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

BAKALÁŘSKÁ PRÁCE

POČÍTAČOVÁ KRIMINALITA A JEJÍ PŘÍČINY

Autor práce: Kateřina Kuchařová

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2019

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce – v elektronické podobě ve veřejně přístupné části infodisku VŠERS a v tištěné podobě knihovnou VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové, za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

KUCHAŘOVÁ, K. *Počítačová kriminalita a její příčiny : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2019. 66 s. Vedoucí bakalářské práce : RNDr. Růžena Ferebauerová.

Klíčová slova: Počítačová kriminalita, kyberkriminalita, kyberprostor, bezpečnostní gramotnost

Práce pojednává o problematice počítačové kriminality a objasňuje pojmy týkající se tohoto tématu. Zabývá se některými z forem projevu počítačové kriminality a jejími pachateli. Popisuje odhalování a vyšetřování, a také některé z organizací potírajících tuto trestnou činnost. V neposlední řadě také řeší vliv lidského činitele na únik informací a dodává některá možná opatření.

V praktické části analyzuje stav bezpečnostní gramotnosti, což byl zároveň hlavní cíl práce. Pro tyto účely byl použit sběr dat formou dotazníkového šetření a stanoveny hypotézy. Vedlejším cílem bylo přiblížit danou problematiku a pojmy s ní související.

ABSTRACT

KUCHAŘOVÁ, K. *Computer Crime and Its Causes : Bachelor Thesis.* České Budějovice : The College of European and Regional Studies, 2019. 66 s. Supervisor : RNDr. Růžena Ferebauerová.

Key words: Computer Crime, Cybercrime, Cyberspace, Computer Security Literacy

This bachelor thesis deals with the issue of computer crime and clarifies the concepts related to this topic. It deals with some of the forms of computer crime and its perpetrators. It describes the detection and investigation as well as some of the organizations fighting this kind of criminal activity. Last but not least, it also deals with the influence of human factor on information leakage and provides some possible measures.

The practical part analyzes the state of computer security literacy, which was also the main goal of this thesis. For these purposes was used data collection using a questionnaire survey and hypotheses were determined. The secondary goal was to explain the issue closer and the concepts related to it.

Obsah

Úvod

Užívání počítače je pro dnešní společnost neodmyslitelnou součástí každého dne a spolu s ním jde ruku v ruce hrozba v podobě počítačové kriminality. Prostředí počítače nabízí neustále nové a sofistikovanější možnosti pro páchání tradičních i ryze počítačových trestných činů.

Počítačová kriminalita je jednou z nejrychleji rozvíjejících se forem trestné činnosti, proti které nelze zajistit stoprocentní ochranu. Škody způsobené počítačovou kriminalitou dosahují vysokých ztrát, ať už důležitých dat, tak i ztrát finančních. Z tohoto důvodu se autorka v této práci snaží zdůraznit důležitost této problematiky, neboť nejslabším článkem je právě uživatel daného systému. Díky osvětě mezi širokou veřejnost, by se tak mohl snížit počet obětí této trestné činnosti.

Téma počítačové kriminality si autorka vybrala z důvodu jeho aktuálnosti. Literatura na toto téma se vzhledem k jeho neustálému vývoji rozšiřuje, a tak autorka neměla nouzi o její dostupnost.

V práci bude v teoretické části nástíněna problematika počítačové kriminality a v praktické části provedena analýza bezpečnostní gramotnosti zkoumaného vzorku prostřednictvím dotazníkového šetření s následným vyhodnocením stanovených hypotéz. V samotném závěru práce budou shrnuty možné příčiny počítačové kriminality.

1 Cíl a metodika bakalářské práce

Cílem bakalářské práce je analyzovat stav bezpečnostní gramotnosti. Pro naplnění tohoto cíle budou stanoveny hypotézy a následně využit sběr dat prostřednictvím dotazníkového šetření.

Vedlejším cílem je pak poskytnout přehled o dané problematice a objasnění pojmů týkajících se počítačové kriminality.

Bakalářská práce bude rozdělena do teoretické a praktické části. V první části autorka zasvětí do problematiky počítačové kriminality a prostředí, v němž se tato trestná činnost odehrává - kyberprostor. V další kapitole bude popsána historie počítačové kriminality a následně charakterizovány některé z forem počítačové kriminality.

Následující kapitola se bude věnovat hrozbám a rizikům počítačové kriminality. Dále autorka bude pokračovat kapitolou, která se bude věnovat jejímu odhalování a vyšetřování.

Další kapitola se bude zabývat některými z organizací potírajících počítačovou kriminalitu. Následující kapitola se bude věnovat hlavní příčině počítačové kriminality – lidskému činiteli a doporučí některá možná opatření. Poslední kapitola bude věnována možným budoucím trendům počítačové kriminality.

Praktická část obsahuje dotazníkové šetření, pro které bylo použito čtrnáct uzavřených otázek a stanoveny tři hypotézy. Na závěr praktické části práce budou shrnuty výsledky dotazníkového šetření a vyhodnoceny stanovené hypotézy.

H1: Uživatelé provádí základní operace k ochraně svého počítače.

H2: Uživatelé, přesto, že si uvědomují hrozbu počítačové kriminality se nechovají v kyberprostoru obezřetně.

H3: Uživatelé nenakládají se svými osobními údaji bezpečně.

2 Teoretická část

2.1 Vymezení základních pojmů

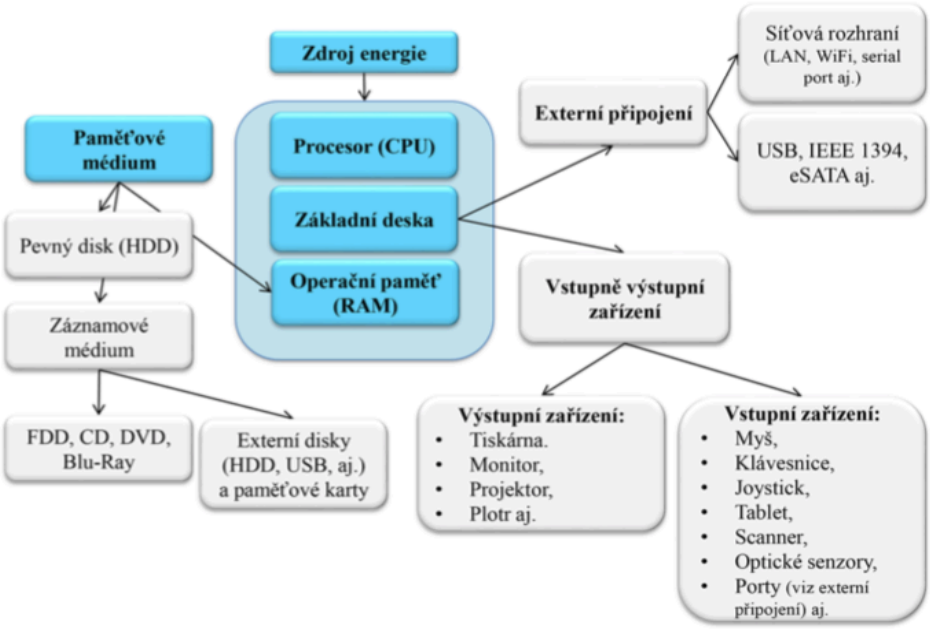
2.1.1 **Hardware**

Hardware je technickým vybavením počítače. „*...vyjadřuje souhrn hmotných technických prostředků umožňujících nebo rozšiřujících provozování počítačového systému.*“ Zahrnuje veškerá hmotná vybavení, která jsou potřeba k zpracování dat systémem. „*Je to v podstatě počítač sám.*“

Dále Kolouch hardware člení na:

- *Vnitřní vybavení počítače* – komponenty, které zařizují chod počítače (základní deska, procesor atd.)
- *Periferie* – doplňující vybavení počítače, které k samotnému fungování počítače není potřebné, ale může sloužit k jeho ovládání (klávesnice, externí pevný disk atd.)[1]

Obrázek č. 1: Hardware a jeho součásti[2]



[1] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 59.
[2] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 62.

2.1.2 **Software**

Software bývá označován jako programové vybavení počítače. To ale Kolouch vyvrací a uvádí, že pojmy programové vybavení, počítačový program a software jsou odlišné a dále je charakterizuje:

- *Programové vybavení* – programy, o které je doplněn hardware, aby uživatel mohl počítač vůbec používat; „*...zahrnuje programy počítačů, počítačové programy včetně software. Jedná se o programy, procedury, pravidla a příslušnou dokumentaci systému zpracování informací nebo jejich část*“.

- *Počítačový program* – je chráněn autorským zákonem a je definován jako: „*...zápis algoritmu v takovém tvaru, ve kterém jej systém na zpracování údajů dokáže zpracovat. Lze jej charakterizovat jako ucelený souhrn instrukcí (příkazů), pomocí nichž provádí počítač určitou činnost.*“

- *Software* – vyjadřuje programové vybavení všeho druhu, které je třeba k chodu počítače, od základních programů, operačních systémů až po všechny aplikace; „*V širším slova smyslu to jsou veškeré informace, které jsou v počítači nějakým způsobem uloženy a dále se dělí podle způsobu použití do dvou základních skupin. Jsou to PROGRAMY a DATA.”*[3]

2.1.3 **Internet**

Historie Internetu sahá až do šedesátých let, kdy se Spojené státy americké rozhodli, že chtějí mít novou sdělovací síť, která by v kterékoliv možné komplikaci zprostředkovala pohotovou výměnu dat. Touto komplikací byla zejména myšlena nukleární válka. Tato sdělovací síť měla poslání propojit země, města či velitelská místa k bezproblémové výměně taktických informací.[4]

„*Je to síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních a vládních sítí, s místním až globálním rozsahem, které jsou propojeny širokou škálou elektronických, bezdrátových a optických síťových technologií.*“[5]

[3] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 62 – 63.
[4] KRČMÁŘ, P. *Linux: postavte si počítačovou síť*. Praha, 2008, s. 20.
[5] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.*Praha, 2015, s. 49.

