/>.
[20]Kyberkriminalita. *Policie.cz.* [online]. 2017. [cit. 20117-4-8]. Dostupné z WWW: <http://www.policie.cz/clanek/kyberkriminalita.aspx?q=Y2hudW09NA%3d%3d>.

Zneužívání dětí[21]

Zneužívání dětí je jeden z nejzávažnějších problémů dnešní doby, který se stále nepodařil potlačit. Díky tomu, že je internet anonymní a uživatelé mnohdy ani ve skutečnosti nevědí, kdo si s nimi na druhé straně sítě dopisuje, je pro pachatele velice snadné si vytvořit fiktivní účet především na sociálních sítích a následně vyhledávat a kontaktovat své potencionální oběti. Z toho také vyplývá, že pachatel nejdříve využívá techniku zvanou kybergrooming. Když naváže pachatel kontakt s obětí tak se z ní snaží vylákat fotografie, na kterých je obnažená, či fotografie se sexuálním kontextem, dále pokračuje videi, či vysíláním v přítomném čase pomocí webkamery.

Oběti si většinou ze začátku neuvědomují, že se oběťmi staly, a fotografie se sexuálním kontextem pachateli zasílají. Pachatel poté oběti může vydírat zaslanými fotografiemi se sexuálním podtextem a může požadovat schůzku s oběťmi, na kterých po nich bude vyžadovat sexuální styk či další materiál se sexuálním podtextem.

Pachatelé se dále dopouštějí trestných činů souvisejícími s dětskou pornografií, zneužíváním dětí a v nejhorších případech i únosech a obchodů s bílým masem.

Kybergrooming[22][23]

Kybergrooming není trestným činem, ale jedná se o takové jednání pachatele, který svým jednáním manipuluje dětské či náctileté oběti za účelem sjednání schůzky a následného sexuálního zneužití či ublížení na zdraví.

Kybergrooming má úzkou vazbu k trestnému činu „Svádění k pohlavnímu styku“. Tito pachatelé vyhledávají své oběti převážně na sociálních sítích, nebo v soukromých chatových místnostech, kde se snaží svou oběť přimět k obnažování, nebo erotickému sebeukájení, které pachatelé sledují pomocí webkamery a následně se snaží oběť přemluvit ke schůzce za účelem pohlavního styku za úplatu, nebo pomocí vydírání.

[21] Zneužívání dětí na internetu. *Policie.cz*. [onine]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <http://www.policie.cz/clanek/zneuzivani-deti-na-internetu.aspx>.
[22] Zneužívání dětí na internetu. *Policie.cz*. [onine]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <http://www.policie.cz/clanek/zneuzivani-deti-na-internetu.aspx>.
[23] Kopecký, K. *KYBERGROOMING. Nebezpečí kyberprostoru.* Olomouc: NET UNIVERSITY s.r.o. 2010. s.3-4.

Tato hrozba se stala fenoménem posledních let, protože moderní společnost a hlavně mladší generace využívají sociální sítě k navázání přátelství, ale i vztahů. Problém je ale ten, že si tito lidé neuvědomují, že na druhém konci sítě ta osoba, se kterou si píší, nemusí být nezbytně ta osoba, za kterou ji považují.

Podvodné E-shopy[24]

Svět e-shopů zažívá posledních pár let veliký rozmach. Lidi se pomalu ale jistě naučily věřit internetovým obchodům a nakupují přes ně vše od drogerie po oblečení, nebo elektroniku. Nakupovat přes internetový obchod je velmi pohodlné. Nejen, že ceny bývají příznivější než v kamenných obchodech, ale zboží vám ještě pohodlně dovezou až domů. Příznivá cena a mnohdy až podezřele nízká cena je ten problém. Zvláště, když daný e-shop má jen jeden druh platby, a to platbu předem. Následně vám zašlou maketu zboží, které jste si objednali, nebo zboží velmi nízké kvality, anebo vám nezašlou zboží žádné.

Další druhy trestných činů, které souvisejí s internetovými obchody, jsou trestný čin legalizace výnosů z trestné činnosti, případně se dopouštějí jiných trestných činů formou podílnictví, a to tím způsobem, že pachatelé nabízejí jiným osobám práci administrativního charakteru. Tyto osoby figurují spíše, jako prostředníci, kteří si založí bankovní účet, na který jsou zasílány peníze z podvodných e-shopů a následně jsou přeposílány pachatelům. Tímto způsobem se jak prostředníci, tak i pachatelé dopouštějí trestného činu, ale díky tomu, že pachatelé jednají přes prostředníka, je těžší je vystopovat.

Malware[25]

Malware jsou počítačové programy, které byly vytvořeny k tomu, aby škodily. Dnešní počítačový svět zná mnoho druhů malwaru, které mají také různé funkce a neustále se vyvíjejí a mutují, proto se dají rozdělit především podle toho, co tyto počítačové programy způsobují. Nejčastějšími druhy malwaru jsou především tyto:

- **Adware** = tento software má za úkol sbírat data o uživateli, jaké stránky navštěvuje a jaká jsou jeho nejčastější vyhledávaná klíčová slova. Poté jsou

[24] Podvodné e-shopy. *Policie.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <http http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx>.
[25]McCarthy, L. a Weldon-Siviy, D. *Buď pánem svého prostoru. Výzkum malwaru*. Praha: CZ.NIC. 2013 s. 32-33.

na základě těchto informací zasílána reklamní sdělení a nabídky, ačkoli si to uživatel často nepřeje. Tyto reklamní nabídky mohou být zobrazovány na webových stránkách, nebo mohou být zobrazovány ve volně stažitelných programech, například se mohou zobrazovat v dolní, nebo postranní části herních aplikací.

- **Backdoor** (neboli zadní vrátka) = tento program způsobuje to, že po jeho proniknutí a naistalování do uživatelského počítače (obětního), pachatel již dále nepotřebuje zdolávat bezpečností ochrany počítače a může čerpat data a citlivé informace bez toho, aby o tom uživatel (oběť) věděl.

- **Logické bomby**= jsou parazité, kteří jsou zakomponováni do volně stažitelných programů a aktivují se v případě, že se splní podmínka, na kterou byli naprogramováni. Tyto bomby mají při spuštění většinou za následek ztrátu, nebo poškození dat v softwaru, poškození, nebo okamžité zkolabování softwaru jako takového.

- **Trojské koně** = to jsou takové programy, které kromě věci, kterou mají vykonávat, vykonávají věc jinou, zkrátka se tváří jako neškodný program ale zároveň vykonává jinou, škodlivou činnost na pozadí. Například se může jednat o sběr informací a hesel, která jsou následně zasílána na útočníkův počítač.

- **Viry**= jsou něco jako parazité a vždy potřebují hostitelský program. Viry jsou většinou vytvořené jen k tomu, aby škodily. Když se dostanou do počítače s již napadeným programem, například, který si uživatel stáhl z internetu jako hru, chovají se jako viry ve skutečném světě a napadají okolní programy, až dojde k poškození softwaru.

- **Červy**= červ je škodlivý program, který se šíří po síti a napadá počítače, které jsou touto sítí propojeny a nenávratně ničí data na těchto počítačích uložená.

- **Zombie** = je takový škodlivý program, s jehož pomocí může útočník napadený počítač následně ovládat ze svého počítače. Pokud, ale je více počítačů napadených stejným škodlivým programem, stává se z této skupiny počítačů botnet, který útočník dále může využívat například ke spammingu.

- **Ransomware**= tento škodlivý software způsobuje zablokování počítače, nebo jen jeho části, či jen programů, kdy po uživateli útočník vyžaduje zaplacení, dalo by se říci výkupného k tomu, aby byl jeho počítač znovu odblokován.

4 Kybernetické prostor a právo

4.1 Trestný čin

Trestní čin je podle trestního zákoníku[26]: protiprávní čin, který trestní zákon označuje za trestný, a který vykazuje znaky uvedené v takovém zákoně. K trestní odpovědnosti za trestný čin je třeba úmyslného zavinění, nestanoví-li trestní zákon výslovně, že postačí zavinění z nedbalosti. Úmyslný trestný čin, je ten trestný čin, který je spáchán úmyslně, jestliže pachatel chtěl způsobem uvedeným v trestním zákoně porušit nebo ohrozit zájem chráněný takovým zákonem, nebo věděl, že svým jednáním může takové porušení nebo ohrožení způsobit, a pro případ, že je způsobí, byl s tím srozuměn. Srozuměním se rozumí i smíření pachatele s tím, že způsobem uvedeným v trestním zákoně může porušit, nebo ohrozit zájem chráněný takovým zákonem.