Dále je Internet třeba brát, mimo jiné, jako publikačního zprostředkovatele, kde může uveřejňovat kdokoli cokoliv. Internet není vázán žádným síťovým centrem, jeho uživatel si může vybrat od poskytovatele až po volbu obsahu na jeho obrazovce. Může plnit informační, komunikační či komerciální úlohu aj. Internet může být pramenem informací k výzkumu, stejně tak jako může tvořit prostor pro hraní her.[6]

V dnešní době Internet nikdo nevlastní, nikdo nad ním nemá moc, ani ho nikdo neřídí. V neposlední řadě je Internet nepostradatelnou a věcnou bází kyberprostoru.[7]

2.1.4 **Kyberprostor**

Kyberprostorem se rozumí: „*Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*“[8] Kyberprostor funguje svobodně a nepřetržitě a data v něm obsažená se neustále přetvářejí. Ze stránky časoprostoru při útoku pozbývá smyslu vzdálenost. Je obvykle podružné, jestli je útočník nablízku či na druhé straně světa.[9] Kyberprostor je brán jako určitá oblast, která je ukotvena ve skutečném světě, obsahuje racionální úroveň a pojímá interakci mezi lidskou percepcí, poznávacími způsobilostmi a činnostmi, totožně jako u jiných sfér.[10] Smejkal[11] mezi hlavní znaky kyberprostoru řadí vzájemné působení, globálnost, šíření údajů a informací, ale také možná nebezpečí v podobě napadení od anonymních, kybernetických útočníků.

Kolouch[12] považuje kyberprostor za nejefektivnější a nejvíce nebezpečnou zbraň útočníků počítačových trestných činů. Dále uvádí, že systém je tak odolný, jak je odolný jeho nejméně silný díl, tím je v tomto případě nejčastěji uživatel daného systému. Ten díky svým nedostačujícím vědomostem a informacím představuje jak pro sebe, tak pro své okolí značnou hrozbu. Aktivity v kyberprostoru mohou mít dopad například v podobě peněžních škod, nabourání se do soukromí, znehodnocení či ztrátu soukromých dat, domlouvání se organizovaných zločineckých skupin na trestné činnosti bez eventuality odposlouchávání třetí strany, odvrácení komerciálních objednávek, vyloupení

[6] SKLENÁK, V. *Data, informace, znalosti a Internet.* Praha, 2001, s. 10.
[7] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 42.
[8] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.*Praha, 2015, s. 70.
[9] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach.* Bratislava, 2016, s. 19.
[10] BASTL, M., GRUBEROVÁ, Z. *Kyberprostor jako „pátá doména”?* [online]. 2013 [cit. 2019-03-20]. Dostupné z WWW: <http://vojenskerozhledy.cz/kategorie/kyberprostor-jako-pata-domena>.
[11] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň, 2015, s. 15.
[12] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 13 - 15.

bankovních účtů, dále umožňuje osobám s duševními poruchami komunikovat prostřednictvím Internetu aj. Upozorňuje také na to, že typickou obětí počítačové kriminality jsou právě koncoví uživatelé kyberprostoru a vyzdvihuje důležitost prevence ve formě vzdělávání se a dostávání se do povědomí o možných hrozbách mezi uživatele informačních technologií.

2.1.5 **Počítačová kriminalita**

Počítačová kriminalita je významným jevem současné doby. Rozumí se jí takové trestné činy, které jsou páchány buď proti počítači či za jeho pomoci. Jsou to trestné činy namířené proti celistvosti, přístupnosti, ukrytí počítačových systémů nebo trestné činy, při nichž je užito oborů sdělovacích a informačních technik. Počítače nevytvářejí nové trestné činy, představují pouze nové postupy a prostředky k dopouštění se trestné činnosti k již známým trestným činům „*...jako sabotáž, krádež, neoprávněné užívání cizí věci, vydírání anebo špionáž.*"[13]

Klimek, Záhora a Holcr[14] vyzdvihují obtížnost definice tohoto pojmu. Počítačovou kriminalitu popisují jako „*konanie pachatel'a za použitia informačnej techniky, ktorým sú naplnené znaky skutkovej podstaty počítačového trestného činu*", načež tyto trestné činy rozdělují na tři kategorie: trestné činy s cílem útoku napadení počítače, trestné činy, kdy počítač je pouhým prostředkem k jejich realizaci a trestné činy, při jejichž konání má počítač pouze postranní funkci. Dále také zmiňují Internet, díky němuž dostává počítačová kriminalita nový formát v podobě bezmeznosti.

Smejkal[15] počítačovou kriminalitu popisuje podrobněji. Uvádí, že je stará stejně jako počítače a také, že se může jednat o rozmanité smíšení trestných činů, propojených kolektivním činitelem, kterým je počítač, program či data. Ty se mohou vzájemně prolínat, například ekonomická kriminalita může být realizována za pomocí počítače. Napadení nemusí mířit pouze proti počítači, cílem útoku může být jakákoli jeho součást, tedy hardware, software či data v něm uložená anebo jím zpracovaná.

Útok proti datům může být uskutečněn nejen na data v počítači, ale i na data, která jsou uložena na nosiči dat, např. USB disk, CD, apod. Takový nosič dat je aplikovatelný s použitím počítače, avšak v průběhu útoku se může vyskytovat kdekoliv. Útok také může

[13] POŽÁR, J. *Informační bezpečnost.* Plzeň, 2005, s. 249
[14] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach.* Bratislava, 2016, s. 19 - 26.
[15] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň, 2015, s. 19

být veden proti datům v průběhu jejich transferu, „*…například v době jejich přenosu prostřednictvím sítě elektronických komunikací, a to jak pomocí hmotného média (kabelu), tak bezdrátovým přenosem (radiovými vlnami).*" Útoky jsou z převážné části cíleny na data, která jsou součástí počítačů či jiných záznamových médií. Útoky jsou vedeny ale také proti počítači jako technickému vybavení, vniknutím do jeho softwaru, např. aktivováním ničivého softwaru v podobě viru, modifikací určitého programu či napadením počítače se záměrem jeho přetížení (DDoS útok)[16].

Bímová[17] počítačovou kriminalitu popisuje jako vážnou a nebezpečnou trestnou činnost, která se musí brát v úvahu ve všech rozvinutých zemích na světě. Má mnoho podstatných rysů, čímž se diferencuje od běžné kriminality. Zejména fakt, že trestný čin může být realizován v mnoha momentech bez přítomnosti útočníka na místě činu. Počítačová kriminalita se dále vyznačuje velkými škodami, jak peněžními, tak ztrátami obtížně získatelných dat z obsáhlých databank. Dalším znakem této trestné činnosti je její vybranost a nenápadnost. Pachateli bývají mnohdy osoby s vysokou inteligencí a vzděláním, které by se jinak klasických trestných činů nedopustily. Dále počítačová kriminalita postrádá dostatek obvyklého důkazního materiálu, především v listinné formě a namísto toho vyšetřovatelé pracují s digitálními důkazy.

Každý autor popisuje počítačovou kriminalitu jako obtížně vysvětlitelný pojem, dále jako nebezpečnou trestnou činnost, kterou převážně páchají lidé s vyšší inteligencí. Shodnou se také na vysoké míře latence a obtížnosti zajištění důkazního materiálu při odhalování a vyšetřování.

3 Historie počítačové kriminality

Počítačová kriminalita vznikla v období 60. a 70. let 20. století. Nepochybně v té době byla od té dnešní rozdílná. Dřívější počítače byly odlišné od dnešních, měly hodnotu v milionech amerických dolarů, prostorově obsáhly celou místnost, potřebovaly klimatizaci a také odborníky, kteří zajišťovali jejich funkčnost. Majitelem počítačů byly obvykle pouze velké instituce, například bankovní. K tomu všemu nebyly zapojené do sítí ani na Internet, jako je tomu dnes.[18]

[16] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň, 2015, s. 19 - 20.
[17] BÍMOVÁ, A. *Počítačová kriminalita a naše doba.* Praha, 1990, s. 5.
[18] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava, 2016, s. 17.

Počítačová kriminalita se zrodila ve chvíli, kdy se počítače začaly transformovat z matematických přístrojů na víceúčelové přístroje, které byly způsobilé ujmout se administrativních prací. V momentě, kdy někoho napadlo, že úpravou programů či dat zformovaných počítačem může někomu přivodit ztrátu či užitek. Počítač se současně ukázal jako prostředek k páchání zločinu. Trestné činy za pomoci počítače mohl spáchat pouze omezený počet jedinců, kteří k počítači měli přístup.[19]

V tomto období v Československu se počítačová kriminalita nevyskytovala, z důvodu opožďování ve vývoji a užívání informačních technologií. „*Kriminalita kopírovala technické a uživatel'ské možnosti počítačov. Prvými trestnými činmi boli sabotáže, ktoré boli motivované rôzne – politicky, ako aj pomstou zamestnávatel'ovi.*" Patrně prvním počítačovým trestným činem byl v 80. letech 20. století nevyrovnaný zaměstnanec Úřadu důchodového zabezpečení, který prostřednictvím magnetu porušoval zápisy na magnetických páskách. Podle někdejšího zákona byl potrestán za trestný čin sabotáže.[20]

Zanedlouho se vyskytly „*tzv. dokladové delikty*", kdy pachatelé přišli na to, že stejně jako pozměňovali informace na listinných dokumentech, tak mohou takto pozměňovat materiály nachystané ke zpracování do počítače. Obvykle šlo o takové trestné činy, které byly založeny na machinacích v mzdových kancelářích a jiných pracovištích, kde měl zaměstnanec eventualitu nakládat s financemi či artikly. V té době, před rokem 1989 se právní posouzení skláněla k někdejšímu TZ §132 – „*Rozkrádání majetku v socialistickém vlastnictví*". Dnes jsou tyto činy posuzovány jako podvod dle §209 TZ „*...v souběhu s trestným činem podle §230 Neoprávněný přístup k počítačovému systému a nosiči informací*." Až poté pachatelé pochopili, že je mnohem snadnější modifikovat data bezprostředně v počítači, avšak museli získat přístup k počítači, a to nebylo snadné.[21]

Nadcházející forma dopouštění se počítačové trestné činnosti byla taktéž svázána s tehdejší nedosažitelností počítačů. Tato forma tkvěla ve vykonávání propočtů na počítači zaměstnavatele. Míra nezákonného používání cizí věci byla různorodá: „*...od tisku populárních obrázků na řádkové tiskárně, přes kondiciogramy a výpočty*

[19] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava, 2016, s. 17 - 18.
[20] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava, 2016, s. 18.
[21] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň, 2015, s. 73.

diplomových prací až po skutečné nelegální podnikání za účelem vlastního obohacování.“[22]

Už v té době se vyskytovala značná výše latence počítačových trestných činů určená poměrem občanů k „*tzv. společnému socialistickému vlastnictví*“, zintenzivněná nemateriálním profilem počítačového času, kdy reálně nic fyzického zcizeno nebylo. „*Zvláštní charakter strojového času vedl v počítačích boje proti počítačové kriminalitě k nutnosti aplikovat na skutkové podstaty ustanovení trestního zákona, která vůbec se skutečným činem na první pohled nesouvisela: klasickým zahraničním případem je odsouzení hackera (průnikáře) za krádež elektrické energie, kterou spotřeboval neoprávněným užíváním počítače.*“[23]

Novou éru počítačové kriminality určuje Smejkal těmito třemi okamžiky:

- nastoupením privátních počítačů
- zrodem počítačových sítí a dálkovým přístupem k počítači
- vzrůstem možností mobilních telefonii a tomu korespondující výbava lidí, počítaje v to „…*využívání anonymních, tzv. předplacených karet*“

Pokrokové technologie vybudovaly „zlatý důl“ pro pachatele, kteří se na počítačích začali přiživovat obvyklou trestnou činností, nyní ale snáze realizovatelnou. Podstatnou sféru tvořily podvody, které buď byly prostřednictvím počítače vylepšeny, eventuálně se vyskytly kompletně nové formy podvodů (např. phishing). Taktéž výraznou skupinu počítačových trestných činů tvoří porušování autorských práv, z kterého se stalo téměř souznačné slovo pro používání počítače a Internetu.[24]

4 Vybrané druhy trestné činnosti páchané v kyberprostoru

Počítačová kriminalita pojímá značné spektrum trestných činů páchaných pomocí informační a komunikační technologie. Počáteční podoba počítačové kriminality byla spjata především s krádeží hmotných komponentů počítače, včetně jejich softwaru. Spolu s rozvojem a zkvalitňováním informačních a komunikačních technologií se vyvíjely i další projevy počítačové kriminality. Od fyzického odcizování začala počítačová

[22] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň, 2015, s. 73.
[23] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň, 2015, s. 74.
[24]SMEJKAL, V. *Kybernetická kriminalita.* Plzeň, 2015, s. 74.

kriminalita přestupovat k propracovanějším trestným činům, kterých se začali dopouštět lidé s vyšším inteligenčním kvocientem. Spolu s vývojem trestných činů se změnily i cíle pachatelů, dříve to bylo prokázání svých dovedností a způsobilostí, peněžní motivace přišla až později. V dnešní době existuje mnoho druhů počítačové kriminality, některé vznikají spojením různých druhů, jiné se rozvíjejí doplněním jednotlivých postupů už vzniklých druhů anebo vznikají další, dosud neznámé druhy.[25]

Mezi hlavní projevy počítačové kriminality, které budou níže popsány, řadí většina autorů následující:

- hacking
- cracking
- malware
- scam.

4.1 Hacking

Hackingem se rozumí vniknutí do počítačového systému cizím osobám, bez oprávnění a nestandardním způsobem - průnikem počítačového systému.[26]

Hacker je osoba, která bez oprávnění vniká do systému počítače či soukromých dat jinému člověku. Dříve hackeři vycházeli ze společenství počítačových fanoušků, zejména osob studujících informační technologii, kteří korespondovali se vzorem zvláště inteligentních introvertů prahnoucích po popularitě. Někteří hackeři i nyní studují informační technologii, jiní mají touhu pomstít se svému bývalému zaměstnavateli anebo jsou členem organizované zločinecké skupiny.[27]

Z hlediska bezpečnosti se hackeři rozdělují na černé klobouky (black hats), bílé klobouky (white hats) a šedé klobouky (gray hats). Mezi černé klobouky se řadí osoby, které produkují a šíří viry či červy, vnikají do systémů počítačů, vyčleňují je z chodu, odcizují data apod. Bílé klobouky jsou zaměstnávány jako osoby, které se specializují na bezpečnost. Užívají shodné prostředky a postupy jako černé klobouky, pouze s opačným

[25] KOSTRECOVÁ, E., JÓKAY, M., KOSTREC, M. *Počítaová kriminalita*. Bratislava, 2010, s. 2 - 3.
[26] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava, 2016, s. 29.
[27] MCCARTHY, L., WELDON-SIVIY, D., ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha, 2013, s. 82 - 83.

úmyslem - vypátrat je. Činnost bílých klobouků je tedy tzv. etické hackování. „*Etické hackování je proces, kdy se bezpečnostní nástroje používají k testování a vylepšování bezpečnosti, nikoli k jejímu narušování*." Šedé klobouky se nacházejí na pomezí černých a bílých klobouků, jelikož morální mez leckdy přesáhnou. Kupříkladu vniknou do systému počítače pouze z důvodu, aby se v něm porozhlédly, a věří, že když v něm nezpůsobí žádné škody, tak se nedopouštějí trestné činnosti.[28]

4.2 Cracking

Cracking, činnost, díky které lze prolomit či se vyhnout bezpečnostním prvkům a užívat tak určitý počítačový program bez oprávnění. Cracking je tak přizpůsobení si počítačových programů se záměrem vyhnutí se či zbavení se ochranných prvků, které programy chrání před ilegálním užíváním. Většina počítačových programů má svou validní licenci, kterou je třeba k jejich užívání opatřit. Hlavním důvodem crackingu je vyšší cena programů, kterou musí potenciální uživatel zaplatit. Mezi tyto programy patří např. kancelářský balíček programů Microsoft Office či program na úpravu PDF souborů Adobe Acrobat atd.[29]

Tvůrci a vývojáři programového vybavení využívají bezpečnostní prvky jako například: „*... sériové čislo, autentifikaciu na servroch výrobcu pri spustení programu po jeho inštalacii, aktivaciu programu telefónom, nutnosť mať pri prvom spustení programu originálne inštalačné médium v CD/DVD mechanike*". Mnohdy tyto prvky mezi sebou kombinují. Takzvané „cracky" jsou dostupné na Internetu, nebo si je lidé mezi sebou sdílí.[30]

4.3 Malware

Malware je pojmenování pro kterýkoli software, který je použit k porušení běžného chodu systému počítače, k vytěžení dat anebo přístupu do systému počítače. Malware pojímá mnoho forem projevu, které jsou různě pojmenované, dle toho, jakou konají aktivitu. Pro malware je také charakteristické, že zvládá vykonávat více úloh najednou, kupříkladu je schopen při vniknutí do počítačového systému se sám rozšiřovat pomocí elektronické pošty a současně těžit informace či data z poštovní schránky. Dříve,

[28] MCCARTHY, L., WELDON-SIVIY, D., ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha, 2013, s. 84 - 85.
[29] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava, 2016, s. 31 - 32.
[30] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava, 2016, s. 32.

pro dnes jednotný název malware existovalo mnoho označení, která byla odvozena od aktivity, kterou určitý program prováděl a patří mezi ně:

1) Spyware
2) Adware
3) Viry
4) Červi
5) Trojské koně
6) Rootkity
7) Keylogger
8) Ransomware
9) Phishing
10) Pharming
11) Spamming
12) Warez
13) Spoofing
14) Sociální inženýrství aj.[31]

4.3.1 **Spyware**

Spyware je škodlivá šifra, která soustřeďuje a posílá data v počítačovém systému, v kterém je instalována bez toho, aniž by o tom uživatel daného systému věděl. Může soustřeďovat data o historii navštívených stránek na Internetu se záměrem zvýšení dosahu reklamy jejím přímějším cílením anebo může soustřeďovat data za účelem posílání soukromých dat uživatele. Spyware uložená data neničí, nepřemisťuje a sám sebe dál nešíří.[32]

4.3.2 **Adware**

Adware je dalším druhem škodlivé šifry, jejíž úlohou je propagovat reklamní sdělení v kterékoli podobě, např. vyskakovací okna ve webovém prohlížeči, samovolné změnění titulní stránky prohlížeče apod. Jde spíše o rušící element, který nebývá nijak nebezpečný a mnohdy je šířen spolu s bezplatnými programy. Adware na rozdíl od

[31] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 204 - 205.
[32] KOHOUT, R., KARCHŇÁK, R., *Bezpečnost v online prostředí*. Karlovy Vary, 2016, s. 32

spywaru nesoustřeďuje data a ani je nikam neposílá, ale může směřovat reklamní sdělení podle dat jím získaných.[33]

4.3.3 **Viry**

Počítačový vir je program či část počítačového programu, která funguje na základě připojení se k programu nebo souboru a rozmáhá se, aniž by o tom uživatel věděl. Účelem počítačového viru je šíření sebe samého z jednoho počítače na další. Vir se spustí spolu s otevřením souboru či programu, v kterém je uložený. „*Napríklad kliknutím na súbor, ktorý je pripojený k elektronickej pošte alebo kliknutím na odkaz webovskej stránky, ktorý sa nachádza na inej webovskej stránke*." Počítačový vir může zasáhnout kohokoli v průběhu výměny dat pomocí „*...elektronickej pošty, prostredníctvom prenosu médií, sťahovánim programov, súborov, dokumentov alebo iného typu a formátu autorských diel z Internetu*".[34]

Viry s sebou můžou přinášet i tzv. payload = náklad, který jim sděluje, že mají zapříčinit poškození, například smazání informací či zaútočit na další systém. I bez payloadu může ale vir zapříčinit problémy. Už jen tím, že se vir kopíruje, může zaplnit veškerou volnou paměť v počítači. Počítačový vir lze připodobnit k biologickému viru. Například chřipka se může přenášet z jedné osoby na druhou a to, do jakého rozsahu člověk onemocní, určí druh chřipky anebo to, zda je člověk očkován. Pokud se člověk chřipkou nakazí, může vir přenášet na všechny osoby se kterými se dá do kontaktu. Na stejném principu funguje i počítačový vir. Pokud se počítač „nakazí" virem, tak výši škody určí to, zda má v sobě počítač nainstalovaný antivirový program s poslední aktualizací a také to, zda virus v sobě zahrnuje payload. Pokud v sobě payload zahrnuje, může smazat veškerá data počítače. Pokud tak učiní, nemůže se ale šířit dále, protože v počítači už nejsou žádné programy, které by nakazil. Obvykle viry payload neobsahují, jen se kopírují a tím šíří dále.[35]