4.2 Legislativa

Následující zákony jsou zákony, které se nejvíce týkají běžných uživatelů, jejich soukromí, nebo informací se kterými je nakládáno, nejen na internetu, ale například i na úřadech. Právě soukromí uživatelů, sdílená data a informace v kybernetickém prostoru jsou předmětem těchto zákonů. Zákony, jsou sobory pravidel, kterými by se měli řídit všichni nejen v normálním světě, ale i v tom virtuálním, a je důležité, aby se předešlo jejich porušení, nebo zneužití.

[27]Základním a nejvýznamnějším právním předpisem, je Základní listina práv a svobod. Tato listina, respektive článek č. 13 nám říká, že „*nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením*.“[28] Tento článek se tedy doslova týká například kybernetických útoků na emailové schránky. Dále se touto problematikou zabývá také

[26] Trestní zákoník. *Zakonyprolidi.cz.*[online]. 2009. [cit. 2017-4-8]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>.
[27]Matejka, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*.Vyd. 1. Praha: CZ.NIC. 2013, s. 128.
[28] Listina základních práv a svobod. *Psp.cz.*[online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <http://www.psp.cz/docs/laws/listina.html>.

zákon č. 127/2005 Sb., o elektronických komunikacích[29], který řeší například ochranu proti úniku osobních dat a informací při využívání telekomunikačních zařízení.

Velice důležitým zákonem pro počítačové uživatele, jejich bezpečnost v kybernetickém prostoru, je [30]zákon č. 181/2014 Sb. o kybernetické bezpečnosti. Tento zákon upravuje „*práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti*". Tento zákon upravuje nejen práva a povinnosti osob, ale také působnost a pravomoci orgánů veřejné moci, které nějakým způsobem nakládají s kybernetickým prostorem a s kritickou informační infrastrukturou, ať už jako poskytovatelé, nebo jako správci sítí, anebo jinak zasahují do oblasti kybernetické bezpečnosti. Dále tento zákon také upravuje práva a povinnosti národního CERT týmu, který se zabývá především ochranou kritické informační infrastruktury.

Další důležitý zákon, který by měli znát všichni počítačoví uživatelé, je zákon o autorských právech č. 121/2000 Sb. Tento zákon se zabývá autory a jejich právy vůči jejich dílu, ať už se jedná o „*dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické, dílo fotografické a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo kinematografické, dílo výtvarné, jako je dílo malířské, grafické a sochařské, dílo architektonické včetně díla urbanistického, dílo užitého umění a dílo kartografické*".[31] Dále se tento zákon zabývá rozmnožováním těchto děl, nebo jejich pronájmem či půjčováním. Dále se tento zákon také zabývá tím, jak správně citovat z děl, aniž by uživatel porušil autorské právo.

Zákon č. 106/1999 Sb. o svobodném přístupu k informacím, je zákon, který se týká všech počítačových uživatelů. Tento zákon především „*zpracovává příslušné předpisy Evropské unie* a *upravuje pravidla pro poskytování informací a dále upravuje podmínky práva svobodného přístupu k těmto informacím*".[32] Tento zákon určuje, jaké objekty mají povinnost poskytovat informace a za jakých podmínek, dále jaké subjekty nesmějí poskytovat informace a za jakých podmínek, a jaké jsou postupy při získávání těchto informací.

[29]Zákon o elektronických komunikacích. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-127>.
[30] Zákon o kybernetické bezpečnosti. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/2014-181>.
[31] Autorský zákon. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/2000-121>.
[32] Zákon o svobodném přístupu k informacím. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/1999-106>.

Další zákon, který je vhodné, aby počítačový uživatel znal, je knihovní zákon č. 257/2001 Sb. Ačkoli se tento zákon zabývá knihovnami a jejich službami, je velice užitečný právě s návazností na autorský zákon a na zákon o svobodném přístupu k informacím. Především je důležité, že „*bez rozdílu zaručuje rovný přístup všem, kdo chtějí využít veřejné a informační služby*“[33].

Dalším velice důležitým zákonem, je zákon č. 101/2000 Sb. o ochraně osobních údajů. Tento zákon se především zabývá poskytováním ochrany „*před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států*“[34]. To znamená, že tento zákon je důležitý pro všechny lidi bez rozdílu, protože s jejich osobními údaji se nakládá denně například v práci, nebo na úřadu, a jejich zneužití by mohlo napáchat veliké škody. Pachatel může využít základní osobní údaje například jméno a příjmení, adresu trvalého bydliště a telefonní číslo k tomu, aby se naboural do internetového bankovního účtu a následně odcizil peníze na něm uložené.

Zákon 365/2000 Sb. o informačních systémech veřejně zprávy, je dalším zákonem, který pracuje s ochranou informací tím, že zpracovává a vytváří informační systémy a zajišťuje jejich integritu. Jeden z takových systémů se nazývá portál veřejné správy, který spravuje ministerstvo. Portál veřejné správy zajišťuje především „*přístup k informacím získaným na základě informační činnosti veřejných orgánů zejména v oblasti sociálního zabezpečení, zdravotnického zabezpečení, správy veřejných financí, dotací, veřejných zakázek, státní statistické služby, evidence a identifikace osob, jejich součástí a práv a povinností těchto osob či jejich součástí a tvorby a publikace právních předpisů*.“[35]

Dalším důležitým zákonem, který je porušovaný, je zákon 412/2005 o utajovaných informacích. Tento zákon *„upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy“.*[36]Tento zákon také určuje stupně utajení, a jací lidé k nim

[33] Knihovní zákon. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/2001-257>.
[34] Zákon o ochraně osobních údajů a o změně některých zákonů. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/2000-101>.
[35] Zákon o informačních systémech veřejné správy. *Zakonprolidi.cz.*[online]. 2017 [cit-2017-4-8]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2000-365>.
[36] Zákon o ochraně utajovaných informací. *Zakonyprolidi.cz*[online]. 2017 [cit- 2017-4-8]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-412>.

mají oprávněný přístup. Zákon dále stanovuje ochranu těchto informací, a kdo ji zajišťuje.

Dále je vhodné zmínit zákon č. 40/2009 Sb. trestní zákoník[37], ve kterém jsou pro uživatele informačních technologií důležité například § 180 Neoprávněné nakládání s osobními údaji, § 191Šíření pornografie, nebo § 230 Neoprávněný přístup k počítačovému systému a nosiči informací a další…

Tyto zákony jsou tvořeny takzvaně za pochodu. Počítačová kriminalita, je nejmladší fenomén v trestním zákoně vůbec. A proto ne všechny zákony stačí pokrýt ten přehršel přestupků a trestných činů, se kterými se moderní společnost potýká. Anebo naopak již nejsou aktuálními. Počítačová kriminalita jde díky vývoji techniky stále dopředu a čím dál tím rychleji jako nikdy dříve. Vedle kybernetické kriminality, jde ruku v ruce Cybersecurity (kybernetická bezpečnost) a právě do tohoto oboru spadají veškeré zákony, metody, doporučení, jak se proti kybernetické kriminalitě bránit, od jednotlivce po firmy až po stát a státní uskupení jako je evropská unie.[38]

4.3 Kdo se ochranou kybernetického prostoru zabývá a kdo ji řeší

Ochrana kyberprostoru se v posledních letech stává prioritou nejen v České republice, ale i světě. Postupem času se formuje stále více organizací a týmů, které mají na starosti kybernetickou bezpečnost, nebo studují její hrozby a dopady na společnost. [39]Nejznámější organizace, které se zabývají kybernetickou bezpečností, jsou nadnárodní organizace TERENA (Trans-EuropeanResearch and Education Networking Association), organizace FIRST (Forumof Incident Response and Security Teams) a ENISA (European Network and InformationSecurityAgency). Mezi týmy, které se zformovaly a působí v České republice a zapojují se do řešení otázek kybernetické bezpečnosti, patří především tým CERT (ComputerEmergency Response Team) a tým CSIRT (ComputerSecurity Incident Response Team). Tyto týmy, jsou formovány v téměř každé organizaci, ve které je otázka kybernetické bezpečnosti velmi důležitá, dále spolu týmy spolupracují a předávají si informace a doporučení. Oficiální týmy CERT a CSIRT jsou členy, anebo mají akreditace od organizací jako je TERENA, nebo FIRST.

[37] Zákon trestní zákoník. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/2009-40>.
[38]Matejka, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*.Vyd. 1. Praha: CZ.NIC. 2013, s. 25.
[39] Kropáčová, A. CERT/SCIRT týmy a jejich role. *Root.cz*. [online]. 2013. [cit. 2017-4-8]. Dostupné z WWW:<https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/>.