4.3.4 **Červi**

Počítačoví červi k průniku do počítačového systému využívají jeho slabých míst, díky kterým počítač infikují a také spojení s jinými počítači přes Internet, díky němuž se rozšiřuje do dalších počítačů. Jsou si blízcí s počítačovými viry, ale s tím rozdílem, že

[33] KOHOUT, R., KARCHŇÁK, R., *Bezpečnost v online prostředí*. Karlovy Vary, 2016, s. 33.
[34] KOSTRECOVÁ, E., JÓKAY, M., KOSTREC, M. *Počítačová kriminalita.* Bratislava, 2010, s. 8.
[35] MCCARTHY, L., WELDON-SIVIY, D., ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha, 2013, s. 41 - 42.

počítačoví červi nevyžadují ke svému šíření a aktivaci „pomoc" lidského činitele. Mají totiž svou mechaniku, díky které se mohou samovolně rozšiřovat v objemném množství, produkovat své kopie a vyhledávat další, ještě nenapadené počítače.[36]

Červ je obyčejně nezávislým programem, přemisťuje sám sebe mezi počítači, na rozdíl od toho vir se přidružuje k souborům. Červi mnohdy útočí proti určitým webovým stránkám. Například posílají takový objem bezvýznamných dat, že stránky přestanou reagovat. Nebo také může vniknout do systému počítače bez vědomí uživatele např. skrze hru na Internetu.[37]

4.3.5 **Trojské koně**

Trojský kůň se skrývá v počítačovém programu jako ničivá šifra. Zprvu se takový program může zdát jako přínosný, může se jednat například i o bezplatné programy k „očistě" počítače od malwaru. Odtud také název Trojský kůň, jako v řeckém bájesloví, kde naplňoval podobný význam. Mnohdy zneužívá bezpečného pramene ve svůj prospěch, například pomocí přílohy elektronické pošty, kde se na první pohled může zdát, že odesílatelem dané zprávy je antivirová společnost. Cílem Trojského koně je ovládnout počítačový systém, do kterého proniknul a vytěžit z něj hesla, ovládat soubory v něm uložené atd.[38]

Trojského koně si uživatel nemusí všimnout, ten tak čeká a může se spojit s tzv. „*útoky nultého dne*". Když se spojí, mají schopnost zapříčinit hromadné ztráty. Útok nultého dne je vybudovaný na bezpečnostní „skulině", které si vývojáři nevšimli anebo na ní nestihli vyvinout ochranu. Spuštění trojského koně může zároveň spustit počítačový vir či červa.[39]

4.3.6 **Rootkity**

Rootkit je komplex prostředků, které zastírají aktivitu škodlivých šifer v počítačovém systému tak, že je obvyklý antivirový program nedokáže nalézt. Zastírání aktivit se může uskutečňovat: „*...skrýváním adresářů s malwarem, skrýváním klíčů*

[36] KOSTRECOVÁ, E., JÓKAY, M., KOSTREC, M. *Počítačová kriminalita.* Bratislava, 2010, s. 8.
[37] MCCARTHY, L., WELDON-SIVIY, D., ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha, 2013, s. 47 – 48.
[38] KOHOUT, R., KARCHŇÁK, R., *Bezpečnost v online prostředí*. Karlovy Vary, 2016, s. 34.
[39] MCCARTHY, L., WELDON-SIVIY, D., ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha, 2013, s. 52 - 53.

v registrech, skrýváním běžících procesů, síťových spojení a dalších systémových služeb".[40]

4.3.7 **Keylogger**

Keylogger je ilgeální prostředek, pomocí kterého se zcizují přihlašovací údaje uživatele. Keylogger zapisuje stisknuté znaky na klávesnici a zaznamenává je v jeden soubor, který pak posílá útočníkovi. Novější druhy keyloggeru dokáží zaznamenat i snímek obrazovky počítače, který útočníkovi usnadňuje určit, k jaké aplikaci získané přihlašovací údaje patří. Tímto způsobem opatřené údaje jsou dále využívány k další počítačové trestné činnosti, kupříkladu phishingu.[41]

4.3.8 **Ransomware**

Ransomware je program, pomocí něhož jsou zakódovány soubory v počítači či je počítačový systém vyčleněn z chodu anebo vyčleněním z chodu útočník vyhrožuje do doby, než uživatel uhradí výkupné = ransom. Výkupné obvykle probíhá formou zpoplatněné SMS zprávy. Tradiční způsob provedení ransomwaru je v podobě nastrojení klamného antivirového systému.[42]

4.3.9 **Phishing**

Phishing díky klamavému způsobu jednání využívá informační a komunikační technologii k přístupu k osobním informacím a datům jako jsou hesla, údaje na platebních kartách apod. Phishing probíhá tím způsobem, že útočník zfalšuje požadavek, nejčastěji bankovní instituce, který je zformován takovým způsobem, aby byl uživatel „povinen" vyplnit údaje ke svému účtu. Tyto požadavky jsou obvykle rozesílány formou elektronické pošty. Ke zprávě s požadavkem je připojen odkaz, který po rozkliknutí uživatele přesměruje na důvěryhodnou kopii webové stránky, kupříkladu právě webové stránky bankovní instituce. Vyplněním přihlašovacích údajů je uživatel svěřuje do rukou útočníka, který s nimi dále nakládá ve svůj prospěch.[43] Phishing probíhá i pomocí mobilního telefonu, nicméně díky počítači se útočník může mnohem důkladněji ukrývat,

[40] KOHOUT, R., KARCHŇÁK, R., *Bezpečnost v online prostředí*. Karlovy Vary, 2016, s. 33.
[41] KOSTRECOVÁ, E., JÓKAY, M., KOSTREC, M. *Počítačová kriminalita.* Bratislava, 2010, s. 10.
[42] MCCARTHY, L., WELDON-SIVIY, D., ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha, 2013, s. 74.
[43] KOHOUT, R., KARCHŇÁK, R., *Bezpečnost v online prostředí*. Karlovy Vary, 2016, s. 29.

jelikož falešná e-mailová adresa a informace o přesměrování jsou takřka nevypozorovatelné. [44]

4.3.10 **Pharming**

Pharming je sofistikovanější verzí phishingu, účelem je přesměrovat uživatele na zfalšované webové stránky, které jsou opět věrohodnou kopií a jsou k nerozeznání od originálu. Uživatel ale není jako u phishingu okamžitě přesměrován na falešné webové stránky. U pharmingu uživatel zadá do svého webového prohlížeče adresu skutečné webové stránky, na kterou se posléze připojí, ale vzápětí je přesměrován na důvěryhodnou kopii této webové stránky, aniž by si něčeho všiml. Zpravidla se jedná o podvody spojené s bankovními institucemi. Po zadání přihlašovacích údajů k bankovnímu účtu uživatele jsou tyto citlivé údaje odeslány útočníkovi, který je dále využívá k provedení finančních machinací.[45]

4.3.11 **Spamming**

Spamming je označení pro nepožadovanou formu elektronické pošty, zpravidla s reklamním obsahem. Spamming jako takový uživatele neohrožuje, ale zavaluje informační a komunikační technologii. Uživatele pouze připravuje o čas, který tráví mazáním nevyžádaných zpráv. „*Odborníci odhadují, že spam tvoří 40 až 60% veškeré e-mailové komunikace*.“[46] Adresáty elektronické pošty, které jsou terčem spammingu těží marketingové a reklamní agentury z nejrůznějších pramenů. Takovým obvyklým pramenem bývají registrace k různým uživatelským účtům pro bezplatné internetové služby, kde uživatel musí vyplnit své soukromé údaje k jejímu dokončení. Pokud jde o legislativní ukotvení spammingu, tak dle českého práva spamming trestným činem není. Trestné by ale mohlo být shromažďování e-mailových adres, dle §180 TZ – Neoprávněné nakládání s osobními údaji, pokud by k nim útočníkovi umožnila přístup třetí osoba bez svolení jednotlivců.[47]

4.3.12 **Warez**

Warezem se rozumí ilegální množení a sdílení děl, které podléhají autorskému právu. Obvyklým médiem pro jejich množení a sdílení je Internet, ale mohou jimi být

[44] MCCARTHY, L., WELDON-SIVIY, D., ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha, 2013, s. 130.
[45] KOSTRECOVÁ, E., JÓKAY, M., KOSTREC, M. *Počítačová kriminalita.* Bratislava, 2010, s. 55.
[46] POŽÁR, J. *Informační bezpečnost.* Plzeň, 2005, s. 240.
[47] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002, s. 69 - 70.

i jiné nosiče dat. Mezi tato díla patří nejčastěji hudba, filmy, počítačové hry, různé programy aj. Internet tzv. warezeři využívají k tvorbě webových stránek, následné reklamě a prodeje „svých“ produktů.[48] Warezeři tuto ilegální aktivitu provádějí ve skupinách s vnitřní organizační strukturou, kdy má každý na starost něco jiného. Jeden se věnuje prolamování ochrany proti množení těchto děl, jiný se věnuje vytváření webových stránek, další propagaci atd. Značná část warezových uskupení tyto produkty poskytuje zdarma volně ke stažení. Zdrojem peněžních prostředků pak bývá zejména prostřednictvím reklamních sdělení na jejich webových stránkách. Mnohdy také warezeři užívají „začarovaného kruhu“, kdy zájemce k vyhledávanému produktu ani nedostane přístup a webové stránky ho neustále přesměrovávají na další a další stránky a jeho systém se zahltí množstvím mimovolně vyskakujících oken.[49]

4.3.13 **Spoofing**

Spoofing je metoda, díky níž útočník vystupuje pod falešnou identitou, kterou zcizuje své oběti. Spoofing je útočníky užíván jako základní báze k dopouštění se jiným typů počítačové kriminality např. hackingu, phishingu aj. Zejména je využíván k odstranění stop po páchání počítačové trestné činnosti. Metoda spoofingu je postavena na útočníkově výběru počítače, o němž si musí zajistit co největší množství informací, aby daný počítač mohl vyčlenit z běžného chodu a mohl použít jeho funkcí a reagovat místo něj. Útočník si může vytvořit i „zadní vrátka“ tím, že si do daného počítače instaluje hackerské prostředky, které mu umožní i pozdější přístup bez toho, aniž by na počítač opět musel útočit formou spoofingu. Po vybudování zadních vrátek může útočník daný počítač opět uvést v chod a odstranit stopy po jeho konání. Příkladem spoofingu může být elektronická komunikace, kdy je uživateli poslán zfalšovaný e-mail např. od bankovní instituce, ale v poli adresanta se nachází pravá e-mailová adresa bankovní instituce.[50]

4.3.14 **Sociální inženýrství**

Sociální inženýrství je spojení dvou složek, které jsou důležité pro zdárné provedení útoku. Prvním složkou je šok a druhou je odkázání se na hodnověrnou společnost či způsobilou osobu, která je autorem žádosti. Kombinací těchto dvou složek se násobí možnost na oklamání oběti, což má za důsledek i pokles jeho rozvážnosti/střízlivosti. Přesto, že společnost zaopatřuje své zaměstnance prevencí ve

[48] KOSTRECOVÁ, E., JÓKAY, M., KOSTREC, M. *Počítačová kriminalita.* Bratislava, 2010, s. 71.
[49] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002, s. 70.
[50] KOSTRECOVÁ, E., JÓKAY, M., KOSTREC, M. *Počítačová kriminalita.* Bratislava, 2010, s. 85 – 86.

formě edukace, proti těmto útokům přes Internet, existují osoby, které nejsou dostatečně „imunní“ vůči šoku a právě ti jsou často terčem útočníka. Sociálním inženýrstvím se rozumí takové útoky, které jsou spojením technik, škodlivých šifer a jiných různých podob ovlivňování pro dosažení zisku. Po vyzískání důvěry oběti se útok vyvíjí například nakažením počítače škodlivou šifrou anebo využitím dalších forem počítačové kriminality, to vše se souhlasem uživatele počítače. Sociální inženýrství je „machinace“, která tkví v použití psychologických prostředků k vytěžení informací, dat či údajů od třetích osob, které posléze útočník využije k provedení podvodu, útoku na síť, vyzvědačství anebo odcizení totožnosti. Nejčastěji bývá útok prováděn skrze Internet, kdy se útočník vydává například za správce sítě.[51]

5 Hrozby a rizika počítačové kriminality

Začlenění informačních technologií a systémů do každodenního života a jejich používání je pro dnešní dobu neodmyslitelné. Spolu s růstem využívání těchto technologií rostou i větší možnosti k jejich zneužívání a zároveň i počet dopouštění se trestné činnosti.[52]

Počítačová kriminalita se vyznačuje jednáním v kyberprostoru, zaměřeným vůči počítači, či jeho síti anebo se počítač využívá jako prostředek k realizaci trestného činu.[53]

Kyberprostor je prostředím, v němž je komplikované pozorovat činy počítačové kriminality z důvodu obtížné vnímatelnosti. Přístup do tohoto prostředí je možný pouze za pomoci dalších přístrojů, které tak umožní sledovat jednání odehrávající se v kyberprostoru. Výhodou kyberprostoru je, že útočník v tomto prostředí může nenápadně měnit svou polohu, vytrácet se či obměňovat svou totožnost. Útočník tak může tvořit, simulovat či uskutečňovat hrozby s tím, že bude mít stále navrch.[54]

Informační systém se skládá ze softwaru, hardwaru a osob, které zajišťují a spravují jeho provoz. Informační systém má zabezpečovat důvěrnost a integritu ochraňovaných dat a také dostupnost pro vybrané činitele. Další součástí bezpečnosti je

[51] KOSTRECOVÁ, E., JÓKAY, M., KOSTREC, M. *Počítačová kriminalita.* Bratislava, 2010, s. 63.
[52] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 31.
[53] KOLOUCH, J. *CyberCrime*. Praha, 2016, s. 34.
[54] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007, s. 19.

například prokazatelnost učiněného úkonu s daty, prokazatelnost vytvoření datového či programového modulu či anonymnost tvůrce.[55]

Dopad útoku na informační systém je podmíněn jeho povahou, může se projevit formou nepatrných komplikací pro uživatele anebo závažnějšími dopady, jako jsou rozsáhlé peněžní škody či výpadky významných funkcí society. Porucha přístupnosti informačního systému se tak projevuje například dočasným spadnutím webových stránek či přerušením dodávky elektřiny v zasaženém území apod. Pokud se útočníkovi povede kradmé proniknutí a následná úprava či pozměnění informačního systému, má pak šanci ho negativně využívat delší dobu. Potenciální útoky je možno zredukovat kvalitnější ochranou systému. Nicméně žádný informační systém není naprosto a zcela úplně chráněný ani zabezpečený.[56]

Jakékoli trestné činy, nejen v kyberprostoru, znamenají pro společnost hrozbu. Hrozby počítačové kriminality se vyznačují především svou latentností, kdy je činnost útočníka neviditelná a následky trestného činu nejsou pozorovatelně sloučeny s vývojem tohoto činu. Hrozbou se rozumí cokoli, co vede k negativnímu ovlivnění informačního systému, tj. nechtěným modifikacím v systému.[57]

Hrozby se tedy projevují útokem a těží z citlivých míst či slabin, Požár, J. uvádí: *„…chyb v programu nebo v jeho konfiguraci, která umožní útočníkovi získat neoprávněný přístup k datům."* Útočníci pak těchto chyb využívají záměrně či nahodile (v případě havárií, závad, …). Každá hrozba má své vlastní subjektivní hodnocení, která jsou součástí výzkumu zabezpečení informačního systému. U hodnocení záměrných činů je brána v úvahu úroveň obtížnosti a motiv k útoku, u nahodilých hrozeb četnost určitého případu. Ohodnotit úroveň hrozby záměrných činů je možné prostřednictvím odhadu, u nahodilých činů pak na základě výpočtu. Ke ztrátám přivozeným hrozbou se připočítávají i výdaje na restituci a tyto ztráty jsou označovány jako dopad hrozby.[58]

---

[55] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007, s. 20.
[56] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007, s. 20.
[57] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007, s. 20.
[58] POŽÁR, J. *Vybrané hrozby informační bezpečnosti organizace.* [online]. Praha, 2010 : Fakulta bezpečnostního managementu PA ČR v Praze. [cit. 2019-02-25]. Dostupné z WWW: <https://www.cybersecurity.cz/data/pozar2.pdf>.

Za ochranu před útoky se považují všechna hmotná zařízení, vymezené strategie a postupy, které jsou určeny k záštitě informačního systému před hrozbami a útoky. Žádná ochrana ale není dokonalá a vyznačuje se svou křehkostí, tj. výše zmíněnými citlivými místy, slabinami.[59]

Riziko je spojeno s cenou ochraňovaného vlastnictví. Čím vyšší je cena ochraňovaného vlastnictví, tím větší je riziko, že bude proveden útok na zranitelné místo v systému. A naopak, čím bude cena nižší, tím menší bude riziko útoku. Postupy zhodnocení rizik jsou popsány v analýze rizik, jejímž účelem je vyčíslení výloh na ochranu dle hodnoty ochraňovaného vlastnictví.[60]

Požár[61] hrozby dělí na objektivní a subjektivní, kdy do objektivních řadí hrozby způsobené neživou přírodou, technického a fyzikálního původu. Subjektivní hrozby charakterizuje jako hrozby v důsledku lidského činitele, které dále rozděluje na úmyslné a neúmyslné.

Úmyslné a neúmyslné hrozby stejně tak kategorizuje i Jirovský[62]. Mezi úmyslné řadí například cílené vniknutí do informačního systému. Dále úmyslné hrozby dělí na aktivní a pasivní. Dle dopadu na systém aktivní a pasivní hrozby definuje také Požár[63]. Aktivní hrozbou dochází ke změně stavu systému v důsledku narušení integrity a dostupnosti. Jedná se například o modifikaci přenášených dat, například sumy při peněžní operaci. Jako příklad pasivní hrozby uvádí Jirovský sledování chodu, při kterém je zkoumán význam přenášených dat, ale bez modifikace. Neúmyslné hrozby vznikají příčinou pochybení operátora, uživatele či přímo informačního systému.

Dále hrozby Jirovský[64] člení na základní, aktivační a podkladové. Základní hrozby mohou být čtyři. První je ztráta dat, při které jsou vyzrazena či odtajněna neveřejná data neverifikovanému činiteli. Druhá je porušení celistvosti, kdy může dojít k modifikaci dat neverifikovaným činitelem. Třetí je záměrné omezení přístupu k datům či jiným

[59] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007, s. 20.
[60] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007, s. 21.
[61] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005, s. 40.
[62] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007, s. 21.
[63] POŽÁR, J. *Vybrané hrozby informační bezpečnosti organizace.* [online]. Praha, 2010 : Fakulta bezpečnostního managementu PA ČR v Praze. [cit. 2019-02-25]. Dostupné z WWW: <https://www.cybersecurity.cz/data/pozar2.pdf>.
[64] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007, s. 21-24.

pramenům a čtvrtá je ilegální užití zdroje neverifikovaným uživatelem, například proniknutí do systému a následné využívání zpoplatněného programu zadarmo.

Aktivačními hrozbami se rozumí takové hrozby, které vedou k přímé realizaci základní hrozby. Příkladem může být vydávání se za jinou osobu a oklamání tak systému či „trojský kůň", při kterém software v sobě zahrnuje nepozorovatelnou součást, která při jeho aktivaci poškodí zabezpečovací složky.

Podkladové hrozby jsou takové, které přímo realizují několik základních hrozeb. Například proniknutím do systému se aktivují hrozby úniku dat, modifikace dat, tajného sledování atd.