V České republice je v současnosti pět týmů, které jsou akreditovány a napojeny na světovou infrastrukturu těchto bezpečnostních týmů a organizací. Jsou to týmy CESNET-CERTS[40], které se zabývají bezpečnostními incidenty v sítích CESNET, CSIRT-MU[41] bezpečnostní tým Masarykovy univerzity, který se zabývá nejen bezpečností univerzitní počítačové sítě, ale i výzkumem kybernetické bezpečnosti. Dále je to CZ.NIC-CSIRT[42] tým, který provozuje sdružení CZ.NIC a zabývají se především incidenty s doménami .CZ, tým ACTIVE24-CSIRT[43], který se zabývá bezpečnostní otázkou na jejich serveru především, co se týká registrací domén a webhostingu. Poslední oficiální tým je CSIRT.CZ, který je národním CSIRT týmem České republiky a je zřízen na základě veřejnoprávní smlouvy uzavřené s Národním bezpečnostním úřadem a provozuje ho sdružení CZ.NIC. Národní CERT tým GovCERT.CZ [44] je pod záštitou Národního centra kybernetické bezpečnosti a nabízí pomoc při řešení kybernetické bezpečnosti.

Tyto týmy se zabývají otázkou kybernetické bezpečnosti a mají za úkol podle zákona 181/2014 Sb., ochránit kritickou informační infrastrukturu a významné informační systémy, dále udržovat vztahy se světovou komunitou CERT a CSIRT týmů a organizacemi, které tyto týmy podporují. Dále tyto týmy pomáhají nejen při řešení incidentů, ale působí i preventivně a edukačně v oblasti kybernetické bezpečnosti.

Další, kdo se zabývá ochranou kybernetického prostoru, je samozřejmě Police České republiky, zpravodajské služby Ministerstvo obrany, Bezpečnostní informační služba a Ministerstvo vnitra. Nejvíce trestných činů, které policie eviduje, jsou zejména podvodná jednání, hacking, mravnostní delikty, autorskoprávní delikty a násilné projevy (hatecrime), zbytek trestních kybernetických trestných činů označují jako ostatní a od roku 2011 do roku 2016 se počet těchto činů neustále zvyšuje. [45]

[40] O nás. *Csirt.cesten.cz*. [online]. 2016. [cit. 2017-4-8]. Dostupné z WWW:<https://csirt.cesnet.cz/cs/index>.
[41] Jsme CSIRT-MU. *Csirt.muni.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://csirt.muni.cz/>.
[42] CSIRT.CZ. *Nic.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.nic.cz/csirt/>.
[43] ACTIVE24-CSIRT. *Active24.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.active24.cz/csirt/>.
[44] GovCERT.CZ. *Govcert.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.govcert.cz/cs/vladni-cert/govcert-cz/>.
[45]Kyberkriminalita. *Policie.cz.* [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<http://www.policie.cz/clanek/kyberkriminalita.aspx>.

4.4 Případ trestné činnosti

V ČR jsou nejčastěji páchaná podvodná jednání a to z více jak 60% z celkové kybernetické kriminality[46]. Konkrétně běžné uživatele například nejvíce ohrožují internetové obchody, které jsou nejjednodušším způsobem, jak si mohou podvodníci vydělat a poté zmizet z internetového prostoru, aniž by na ně policie přišla. Nebezpečí hrozí celý rok, ale nejvíce podvodných internetových obchodů vzniká během svátků konkrétně pak o Vánocích, kdy spousta lidí nakupuje dárky. Snaží se co nejvíce ušetřit, takže si vůbec neuvědomují, že podezřele nízké ceny mohou znamenat podvodné jednání.

V roce 2016 policie dopadla dva muže, kteří na podvodných e-shopech s elektronikou okradli lidi o více než 4 000 000 korun. Dosáhli toho tak, že si nechali za své zboží platit předem a poté peníze posílali na účty do Dominikánské republiky. Oba muži jsou nyní ve vězení.[47]

5 Dotazníkové šetření

Ke sběru dat, která budou následně použita a vyhodnocena, bylo provedeno dotazníkové šetření, jehož cílem bylo zjistit všeobecnou povědomost uživatelů o kybernetické kriminalitě a o základních bezpečnostních pravidlech při používání počítače. Dotazníkové šetření je metoda/nástroj ke sběru dat, která jsou následně dále zpracována a využita k analýze zvoleného tématu.

Dotazníkové šetření na téma kybernetická kriminalita bylo distribuováno pomocí internetových stránek vyplnto.cz[48]a uskutečnilo se v březnu 2017. Dotazníkového šetření se zúčastnilo 133 respondentů ve věku 14 a výše let. Dotazník byl anonymní, aby se respondenti cítili jistěji a tím spíše odpovídali pravdivě, bez případných obav ze zveřejnění výsledků. Otázek bylo celkem 28 a byly jednoduché, uzavřené, převážně zaměřené na jednoznačnou odpověď ano, nebo ne. Tím tak pomohly snadněji vyhodnotit, jakou mají uživatelé povědomost o bezpečnosti svého počítače a bezpečnosti internetu.

[46]Kyberkriminalita. *Policie.cz.* [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<http://www.policie.cz/clanek/kyberkriminalita.aspx>.
[47]Matzner, J. Policie dopadla dva podvodníky. Pomocí e-shopů ukradli 4 miliony. *Zpravy.idnes.cz.* [online]. 2016. [cit. 2017-4-8]. Dostupné z WWW: < http://zpravy.idnes.cz/falesne-e-shopy-podvod-obvineni-dvou-muzu-fgw-/krimi.aspx?c=A160619_151833_krimi_bse>.
[48]Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

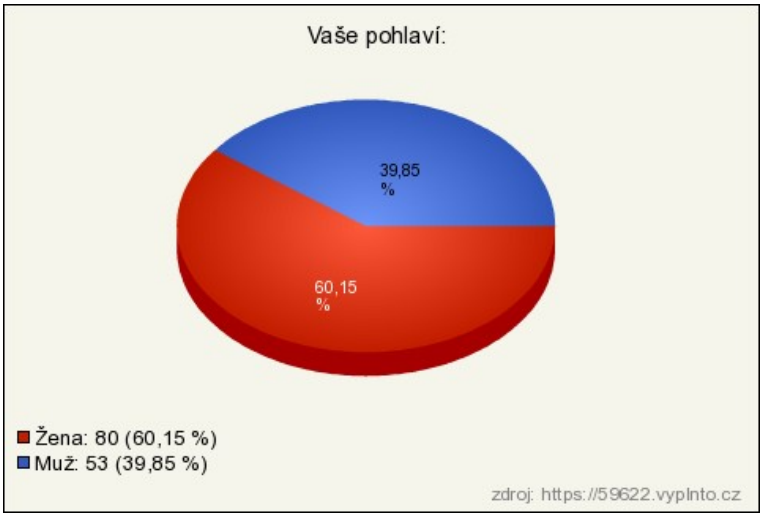
Hypotéza při sestavování otázek byla ta, že respondenti budou spíše ve věku 19-23 let, budou spíše běžní uživatelé, kteří znají většinu forem kybernetické kriminality, svůj počítač kontrolují a aktualizují alespoň 1x týdně a běžně stahují z internetu různé soubory, ať už se jedná o knihy, hry, nebo filmy.

5.1 Vyhodnocení dotazníkového šetření

Otázka č. 1: Pohlaví respondenta

Dotazníkové šetření se zúčastnilo133 respondentů a z toho bylo 60,15 % respondentů ženského pohlaví a 39,85 % mužského pohlaví.