Hrozba, kterou si útočník vybere, bude záviset na jeho motivu a také jeho zkušenostech. Výběr hrozby tedy bude odpovídat útočníkovu úmyslu. Hrozba může být buď zastrašovací, kdy ji útočník nedokončí a k dosažení jeho cíle mu stačí pouze hrozbu znázornit, anebo může dojít k samotnému uskutečnění hrozby. Útočník tak těží ze spletitosti kyberprostoru či nevědomosti své oběti. Bez speciálních vědomostí a schopností je komplikované kybernetickou hrozbu vypátrat, zachytit či ji podmanit. Hrozba může mít i takový charakter, že útočník ani nemusí být způsobilý ji realizovat. Jirovský[65] mezi nejčastější pachatele hrozeb uvádí především radikální, národnostní nebo duchovní uskupení.

6 Odhalování a vyšetřování počítačové kriminality

Trestné činy způsobené počítačovou kriminalitou jsou charakteristické svou proměnlivost, dynamičnost a také značnou mírou latence, která komplikuje práci kriminalistů. Potíží také bývá složitost informačních systémů a to, že stopy obvykle nebývají hmotného charakteru, proto mezi atributy kriminalistů patří zejména odborné vědomosti a dovednosti v této problematice.

Pachatelé těchto činů oplývají vysokým inteligenčním koeficientem, schopností odstraňovat vzniklé důkazy a leckdy také vlivnými kontakty. Škody, které trestnými činy v této oblasti vznikají, nabývají velkého rozsahu a jejich odhalování je složité a z časového hlediska také dlouhé.[66]

[65] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007, s. 25.
[66] GŘIVNA, T., POLČÁK, R., ed. *Kyberkriminalita a právo*. Praha, 2008, s. 87.

Právě prevenci, i přesto, že už k danému trestnému činu došlo, vyzdvihuje Jirovský. Má totiž za to, že prevence, která může omezovat důsledky případného útoku, bývá často opomíjena.[67] Stejně tak i Matějka[68] považuje prevenci za nezastupitelnou a dále ji rozděluje na psychologickou a technologickou.

Psychologickou prevenci považuje za prostředek k šíření osvěty mezi společnost, který přispívá k povědomí o nepovolených jednáních v kyberprostoru. Technologickou prevenci pak především za ochranu technologií. Vývojáři programů nepřetržitě usilují o vývoj lepší a lepší ochrany a útočníci se snaží o její prolomení, bezmezně tak mezi sebou zápolí. Dále je pro psychologickou a technologickou prevenci charakteristické jejich vzájemné působení. Autor také zdůrazňuje nezbytnou vzájemnou kooperaci mezi uživateli počítačů a správci sítí, kteří se musí podílet na snižování možných nebezpečí, kterými počítačová kriminalita oplývá. Jako příklad uvádí: „*Uživatelé například tím, že nebudou spouštět podezřelé soubory získané z Internetu či přílohy z e-mailů, administrátoři zase musí pravidelně sledovat situaci, instalovat zveřejněné záplaty, pravidelně aktualizovat antivirové programy apod.*"[69]

Trestné činy spáchané v kyberprostoru řeší policie, která se snaží dopadnout pachatele v reálném světě[70]. Speciální vyšetřovací týmy sestavené z odborníků v různých oblastech pak pomáhají řešit hrozby, útoky a incidenty, Jirovský, V. : *„ …- od technických expertů přes psychology nebo sociology až po finanční odborníky."*[71]

Takto stanovený tým se primárně zabývá pátráním po příčinách, za kterých daný čin vznikl. Vyšetřovací tým pak dále vymezuje vyšetřovací hypotézy, pracuje s důkazními podklady, podrobuje svědky výslechu, zpětně analyzuje proniknutí do systému, určuje výši škod a ztrát, které spolu s činem nastaly a mnohé další činnosti, které jsou v kontextu s vyšetřováním.[72]

[67] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha, 2007, s. 252-253.
[68] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002, s. 77.
[69] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002, s. 78-80.
[70] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002, s. 82-83.
[71] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha, 2007, s. 261.
[72] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha, 2007, s. 261.

Vzhledem k obtížnosti usvědčení pachatele bývá mnoho činů nepotrestáno, uvádějí Matějka[73] i Smejkal[74]. Mezi nejčastější případy neoznámení trestné činnosti řadí napadení bankovních společností, které si chybu opraví uvnitř společnosti svými zaměstnanci a útok tak vůbec neoznámí. Důvodem je ochrana pověsti a dobrého jména společnosti.

6.1 Důkazní materiál

Při vyšetřování počítačové kriminality se analyzují digitální stopy, tj. elektronické důkazy. Získávají se buď tajným dozorem nad podezřelými, od dodavatelů služeb elektronických komunikací či nedobrovolnými kontrolami podezřelých osob a následným zabavováním.[75]

Z vyšetřovacího hlediska se digitálními stopami rozumí údaje, které za sebou ponechávají všechna technologická zařízení, která nabývají, upravují, poskytují či ukládají data. Smejkal, V.: „*Lze také říci, že digitální stopa je fyzikální interpretací (záznamem) nehmotné informace, zakódované do digitálního formátu."* Významnou roli ve vyšetřování také hraje prokazatelnost digitálních důkazů, neboť je potřeba, aby od jejich zabavení až do dokončení odborného vyšetřování zůstaly v neměnném stavu. *„Proto se pracuje s duplikátem digitální stopy, což je přesná digitální reprodukce všech datových objektů obsažených na originálním fyzickém objektu na fyzicky stejný typ datového média.*" Jestliže vyšetřovatelé nezískají přístup ke hmotnému nosiči dat a vyhotovení duplikátu digitální stopy je nerealizovatelné, vytvářejí poté kopii digitální stopy, kterou zhotovují z datových objektů, které mají totožný informační obsah. Ne všechny původní informace ale musí být opatřeny, některé totiž mohou být skryty nebo nejdou zkopírovat a jejich význam prokazatelnosti je tak nižší.[76]

Počítačová kriminalita se svou podstatou liší od obvyklých forem klasické kriminality a jsou pro ni příznačné tyto rysy:

- škody zapříčiněné počítačovou kriminalitou se svízelně vyšetřují i vykonstruovávají
- hardware, na který byl proveden útok, nelze ve všech případech zaobstarat jako podklad k důkazům, neboť by z toho pro oběť vyplývaly další škody

[73] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002, s. 81.
[74] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2015, s. 498.
[75] ZAVRŠNIK, A. *Kyberkriminalita*. Praha, 2017, s. 55 - 57.
[76] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2015, s. 492 - 493.

- na zdařilé vyšetřování počítačové kriminality působí fundamentálně kvalita a včasné zajištění digitálních stop
- digitální stopy se vyznačují svou rozsáhlostí, rychlým vývojem, krátkou životností a také tím, že mohou být obšírně dislokovány do značně velké plochy
- k rozboru a rozšifrování digitálních stop je třeba expertního softwaru či hardwaru
- v právních postupech je přijetí digitálních stop omezené, neboť je obtížné je prokázat (zde autor uvádí: *„ …je obtížné prokázat např. kopii od originálu"*)[77]

Velkou roli ve vyšetřování také hraje odhalení motivu kybernetického trestného činu, který zmiňuje jak Matějka[78], tak Smejkal[79], neboť se z něj dá vytipovat možný pachatel z již definovaných podezřelých jedinců. Motivem pak bývá např. snadný zisk, zastírané motivy k zatajení odlišného trestného jednání, motivy s politickým kontextem, motivy související s porušováním autorského práva atd. Pachateli bývají často zaměstnanci, dále hackeři, kteří umí např. zavirovat či proniknout do jiných počítačů, pak jsou pachatelé kteří svou skupinovou činností páchají organizovaný zločin, kdy členové tohoto uskupení využívají počítače například k výrobě padělků. Dále jsou pak profesionálové, kteří jsou za určitý finanční obnos schopni např. odhalit státní tajná data. Kybernetickou trestnou činnost páchají ale také děti a mladiství. Pro ně je příznačná díky věku nízká rozpoznávací schopnost, a tak si mnohdy ani neuvědomují, že páchají trestnou činnost.[80]

7 Organizace bojující proti počítačové kriminalitě

Problematikou počítačové kriminality, jakožto problematikou s přeshraničním charakterem se zabývá několik organizací, které spolupůsobí na úrovni států. Tyto organizace mají nelehký úkol. Jejich cílem je proti kybernetickým trestným činům bojovat či jim předcházet, anebo se podílet na jejich odhalování a vyšetřování apod.[81] Dále je uveden jen malý výčet z nich.

[77] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha, 2007, s. 251-252.
[78] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002, s. 85.
[79] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2015, s. 486.
[80] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2015, s. 487 - 488.
[81] ZAVRŠNIK, A. *Kyberkriminalita.* Praha, 2017, s. 74.

7.1 Organizace pro hospodářskou spolupráci a rozvoj

Organizace pro hospodářskou spolupráci a rozvoj (Organisation for Economic Co-Operation and Development, dále jen OECD), má za cíl podporu politik, které zvýší úroveň hospodářského a sociálního zabezpečení osob na celém světě. Propůjčuje vládám tzv. fórum, kde se mohou podílet se svými znalostmi a zkušenostmi a hledat tak ke kolektivním problémům východiska.[82] Jako první začala bojovat proti počítačové kriminalitě poté, co její rada prozkoumala eventuality mezinárodní koordinace trestních zákonů ve střetu s hospodářskou kriminalitou spjatou s počítači. Roku 2002 schválila OECD Směrnice pro bezpečnost sítí a informací, ty se od roku 2012 podrobují revizi.[83]

7.2 Evropská unie

Evropská unie coby mezinárodní organizace s 28 členskými státy má za cíl zvednout úroveň kooperace v Evropě.[84] Až do konce druhého milénia téma počítačové kriminality neznázorňovalo pro Evropskou unii nijak zvlášť podstatný problém, a tak do té doby neexistoval v EU žádný právní předpis týkající se počítačové trestné činnosti. V roce 2000 si Evropská komise dala za cíl podat zákonodárné iniciativy se záměrem spojování trestního práva hmotného v odvětví počítačové kriminality.[85]

V roce 2016 zavedla podobnou směrnici jako OECD - Směrnice o bezpečnosti sítí a informací v Unii, „*...první horizontální právní předpis EU, který řeší výzvy oblasti kybernetické bezpečnosti a přináší skutečnou změnu z hlediska odolnosti vůči bezpečnostním hrozbám a spolupráce v Evropě.*

Má tři hlavní cíle:

- *zlepšení vnitrostátních schopností v oblasti kybernetické bezpečnosti,*
- *rozvíjení spolupráce na úrovni EU a*
- *podporu kultury řízení rizik a hlášení incidentů mezi klíčovými hospodářskými subjekty, zejména provozovateli poskytujícími základní služby pro zachování hospodářských a sociálních činností a poskytovateli digitálních služeb.*“ [86]

---

[82] *Our mission* [online]. [cit. 2019-03-20]. Dostupné z WWW: <http://www.oecd.org/about/>.
[83] ZAVRŠNIK, A. *Kyberkriminalita.* Praha, 2017, s. 74.
[84] *Evropská unie.* [online]. [cit. 2019-03-20]. Dostupné z WWW: <https://www.mvcr.cz/clanek/mezinarodni-organizace-a-vs-evropska-unie.aspx>.
[85] *Kriminológia ako súčasť trestnej politiky: pocta prof. PhDr. Květoňovi Holcrovi, DrSc. k 80. narodeninám.* Praha, 2018, s. 107
[86] *Sdělení komise evropskému parlamentu a radě.* Brusel : Evropská komise, 2017 [cit. 2019-03-20]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52017DC0476>.