Graf č. 1[49]:

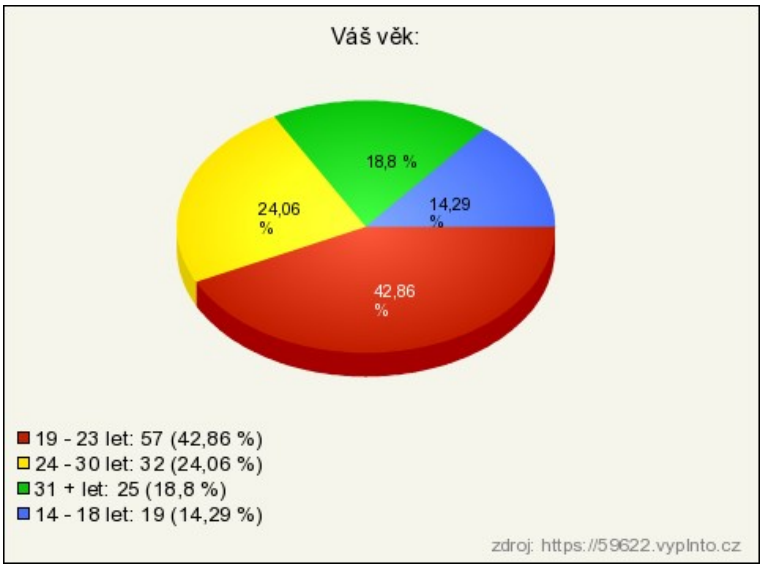


Otázka č. 2: Věk respondenta

Druhá otázka, byla zaměřena na věk respondenta. Věk byl vymezen v rozmezí 14-18 let, 19-23 let, 24-30 let a 31+. Nejvíce respondentů odpovědělo, že jim je 19-23 let což bylo 42,86 % (57) z celkového počtu respondentů (133). Dále 24,6 % (32) respondentů uvedlo, že jsou ve věku od 24 do 30 let a 18,8 % (25) respondentů uvedlo, že jsou ve věku 31 a výše. Nakonec 14,29 % (19) respondentů uvedlo, že jsou ve věku od 14 do 18 let.

[49] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Graf č. 2[50]:

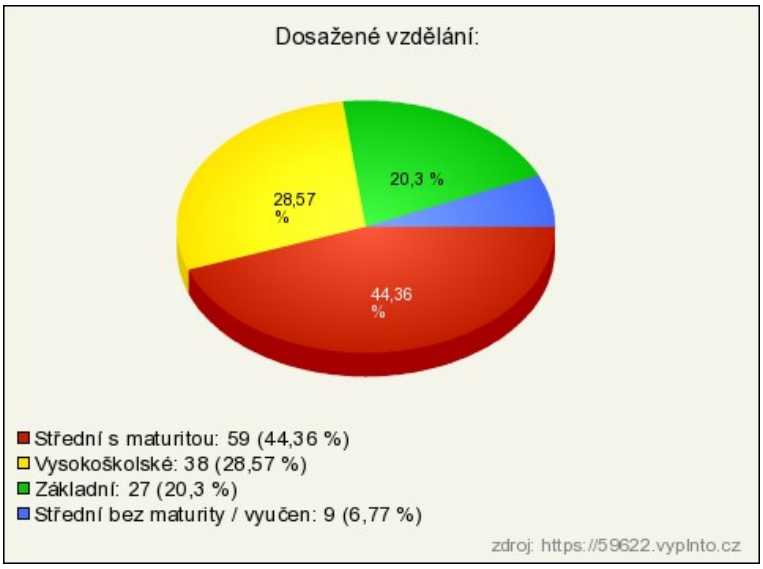


Otázka č. 3: Vzdělání respondenta

Otázka číslo 3 sloužila ke zjištění dosaženého vzdělání respondenta. Nejvíce respondentů 44,36 % (59) odpovědělo, že jejich nejvýše dosažené vzdělání je střední škola zakončená maturitou, dále 28,57 % (38) respondentů uvedlo, že jejich nejvyšší vzdělání je vysokoškolské, 20,3% (27) respondentů uvedlo, že mají základní vzdělání a nakonec 6,77% (9) respondentů uvedlo, že mají střední školu zakončenou výučním listem.

[50] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Graf č.3[51]:



Otázka č. 4: Uživatelská úroveň respondenta

Čtvrtá otázka byla zaměřena na zjištění uživatelské úrovně respondenta. Nejvíce respondentů 49,62 % (66) odpovědělo, že jsou spíše běžní uživatelé, úroveň pokročilý uživatel zaškrtlo 36,09 % (48) dotázaných respondentů, do úrovně specialista se řadí 12,03 % (16) dotázaných, a nakonec úroveň začátečník zaškrtlo pouze 2,26 % (3) respondentů.

Graf č. 4[52]:

[51] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.
[52] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Otázka č. 5: Pojem kybernetická kriminalita

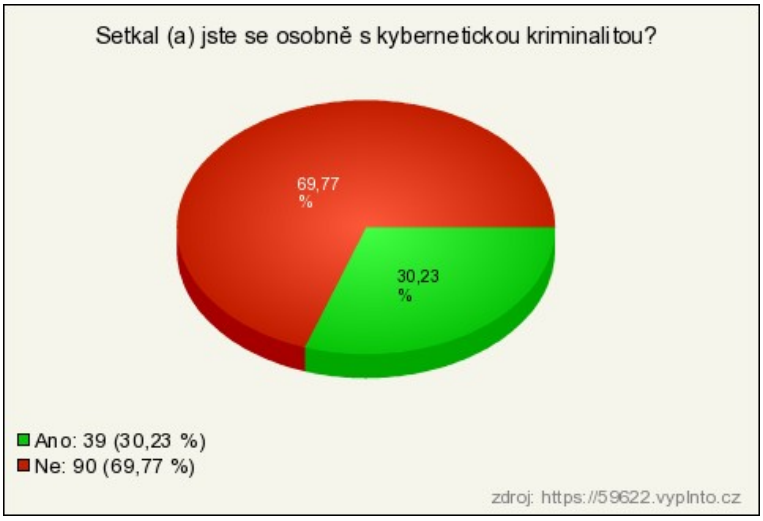
Na otázku číslo 5, která se ptá, zdali respondenti vědí, co znamená pojem kybernetická kriminalita, odpověděla většina 90,98 % (121) respondentů kladně a záporně odpovědělo 9,02 % (12) respondentů.

Graf č. 5[53]:

Otázka č. 6: Kybernetická kriminalita a respondent

Na otázku, zdali se respondent s kybernetickou kriminalitou setkal osobně, odpovědělo záporně 69,77 % (90) respondentů a kladně 30,23 % (39) respondentů.

Graf č. 6[54]:

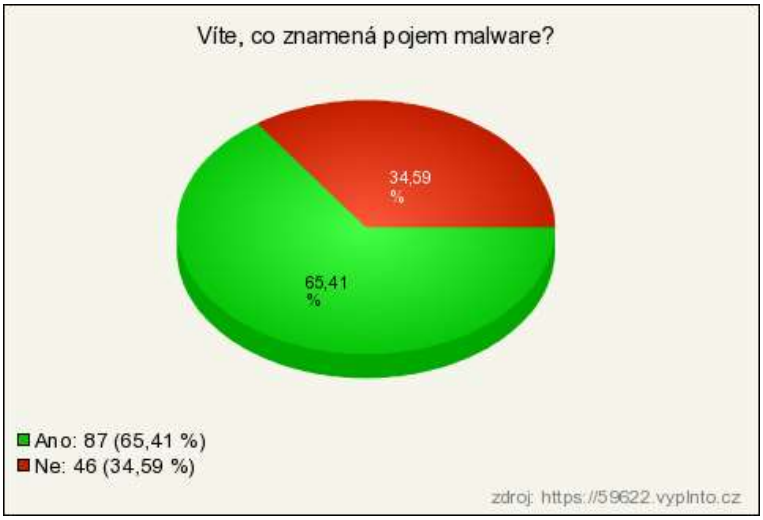


[53] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.
[54] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Otázka č. 7: Pojem malware

Na otázku č. 7 odpovědělo 65,41 % (87) respondentů kladně a záporně odpovědělo 34,59 % (4) respondentů.

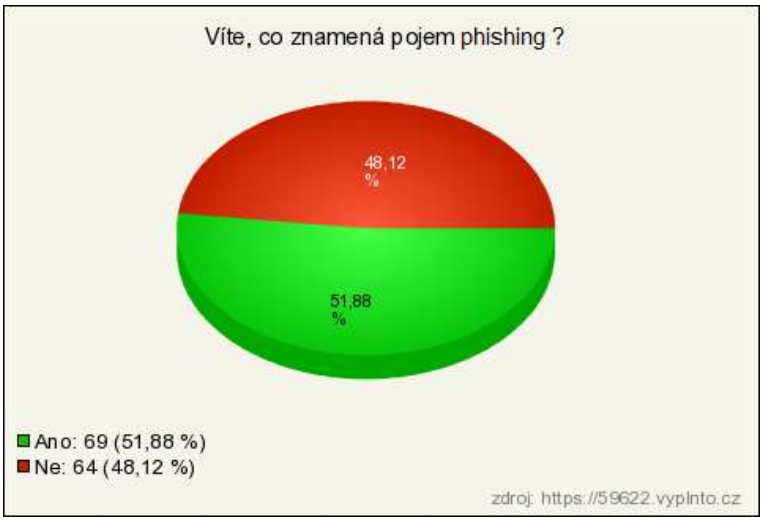
Graf č. 7[55]:



Otázka č. 8: Pojem phishing

Na otázku, zdali respondenti vědí, co znamená pojem phishing odpovědělo kladně 51,88 % (69) respondentů a záporně 48,12 % (64) respondentů.

Graf č. 8[56]:



9

[55] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.
[56] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Otázka č. 9: Pojem spam

Na otázku č. 9 zdali respondenti vědí, co znamená pojem spam, odpovědělo kladně 97,74 % (130) respondentů a záporně 2,26 % (3) respondentů.

Graf č. 9[57]:

Otázka č. 10: Pojem hoax

Na otázku, zdali respondenti vědí, co znamená pojem hoax odpovědělo kladně 66,92 % (89) respondentů a záporně odpovědělo 33,08 % (44) respondentů.

Graf č. 10[58]:

[57] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.
[58] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Otázka č. 11: Pojem trojský kůň

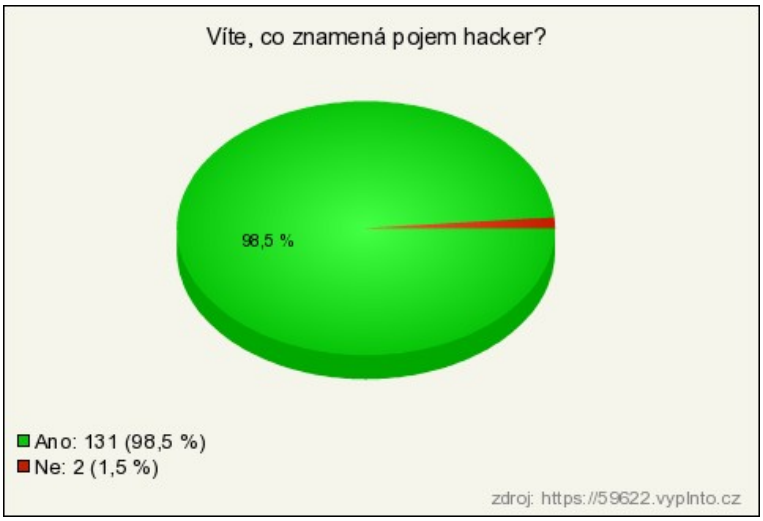
Na otázku, zdali respondenti vědí, co znamená pojem trojský kůň, odpovědělo kladně 97,74 % (130) respondentů a záporně 2,26 % (3) respondentů.

Graf č. 11[59]:

Otázka č. 12: Pojem hacker

Na otázku, zdali respondenti vědí, co znamená pojem hacker, odpovědělo kladně 98,5 % (131) respondentů a záporně odpovědělo 1,5 % (2) respondentů.

Graf č. 12[60]:



Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

[60] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Otázka č. 13: Pojem warez

Na otázku, zdali respondenti vědí, co znamená pojem warez odpovědělo záporně 62,41 % (83) respondentů a kladně odpovědělo 37,59 % (50) respondentů.

Graf č. 13[61]:

Otázka č. 14: Zavirovaný počítač

Na otázku, zdali respondenti již měli zavirovaný počítač, odpovědělo kladně 75,94 % (101) respondentů a záporně odpovědělo 24,06 % (32) respondentů.

Graf č. 14[62]:

[61] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.
[62] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Otázka č. 15: Pojem antivirový program

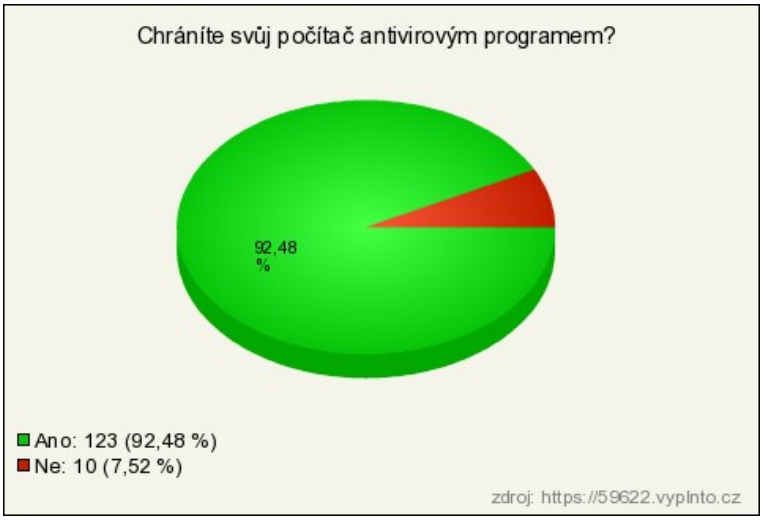
Na otázku, zdali respondenti vědí, co je to antivirový program odpovědělo kladně 98,5 % (131) respondentů a záporně odpovědělo 1,5 % (2) respondentů.

Graf č. 15[63]

Otázka č. 16: Ochrana antivirovým programem

Na otázku, zdali respondenti chrání svůj počítač antivirovým programem, odpovědělo kladně 92,48 % (123) respondentů a záporně odpovědělo 7,52 % (10) respondentů.

Graf č. 16[64]:



[63] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.
[64] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Otázka č. 17: Druh antivirového programu

V otázce č. 17 odpovědělo 70,68 % (94) respondentů, že využívají volně stažitelný antivirový program a 29,32 % (39) dotázaných odpovědělo, že využívají placený antivirový program.

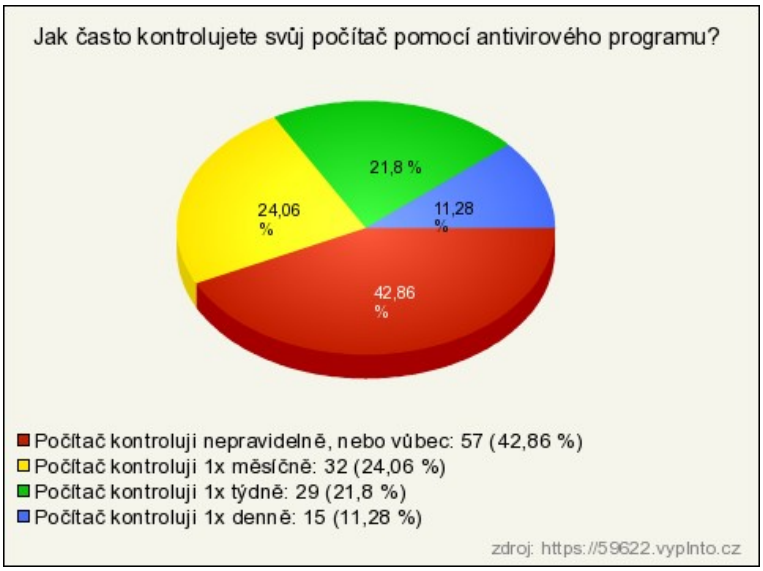
Graf č. 17[65]:

Otázka č. 18: Kontrola počítače antivirovým programem

Na otázku, jak často respondenti kontrolují svůj počítač pomocí antivirového programu, odpovědělo 42,86 % (57) respondentů, že svůj počítač kontrolují nepravidelně, nebo vůbec, 24,06 % (32) respondentů provádí kontrolu 1x měsíčně, 1x týdně provádí kontrolu 21,8 % (29) respondentů a 1x denně provádí kontrolu 11,28 % (15) dotázaných.

[65] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Graf č. 18[66]:



Otázka č. 19: Aktualizace softwaru

Na otázku, jak často respondenti aktualizují svůj software, odpovědělo 61,65 % (82) respondentů, že mají svůj počítač aktualizovaný automaticky, 19,55 % (26) respondentů odpovědělo, že svůj počítač aktualizují 1x měsíčně, 9,77 % (13) respondentů odpovědělo, že svůj počítač aktualizují 1x týdně a denně svůj počítač aktualizuje 9,02 % (12) dotázaných.

Graf č. 19[67]:

[66] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.
[67] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Otázka č. 20: Silné a bezpečné heslo

Na otázku, zdali respondenti používají silná a bezpečná hesla, odpovědělo kladně 69,92 % (93) respondentů a záporně odpovědělo 30,08 % (40) respondentů.

Graf č. 20[68]:

Otázka č. 21: Bezpečnost při komunikaci na sociálních sítích

Na otázku, zdali jsou respondenti opatrní při komunikaci na sociálních sítích, odpovědělo kladně 90,98 % (121) dotázaných a záporně odpovědělo 9,02 % (12) dotázaných.