7.3 Rada Evropy

Rada Evropy je nadnárodní organizací, jejímž cílem je vybudování kolektivního demokratického a právního prostředí, které zajišťuje zachovávání lidských práv a svobod, demokratickou formu vlády a dodržování právních norem.[87] V roce 2001 vytvořila první komplexní úmluvu v oblasti kybernetické kriminality, která sloučila hmotná vymezení pojmů v této oblasti, stanovila další východiska pro trestní právo procesní ke snadnějšímu a pohotovějšímu vyšetřování a také ulehčila internacionální součinnost soudních orgánů.[88]

Později, v roce 2003 byla rozšířena o Dodatkový protokol k Úmluvě Rady Evropy o počítačové kriminalitě. Ten se zaobírá obviněními z trestných činů v oblasti xenofobie či rasismu provedených skrze počítač. Dále byl zřízen Výbor Úmluvy o počítačové kriminalitě a přijat projekt s názvem Chobotnice, který pořádá celosvětové kongresy na téma počítačová kriminalita. Mimo své členy poskytuje Rada Evropy celosvětovou technickou asistenci soudním orgánům ve věcech trestních při odezvě na počítačovou kriminalitu a při zajišťování a aplikování důkazního materiálu.[89]

Dále každoročně organizuje kongres a spravuje sdružení Octopus Cybercrime Community. [90]

„*Octopus Community je platformou pro sdílení informací a spolupráci v oblasti počítačové kriminality a elektronických důkazů. Online nástroje - Profily zemí Wiki o legislativě a politikách v oblasti počítačové kriminality, školicích materiálů, blogu - sdružují odborníky, partnery, akademiky a profesionály v oblasti počítačové kriminality.*“ („*The Octopus Community is a platform for information sharing and cooperation on cybercrime and electronic evidence. The online tools – Country Wiki profiles on cybercrime legislation and policies, training materials, blog – bring together experts, counterparts, academics and professionals in the cybercrime field*.“)[91]

[87] *Rada Evropy (RE), anglicky Council of Europe (CoE).* [online]. 2015 [cit. 2019-03-20]. Dostupné z WWW: <http://www.radaevropy.cz>.
[88] ZAVRŠNIK, A. *Kyberkriminalita.* Praha, 2017, s. 74.
[89] ZAVRŠNIK, A. *Kyberkriminalita.* Praha, 2017, s. 74 - 75.
[90] ZAVRŠNIK, A. *Kyberkriminalita*. Praha, 2017, s. 75 - 76.
[91] *Octopus Cybercrime Community*. [online]. [cit.2019-04-05]. Dostupné z WWW: <https://www.coe.int/en/web/octopus/home>.

7.4 G8

G8 - organizace 7 ekonomicky nejvyspělejších států světa + Ruska se přidružila k podnětům o koordinaci právních regulací v odvětví počítačové kriminality. Komise odborníků podpořila Radu Evropy a doporučila přijetí a podepsání Úmluvy Rady Evropy o počítačové kriminalitě a také zdůraznila, že úmluva může být taktéž schválena a podepsána i nečlenskými zeměmi Rady Evropy.[92]

7.5 OSN

OSN je organizací spojených národů a jejím hlavním cílem je zachovávat mezi národy mír a také bezpečnost.[93] Nejstarší organizací OSN je Mezinárodní telekomunikační unie (International Telecommunication Union, dále jen ITU) založená v roce 1865 spolu se zrodem telegrafů. Jejím cílem bylo ústředně tvořit a stvrzovat normy pro telekomunikace. S počátkem Internetu přišla ITU o hlavní úlohu v řízení telekomunikace. Také se spolu se vznikem Internetu chtěla dostat do střetu s počítačovou kriminalitou, neúspěšně. Nyní se věnuje devíti odvětvím, která jsou spojena s informační a komunikační technologií. Například inteligentní komunikací či inteligentními automobily do budoucna, ale také počítačovou bezpečností. Počítačové bezpečnosti se věnuje odvětví ITU - Sektor rozvoje telekomunikací, jenž má za úkol zaručit počítačovou bezpečnost a také vytvářet důvěru spolu s užíváním informační a komunikační technologie. Mezi další činnosti ITU patří rozbor pěti odvětví, který po jeho vyhodnocení publikuje jako ukazatel poměru světové počítačové bezpečnosti (Global Cybersecurity Index). Dále také poskytuje podporu státům při zřizování středisek, která se zabývají východisky v informační bezpečnosti atd.[94]

8 Vliv lidského činitele na únik informací

„Při hodnocení úniku nebo zneužití informací se ukazuje, že nejslabším článkem v celém systému ochrany je lidský faktor.“[95]

Lidský činitel plní důležitou funkci při záštitě informací, je jejím nejvýznamnějším a zároveň tím nejméně silným dílkem v celém sledu jejich

[92] KOSTRECOVÁ, E., JÓKAY, M., KOSTREC, M. *Počítačová kriminalita.* Bratislava, 2010, s. 4.
[93] *Cíle organizace.* [online]. Praha [cit. 2019-03-20]. Dostupné z WWW: <https://www.osn.cz/osn/cil/>.
[94] ZAVRŠNIK, A. Kyberkriminalita. Praha, 2017, s. 76 - 77.
[95] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005, s. 60.

transformace. Člověk buduje a systematizuje systém ochrany, naproti tomu je to zase on, kdo tento systém porušuje, vyhýbá se mu a střežené informace odhaluje.[96]

Ochranou dat se rozumí komplex ochranných prostředků vůči neoprávněnému využití, rozmnožování, deformování, poškozování a destrukci počítačových informací či dat. Tato ochrana se uskutečňuje prostřednictvím programových a technických nástrojů, organizačních nařízení apod.[97]

Významnou úlohu spojenou s ochranou dat má programové vybavení počítače, které může plnit funkci dohledu, formu uspořádání a formování programů počítače. Programová ochrana počítače pojímá celou řadu nástrojů, například bezpečný operační systém, speciální programy zajišťující ochranu, mazání mezipaměti, kódovací a testovací programy apod.[98]

Pro zdárné vzdorování četným nástrahám je vhodné dbát na pár důležitých principů zabezpečení, mezi něž R. Kohout a R. Karchňák[99] například řadí a dále popisují:

- „*aktualizovaný operační systém*
- *aktualizovaný software*
- *antivirový program*
- *firewall*
- *zabezpečený router*.“

8.1 Aktualizovaný operační systém

Operační systém je výchozí program, kterým je opatřeno každé technické zařízení a které dává možnost uživateli takové zařízení řídit včetně zařízení, která jsou k němu připojena. Jde o značně složitý software, který v sobě zahrnuje ovladače připojených periferií, rozčleňuje systémové nástroje mezi zapnuté programy atd. Je nezbytné zachovávat operační systém aktualizovaný, neboť útočníci zneužívají jeho chyb. Vývojáři pravidelně opravují chyby v programových kódech a přinášejí nové aktualizace operačního systému.

[96] BÍMOVÁ, A. *Počítačová kriminalita a naše doba.* Praha, 1990, s. 84 - 85.
[97] BÍMOVÁ, A. *Počítačová kriminalita a naše doba.* Praha, 1990, s. 85.
[98] BÍMOVÁ, A. *Počítačová kriminalita a naše doba.* Praha, 1990, s. 90.
[99] KOHOUT, R., KARCHŇÁK, R., *Bezpečnost v online prostředí*. Karlovy Vary, 2016, s. 10 - 12.

8.2 Software

Uživatelé využívají několika rozdílných programů – softwarů, příznačných pro určitý okruh činnosti (webové prohlížeče, programy pro úpravu PDF souborů, kancelářské balíčky atd.). Každý takový program, stejně jako operační systém, sestává ze stovek tisíc řádků programové šifry, kde je velká možnost eventuální chyby. Blízko k útokům v internetovém prostředí mají především webové prohlížeče, proto je nezbytná jejich pravidelná aktualizace. Předností webového prohlížeče je jeho ovládání, uživatel tak může mnohdy sám postřehnout potenciální útok a zavčas se ho vyvarovat.

8.3 Antivirový program

Antivirový program je takový software, který poskytuje ochranu před malwarem - jeho odhalování, odstranění jeho aktivity či kompletní odstranění. Ničivé šifry odhaluje podle svých souborů informací a dat a také dle stylu jednání nainstalovaných programů. Antivirové programy uskutečňují mnoho funkcí současně z důvodu hodnotné ochrany, např. ochrana před viry, rezidentní antivirový štít atd. Dle odborníků vzniká každým dnem minimálně deset nových virů, na které je zapotřebí, aby antivirový program projevil reakci. Používání antivirového programu, který by nebyl aktualizovaný, by tak bylo bezúčelné.

8.4 Firewall

„*Firewall je program, který dohlíží na datový tok mezi užívaným zařízením a vnější počítačovou sítí*.“ Takový datový tok dovede revidovat, usměrňovat či vadný datový tok zarazit. Uživatel může na tento datový tok dohlížet či korigovat kterýkoli datový tok zvnějšku. Firewall je obvykle dodáván spolu s antivirovým programem společností, jako souhrnná ochrana.