[68] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Graf č. 21[69]:

Otázka č. 22: Bezpečnost sdílení osobních informací na sociálních sítích

Na otázku, zdali jsou respondenti opatrní při sdílení osobních informací na sociálních sítích, odpovědělo kladně 90,23 % (120) dotázaných a záporně odpovědělo 9,77 % (13) dotázaných.

Graf č. 22[70]:

[69] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.
[70] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Otázka č. 23: Bezpečnost elektronické korespondence

Na otázku, zdali si respondenti dávají pozor při otevírání elektronické korespondence, odpovědělo kladně 91,73 % (122) dotázaných a záporně odpovědělo 8,27 % (11) dotázaných.

Graf č. 23[71]:

Otázka č. 24: Pojem autorská práva

Na otázku, zdali respondenti vědí, co jsou to autorská práva, odpovědělo kladně 97,74 % (130) dotázaných, 1,5 % (2) odpovědělo nevím a záporně odpovědělo 0,75 % (1) dotázaných.

[71] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Graf č. 24[72]:

Otázka č. 25: Stahování kopie hudby z internetu

Na otázku, zdali respondenti stahují kopie hudby z internetu, odpovědělo kladně 72,8 % (96) dotázaných a záporně odpovědělo 27,82 % (37) dotázaných.

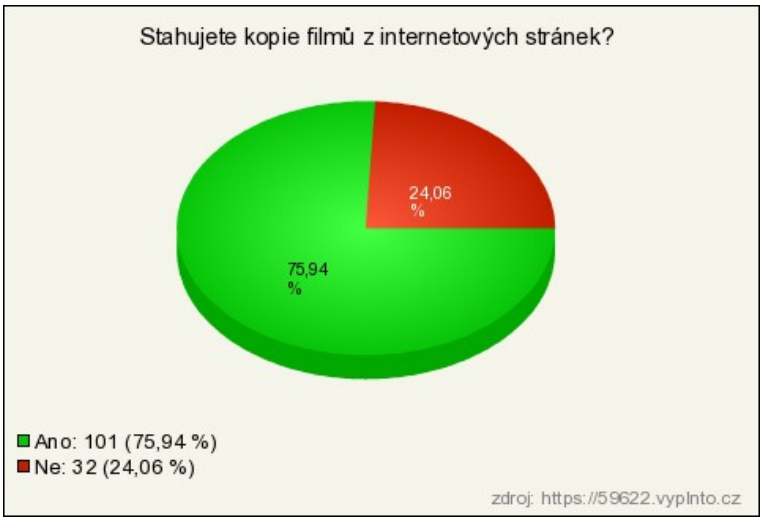
Graf č. 25[73]:

Otázka č. 26: Stahování kopie filmů z internetu

Na otázku, zdali respondenti stahují kopie filmů z internetu, odpovědělo kladně 75,94 % (101) dotazovaných a záporně odpovědělo 24,06 % (32) dotazovaných.

[72] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.
[73] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Graf č. 26[74]:



Otázka č. 27: Stahování kopie e-knih z internetu

Na otázku, zdali respondenti stahují kopie e-knih z internetu, odpovědělo záporně 69,17 % (92) dotázaných a kladně odpovědělo 30,83 % (41) dotázaných.

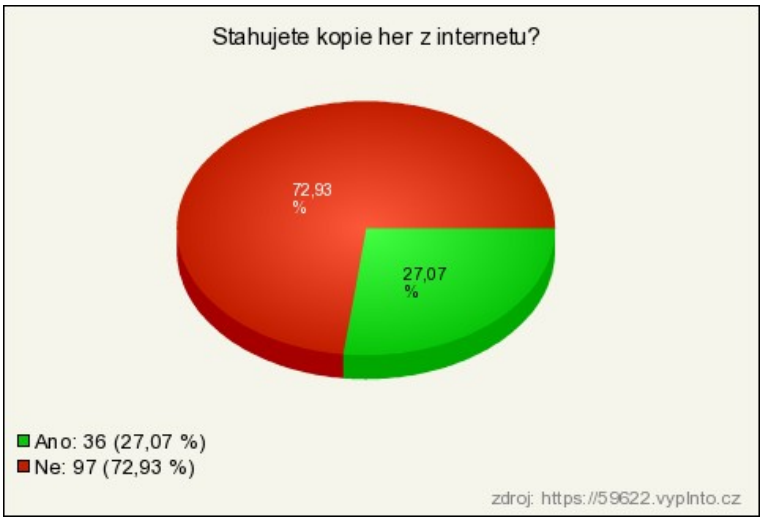
Graf č. 27[75]:

Otázka č. 28: Stahování kopií her z internetu

Na otázku, zdali respondenti stahují kopie her z internetu, odpovědělo záporně 72,93 % (97) dotázaných a kladně odpovědělo 27,07 % (36) dotázaných.

[74] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.
[75] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Graf č. 28[76]:



5.2 Shrnutí dotazníkového šetření

Cílem dotazníkového šetření bylo zjistit všeobecnou povědomost uživatelů o kybernetické kriminalitě, jejích pojmech a pojmech související s kybernetickou bezpečností.

Z dat, která byla získána pomocí tohoto dotazníkového šetření vyplynulo, že povědomost o kybernetické kriminalitě je u běžných uživatelů vysoká a téměř 70 % respondentů se s kybernetickou kriminalitou osobně nesetkali. Pozitivní zjištění je, že většina respondentů dodržuje základní bezpečnostní pravidla při sestavování hesel, svůj počítač chrání antivirovým programem. Ovšem negativní je, že více jak 75 % respondentů již mělo zavirovaný počítač. Problém může být v tom, že většina těchto respondentů využívá volně stažitelný antivirový program, který nemusí mít například aktuální virovou databázi. Nebo svůj počítač kontrolují nepravidelně a k tomu zjištění se přiznalo více jak 40 % těchto respondentů. Další pozitivní zjištění je, že více jak 60 % respondentů aktualizuje svůj počítač automaticky a tím se tak zabrání neodborným zásahům do počítačového softwaru. Velmi pozitivní zjištění potom je, že většina respondentů dodržuje základní bezpečnostní pravidla při sdílení informací na sociálních sítích a dávají si pozor na podvodné emaily.

Předběžná hypotéza byla, že respondenti budou spíše ve věku 19-23 let, budou spíše běžní uživatelé, kteří znají většinu forem kybernetické kriminality, svůj počítač

[76] Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

kontrolují a aktualizují alespoň 1x týdně a běžně stahují z internetu různé soubory, ať už se jedná o knihy, hry, nebo filmy.

Tato hypotéza se vyplnila, kromě běžného stahování z internetu, kdy respondenti odpovídali, že převážně stahují hudbu a filmy.

6 Rozhovor

Ke zjištění dalších informací o tom, na co by si uživatelé měli dát pozor a které chyby nejčastěji dělají, byl proveden položřízený rozhovor se dvěma IT pracovníky, a to s Jiřím Práškem a Ing. Rostislavem Homolkou, DiS., kteří mají zkušenosti nejen se zabezpečením a provozem firemní sítě firmy SIKO, ale také se zabezpečením firemních i soukromých počítačů a mobilů zaměstnanců této firmy.

1. **Otázka: Na co by si uživatelé měli dát především pozor?**

- *Uživatelé by si měli především sestavit dostatečně kvalitní heslo pro každou službu, které se neopakuje a nemá logickou návaznost na jiná hesla pro ostatní přístupy a uživatelské účty. Heslo by se mělo skládat z !1xY (respektive ze symbolů, čísel, malých a velkých písmen).*

- *Uživatelé by měli používat pro vytvoření hesel Password generátor a password manager.*

- *Také by neměli uživatelé klikat na neznámé odkazy, které jim přijdou na email, nebo na sociální sítě.*

- *Neotvírat neznámé přílohy u emailů neznámého původu.*

- *Mít nastavenou nejméně dvoufaktorovou autentizace např. jméno + heslo + mobilní telefon (sms, nebo aplikace).*

- *Při prohlížení internetových stránek dávat pozor na Certifikáty – v internetovém prohlížeči by měl být v url. zelený certifikát.*

- *Uživatelé by se měli také především vyvarovat procházení nezabezpečených a nebezpečných webových stránek (například při oznámení prohlížečem).*

- *Nepřipojovat se k neznámým WIFI sítím (veřejné WIFI sítě, kavárny atd.…)*

- *Nevytvářet na již ukradeném softwaru další produkci, další práci atd. - lze využít alternativ ve formě opensourcových programů.*

- *Vždy zamykat mobilní zařízení pomocí otisků prstů, číselného kódu, nebo piktogramu.*

- *Nikdy nepovolovat instalaci aplikací z neznámých zdrojů!*

2. Otázka: Jaké jsou nejčastější chyby, kterých se uživatel dopouští?

- *Uživatelé mají většinou triviální hesla.*
- *Uživatelé klikají na všechno, na co jde, aniž by u toho přemýšleli! To je nejhorší.*
- *Nečtou zprávy, které jim vyskočí na obrazovce a pak nám řeknou, že to nefunguje, ale na otázku, co jim ten konkrétní program nahlásil za chybu, už nedokážou odpovědět.*
- *Jsou náchylní na změnu grafiky čehokoli – nic pak nefunguje, nic nemůžou najít…*
- *Nezálohují si data a nic si neukládají.*
- *Připojují neznámá USB zařízení, například flash disky do počítače!*
- *U domácích wifi routerů nechávají defaultní hesla, a starý neaktualizovaný firmware.*
- *Na soukromých počítačích pracují pod účtem správce!*
- *Největším problémem jsou vždy samotní uživatelé! Zabezpečení počítače může být jakékoli, ale když uživatel něco špatně vypne, je problém.*

Z tohoto rozhovoru vyplynulo, že většině chyb, kterých se uživatelé dopouštějí, by se dalo snadno vyvarovat, kdy by pozorněji četli hlášení a doporučení, které jim počítač ohlašuje, a dbali základních bezpečnostních pravidel. Z rozhovoru také vyplynulo, že rizika, která hrozí uživatelům, jsou díky jejich nepozornosti vysoká.

7 Základní bezpečnostní pravidla[77]

Na základě informací získaných z rozhovoru s IT pracovníky, knihy Jak na Internet[78]autorka vytvořila seznam pravidel, uživatelské minimum, které by měl používat a dodržovat každý počítačový uživatel bez výjimky.

- Bezpečné heslo
- Aktualizovaný a legální Operační Systém
- Aktualizovaný antivirový program
- Aktivní firewall
- Aktualizovaný internetový prohlížeč
- Zabezpečené internetové připojení
- Záloha dat
-

1. Heslo

Heslo[79] je kód, který používají uživatelé k tomu, aby mohli vstoupit do zabezpečeného systému, nebo prostoru. Tím, že zadají správný kód, dojde k ověření jejich totožnosti. Bezpečné heslo[80] by tedy mělo obsahovat nejméně 8 znaků, které se skládají z malých a velkých písmen, čísel a symbolů. Hesla by se neměla nikdy opakovat a nejlepším řešením by bylo použití hesla s další službou, například sms zprávou nebo elektronickým klíčem.

Vhodné je, pokud se uživatel necítí na to, aby si sám vytvořil silné a bezpečné heslo, může využít například generátor náhodných hesel. Dále by nikde uživatel neměl nikdy nechávat defaultní hesla. Samozřejmostí by také mělo být to, že se uživatel nikdy o heslo s nikým nepodělí, případně ho poté ihned změní.

2. Aktualizovaný operační systém

Operační systém je základní vybavení počítače, bez kterého by počítač prostě nefungoval, a proto je důležité se o něj starat. Žádný operační systém není bezchybný, vždy se najdou chyby, které administrátoři musejí opravit. Například nekompatibilita s novým programem, nebo nějaká skulina, které si vývojáři nevšimli, a které by mohli následně využít počítačoví piráti.

---

[77] Kohout, R. *Internetem bezpečně*. Karlovy vary: AZUS Březová. 2017. s. 30-31.
[78] Vaněk, J. a kol. *Jak na internet: Na motivy stejnojmenného seriálu*. Praha: CZ.NIC s.15-42.
[79] Heslo. *It-slovnik.cz.*[online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <http://it-slovnik.cz/pojem/heslo/?utm_source=cp&utm_medium=link&utm_campaign=cp>.
[80] Kohout, R. *Internetem bezpečně*. Karlovy vary: AZUS Březová. 2017. s. 12-13.

Když takovou chybu najdou, vyjde nová aktualizace softwaru, kterou je potřeba si stáhnout a nainstalovat. Proto je doporučované, ale také nejlepší a nejjednodušší řešení, mít přednastavené automatické aktualizace systému.

3. Aktualizovaný antivirový program[81]

Samozřejmostí každého počítače je mít antivirový program. Antivirový program, slouží k vyhledávání škodlivého softwaru v počítači. Druhy antivirových programů se ve větší míře liší v tom, zda jsou placené, nebo je lze stáhnout zdarma. Poté už se liší jen ve službách, které antivirový program nabízí. Vesměs stačí ten zdarma, ale je opět nejlepší, mít přednastavené automatické aktualizace, aby s každou aktualizací a změnou virové databáze, následně proběhla i aktualizace antivirového programu i v počítači uživatele. Samozřejmě by bylo dobré si jednou začas spustit scan celého systému manuálně. Výjimkou mohou být ti uživatelé, kteří používají například operační systém Linux, nebo Mac OS.

4. Aktivní firewall[82]

Firewall je takzvaná brána, která brání neznámému a škodlivému softwaru z internetu a sítě dostat se do počítače. Ačkoli samotný aktivní firewall není stoprocentní ochrana, při správné konfiguraci se riziko napadení uživatelského počítače určitě zas o něco zmenší. Proto by mělo být základním pravidlem mít vždy bránu firewall aktivní. Jsou dva typy firewallů, a to aplikační proxy servery a paketové filtry.

Uživatel by bránu firewall neměl nikdy vypínat, naopak počítačový začátečník, by si jí neměl snažit sám nekonfigurovat a měl by to nechat na odbornějším uživateli.

5. Aktualizovaný internetový prohlížeč

Stejně jako operační systém je internetový prohlížeč stále zdokonalován, a proto je důležité ho pravidelně aktualizovat. Internetový prohlížeč se zpravidla aktualizuje sám, ačkoli je možné, že se někdy nejdříve zeptá. Dobré je mít i aktualizované doplňky v internetovém prohlížeči, ale uživatel si vždy musí nejdříve zkontrolovat důvěryhodnost doplňku, ještě předtím, než si ho stáhne a nainstaluje. Dále je důležité, aby si uživatel vždy ověřil, zda je internetová stránka, kterou navštěvuje, bezpečná.

---

[81] Doseděl, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Vydavatelství a nakladatelství Computerpress. 2004. s.16.

[82] Scambray, J, a kol. *Hecking bez tajemství*.Vyd. 2. Praha: Vydavatelství a nakladatelství Computerpress. 2002. s. 422.

6. **Zabezpečené internetové připojení**

Jak již bylo dříve řečeno, i internetové připojení je zneužitelné, a proto je důležité si ho zabezpečit silným a bezpečným heslem.

7. **Záloha dat**

Vždy se mohou stát situace, kdy se znenadání začne aktualizovat program, nebo rovnou operační systém, nehledě na to, že v něm uživatel pracuje, nebo může dojít k poškození počítače uživatelovou nešikovností, jako je například vylití pití do klávesnice notebooku. Proto je důležité si vždy práci a počítačová data zálohovat. Možností je hned několik. Záloha může být například uložená na flash disku, na externím harddisku, nebo na internetovém úložišti.

Uživatel by si měl vždy dávat pozor i při psaní například v textovém editoru, kdy je potřeba si vždy práci průběžně ukládat a při dokončení ji poté uložit například na flash disk, aby nedošlo ke ztrátě dat.

Doporučení na závěr

Jako poslední nejdůležitější doporučení je číst oznámení, které systém hlásí a nemusejí to být jen chyby, ale i jen například oznámení o zpomalení systému, nebo i o ohlášení vybité baterie. Předejde se pak většině problémů, které běžného uživatele trápí, a které si většinou způsobí sám.

Uživatel je také jenom člověk, který chybuje. Dokud budou počítače obsluhovat lidi, je vždy vysoká pravděpodobnost selhání i toho nejlepšího zabezpečujícího systému.

Závěr

Teoretická část bakalářské práce se zabývá pojmem kybernetická kriminalita, následně jsou vyjmenovány a vysvětleny druhy kybernetické kriminality a dále pak jsou vyjmenovány a vysvětleny hrozby, se kterými se tento fenomén potýká. V této části bakalářské práce jsou také vyjmenovány základní zákony, se kterými se běžný uživatel může setkat. V praktické části bakalářské práce, je provedeno dotazníkové šetření, které vede ke zjištění povědomí běžných uživatelů o kybernetické kriminalitě, jejích druzích a legislativě, která se tohoto tématu zabývá. S pomocí analýzy dat získaných od respondentů, byl splněn hlavní cíl této bakalářské práce.

Dalším cílem bylo zhodnotit rizika a navrhnout opatření. Tento cíl byl splněn s pomocí analýzy odborné literatury a polořízeného rozhovoru s IT pracovníky, které se touto problematikou zabývají. Navrhnutá opatření jsou základní pravidla, bez kterých se neobejde žádný počítačový uživatel bez ohledu na to, zda je běžný, nebo pokročilý uživatel. Díky dodržování těchto pravidel, a to zejména vytváření silných hesel a aktualizace systému, může každý uživatel minimalizovat nebezpečí, které mu v kyberprostoru hrozí.

Dále autorka této práce dospěla k názoru, že dokud budou lidé mít možnost zasahovat do bezpečnostních prvků jakékoli informační technologie, je vysoká pravděpodobnost, že může nastat chyba, která vede ke ztrátě dat a informací z jakéhokoli zařízení. Říká se, že každý bezpečnostní systém je tak silný, jako jeho nejslabší článek. V tomto případě to platí nejvíce, protože díky nepozornosti uživatele může dojít k fatální chybě.

Seznam použitých zdrojů

Literární zdroje

1. Mehan, J. E. *Cyberwar, cyberterror, cybercrime and cyberactivism*. Second Edition. United Kingdom: IT GovernancePublishing, 2014 257s. ISBN: 978-1-84928-573-5.
2. Jirovský, V. *Kybernetická kriminalita*. Vyd. 1. Praha: GradaPublishing, a.s., 2008. 288 s. ISBN: 978-80-247-1561-2.
3. Kolouch, J. *CyberCrime*. Vyd. 1. Praha: CZ.NIC, 2016. 522s. ISBN: 978-80-88168-18-8.
4. McQuade, S.C. *EncyclopediaofCyberCrime*. Firstedition. 2009. USA: GreenwoodPublishing Group, Inc. s. 210. ISBN: 978-0-313-33974-5.
5. McCarthy, L. a Weldon-Siviy, D. *Buď pánem svého prostoru. Výzkum malwaru*. Praha: CZ.NIC. 2013 s. 316. ISBN: 978-80-904248-6-9.
6. Matejka, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*.Vyd. 1. Praha: CZ.NIC. 2013, s. 128.ISBN: 978-80-904248-7-6.
7. Vaněk, J. a kol. *Jak na internet: Na motivy stejnojmenného seriálu*. Praha: CZ.NIC. s.108. ISBN: 978-80-905802-8-2.
8. Kohout, R. *Internetem bezpečně*. Karlovy vary: AZUS Březová. 2017. s. 31. ISBN: 978-80-270-1148-3.
9. Scambray, J, a kol. *Hecking bez tajemství*.Vyd. 2. Praha: Vydavatelství a nakladatelství Computerpress. 2002. s. 625. ISBN: 80-7226-644-6.
10. Kopecký, K. *KYBERGROOMING. Nebezpečí kyberprostoru.* Olomouc: NET UNIVERSITY s.r.o. 2010. s.16. ISBN: 978-80-254-7573-7.
11. Doseděl, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Vydavatelství a nakladatelství Computerpress. 2004. s.190. ISBN: 80-251-0106-1.

Elektronické zdroje

1. Kyberkriminalita. *Policie.cz*[online]. 2017 [cit. 2017-4-8]. Dostupné z WWW: <http://www.policie.cz/clanek/kyberkriminalita.aspx>.
2. Data, Informace, Znalosti. *is.bivs.cz*. [online]. 2014 [cit. 2017-8-4]. Dostupné z WWW: <https://is.bivs.cz/el/6110/zima2013/B101API/um/Data__Informace__Znalosti_v2014.pdf>.
3. Látal, I. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *scritub.com*[online]. 2017[cit. 2017-4-8]. Dostupné z WWW: <http://www.scritub.com/limba/ceha-slovaca/Potaov-informan-kriminalita-a-1513463.php>.
4. Kyberkriminalita. *Policie.cz.*[online]. 2017 [cit. 2017-4-8]. Dostupné z WWW: <http://www.policie.cz/clanek/kyberkriminalita.aspx?q=Y2hudW09Mw%3d%3d>.
5. Spam. *It-slovnik.cz*. [online]. 2017 [cit. 2017-4-8]. Dostupné z WWW: <http://it-slovnik.cz/pojem/spam>.
6. Kopecký, K. Co je hoax. *E-bezpeci.cz*. [online]. 2008 [cit. 2017-4-8]. Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25>.

7. Macháček, M. Počítačová kriminalita a bezpečnost. *Internetprosvechny.cz.*[online]. 2013. [cit. 2017-4-8]. Dostupné z WWW: <http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/>.
8. Warez. *Pocitacova-kriminalita.webnode.sk*. [online]. 2014. [cit. 2017-4-8]. Dostupné z WWW: <http://pocitacova-kriminalita.webnode.sk/nieco-k-teme/warez/>.
9. Kyberkriminalita. *Policie.cz.* [online]. 2017. [cit. 20117-4-8]. Dostupné z WWW: <http://www.policie.cz/clanek/kyberkriminalita.aspx?q=Y2hudW09NA%3d%3d>.
10. Zneužívání dětí na internetu. *Policie.cz*. [onine]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <http://www.policie.cz/clanek/zneuzivani-deti-na-internetu.aspx>.
11. Podvodné e-shopy. *Policie.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx>.
12. Kropáčová, A. CERT/SCIRT týmy a jejich role. *Root.cz*. [online]. 2013. [cit. 2017-4-8]. Dostupné z WWW:<https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/>.
13. O nás. *Csirt.cesten.cz*. [online]. 2016. [cit. 2017-4-8]. Dostupné z WWW:<https://csirt.cesnet.cz/cs/index>.
14. Jsme CSIRT-MU. *Csirt.muni.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://csirt.muni.cz/>.
15. CSIRT.CZ. *Nic.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.nic.cz/csirt/>.
16. ACTIVE24-CSIRT. *Active24.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.active24.cz/csirt/>.
17. GovCERT.CZ. *Govcert.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.govcert.cz/cs/vladni-cert/govcert-cz/>.
18. Kyberkriminalita. *Policie.cz.* [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<http://www.policie.cz/clanek/kyberkriminalita.aspx>.
19. Matzner, J. Policie dopadla dva podvodníky. Pomocí e-shopů ukradli 4 miliony. *Zpravy.idnes.cz.* [online]. 2016. [cit. 2017-4-8]. Dostupné z WWW: < http://zpravy.idnes.cz/falesne-e-shopy-podvod-obvineni-dvou-muzu-fgw-/krimi.aspx?c=A160619_151833_krimi_bse>.
20. Vrbová, D. Kybernetická kriminalita. *vyplnto.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.vyplnto.cz/realizovane-pruzkumy/59622/>.

Legislativní dokumenty

1. Zákon 101/2000 Sb., o ochraně osobních údajů. *uoou.cz*[online]. 2000 [cit-2017-4-8]. Dostupné z WWW: <https://www.uoou.cz/files/101_cz.pdf>.
2. Sbírka mezinárodních smluv č. 104/2013. Praha 2004 [cit. 2017-4-8] s. 10812 - 10824
3. Zákon o ochraně utajovaných informací. *Zakonyprolidi.cz*[online]. 2017 [cit-2017-4-8]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-412>.

4. Zákon o informačních systémech veřejné správy. *Zakonprolidi.cz.*[online]. 2017 [cit-2017-4-8]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2000-365>.
5. Moštěk, M. Úplné znění, Trestní předpisy. *trestnizakonik.cz*[online] 2017 [cit. 2017-4-8] Dostupné z WWW: <http://www.trestnizakonik.cz/>.
6. Trestní zákoník. *Zakonyprolidi.cz.*[online]. 2009. [cit. 2017-4-8]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>.
7. Listina základních práv a svobod. *Psp.cz.*[online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <http://www.psp.cz/docs/laws/listina.html>.
8. Zákon o elektronických komunikacích. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-127>.
9. Zákon o kybernetické bezpečnosti. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/2014-181>.
10. Autorský zákon. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/2000-121>.
11. Zákon o svobodném přístupu k informacím. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/1999-106>.
12. Zákon o ochraně osobních údajů a o změně některých zákonů. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/2000-101>.
13. Zákon trestní zákoník. *Zakonyprolidi.cz*. [online]. 2017. [cit. 2017-4-8]. Dostupné z WWW:<https://www.zakonyprolidi.cz/cs/2009-40>.