8.5 Zabezpečený router

„*Router je zařízení, které propojuje dvě různé počítačové sítě a routuje (směruje) mezi nimi datový tok. Většina všech domácností je k internetu připojena právě skrze router.*“ Router, který není zabezpečený bývá nástrojem pro vniknutí do počítačové sítě bez oprávnění anebo je použit jako „vstup“ pro dopouštění se trestné činnosti na Internetu.

Zřídkakdo router totiž otočí, aby se dozvěděl, že přístupové jméno i heslo do správy tohoto zařízení je opatřeno totožným slovem „admin“. Postačí, když uživatel po koupi a uvedení routeru v provoz změní předem dané heslo pro jeho správu.

8.6 Zálohování dat

Zálohování dat je jeden z nejbezpečnějších způsobů, jak si může uživatel uchránit svá data. Ztráta dat nemusí být zapříčiněna pouze kybernetickými útoky, ale mohou být omylem smazány samotným uživatelem či poničením pevného disku počítače. Data si uživatel může zálohovat na optická média, jako jsou CD, DVD aj. Nedostatkem optických médií je, že jsou časově omezena. Po delší době se mohou stát nečitelná, a tak je třeba zálohu po nějakém čase opakovat. Dále může zálohovat na externí pevné disky či na cloudové úložiště – virtuální datový prostor, který je přístupný z jakéholiv zařízení a odkudkoliv (např. iCloud, OneDrive aj.). Předností cloudového úložiště je bezprostřední spárování dat mezi zařízeními, která jsou připojena. Nedostatkem cloudového zařízení je, že je vázané na rychlosti Internetového připojení a také fakt, že uživatel svá data poskytuje třetí osobě.[100]

8.7 Heslo

Dalším zabezpečovacím prvkem je heslo. Heslo je primární obrannou bariérou uživatele vůči potencialním útočníkům. Dnes musí uživatel mít heslo k většině webových služeb a aplikacím, a to vede k tomu, že uživatel používá pro všechny tyto služby jedno heslo. Toho využívají útočníci a jeden z jejich způsobů je prolomení a identifikování hesla k webovým službám, které nejsou tolik zabezpečené a poté jich užije u více zabezpečených webových služeb.[101]

Mělo by mít více jak 8 znaků, užití malých a velkých písmen, číslic a jiných speciálních znaků. R. Kohout a R. Karchňák popisují návod, jak si vytvořit heslo, které bude pro uživatele snadno zapamatovatelné a neprolomitelné.[102]

[100] KOHOUT, R., KARCHŇÁK, R., *Bezpečnost v online prostředí*. Karlovy Vary, 2016, s. 13 - 14.
[101] KOHOUT, R., KARCHŇÁK, R., *Bezpečnost v online prostředí*. Karlovy Vary, 2016, s. 18.
[102] KOHOUT, R., KARCHŇÁK, R., *Bezpečnost v online prostředí*. Karlovy Vary, 2016, s. 18.

Tak dlouho se chodí se džbánem pro vodu, až se ucho utrhne. - Tdscsdpv;Asuu!

Tabulka 1: Příklad

T	Tak
d	dlouho
s	se
c	chodí
s	se
d	džbánem
p	pro
v	vodu
;	,
A	až
s	se
u	ucho
u	utrhne
!	.

Zdroj: vlastní zpracování dle návodu R. Kohouta a R. Karchňáka (2016)

K výše zmíněnému problému užívání jednoho hesla pro všechny webové služby a aplikace uvádí R. Kohout a R. Karchňák řešení, a to takové, že uživatel k heslu přidá zkratku zařízení, programu či služby apod., ke kterým se přihlašuje.[103]

Příklad: Tdscsdpv;Asuu!Pc - přihlášení k počítači

Zdroj: vlastní zpracování dle návodu R. Kohouta a R. Karchňáka (2016)

T. Petrowski[104] rozděluje uživatele dle výběru hesla na tyto skupiny:

Důvěřivec - do této skupiny řadí lidi, kteří používají jednoduchá hesla typu: 12345, heslo, …

Rodinný typ - osoby, které použijí jméno své manželky, dětí či jiných blízkých

Příznivec sportu - volba hesla padá na oblíbený fotbalový tým, oblíbený sport, hráče apod.

Konzervativec - sem patří hesla odvozená z minulosti, např. název studované školy apod.

[103] KOHOUT, R., KARCHŇÁK, R., *Bezpečnost v online prostředí*. Karlovy Vary, 2016, s. 21.
[104] PETROWSKI, T. *Bezpečí na internetu.* Liberec, 2014, s. 102 – 103.

Hračička - lidé spadající do této skupiny kombinují předešlá hesla s čísly, kupříkladu ke svému oblíbenému sportu přidají číslo.

Dále T. Petrowski[105] uvádí škálu nejpopulárnějších hesel od 1 do 10:

1. *„jména domácích zvířecích mazlíčků*
2. *koníčky*
3. *rodné příjmení matky*
4. *den narození někoho z rodiny*
5. *vlastní narozeniny*
6. *jméno partnera*
7. *vlastní jméno*
8. *název oblíbeného fotbalového klubu*
9. *oblíbená barva*
10. *název základní školy.“*

9 Trend vývoje počítačové kriminality

Počítačová kriminalita stále rozkvétá díky těm, kteří v ní hledají svůj zdroj výdělku. Způsoby útočníků jsou stále sofistikovanější, z tohoto důvodu je ochrana nepostradatelná. V roce 2004 překročil počet uživatelů Internetu 100 milionů[106], v roce 2019 je toto číslo mnohonásobně větší, přes tři a půl miliardy.[107]

Požár[108] v knize z roku 2005 uvádí možné trendy v oblasti počítačové kriminality. Tyto trendy je možné použít i pro dnešní dobu:

- útoky bude možné vykonat výhradně online

[105] PETROWSKI, T. *Bezpečí na internetu.* Liberec, 2014, s. 103.
[106] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005, s. 258.
[107] *Internet.* [online]. 2019 [cit. 2019-04-15]. Dostupné z WWW: <http://www.statistiky.wz.cz/?pg=internet>.
[108] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005, s. 258 - 260.

- vzestup phishingu, budou ve větším množství rozesílány klamné zprávy pomocí elektronické pošty z domnělých oficiálních pramenů; tyto zprávy zahrnují požadavky na aktualizaci osobních či přihlašovacích údajů, např. změna hesla aj.

- nárůst spammingu, který zprostředkuje stažení viru, např. trojského koně a nakazí tak nezabezpečný počítač bez vědomí uživatele

- nárůst spywaru, útočníci stále více cílí na peněžní zisk a prostřednictvím spywaru tak budou mnohem více využívat cizí identity, či zaznamenávat stisklé znaky na klávesnici uživatele se záměrem získání osobních údajů

Dalšími trendy pokračuje Matějka (2002)[109]:

- útočníci budou pramenit více z novodobých organizovaných zločineckých skupin, s veškerými náležitostmi – „*...rozdělením pravomocí, mlčenlivostí, dokonalou podporou právníků a v neposlední řadě i politickou ochranou.*“

- nárůst zneužívání lidského činitele formou úplatku či zastrašení k vyzrazení citlivých údajů

- redukce poskytovaných bezplatných online služeb na Internetu.

[109] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002, s. 90 - 95.

10 Praktická část

10.1 Metodologie výzkumu

Jako metoda pro šetření bylo sestaveno dotazníkové šetření, které se skládalo ze 14 uzavřených otázek.

Cílem dotazníkového šetření bylo zjistit, zda si dotazovaní uvědomují rizika plynoucí z používání počítače a zda se na Internetu chovají obezřetně, a také jak tyto otázky souvisí s věkem a vzděláním dotazovaného. Čím starší a vzdělanější, tím víc by se dotazovaný měl chovat v kyberprostoru prozíravě. Naopak jestli je dotazovaný žena či muž by na tento problém nemělo mít vliv.

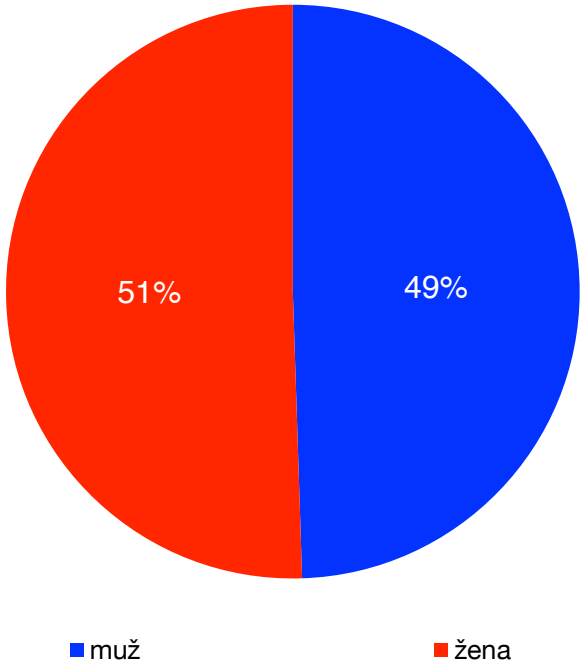
Sběr dat byl proveden tištěnou formou. Autorka se snažila oslovit veřejnost na ulici, kde byla povětšinou odmítána z důvodu nedostatku času. Dále dotazníky rozdala mezi své přátele, svým příbuzným, kteří je rozdali u sebe v práci a bratrovi, který je rozdal ve své třídě v devátém ročníku základní školy. Z celkových 300 rozdaných dotazníků se jich 196 vrátilo vyplněných. Návratnost tak byla 65,3%. Ve dvou dotaznících odpověděli dva muži ve věku 15 - 18 let, že jejich nejvyšší dosažené vzdělání je vysokoškolské. Tyto dotazníky autorka z průzkumu vyřadila, neboť by zkreslovaly výsledky. Zkoumaný vzorek tak čítal 194 respondentů, tj. 64,6% z celkového počtu rozdaných dotazníků.

Dotazníkové šetření bylo započato 12. 12. 2018, poslední dotazníky byly vybrány 4. 1. 2019.

Jednotlivé odpovědi na otázky jsou zhodnoceny v tabulkách dle posloupnosti v dotazníkovém šetření a poté vyobrazeny ve výsečových grafech.

10.2 Diskuse výsledků

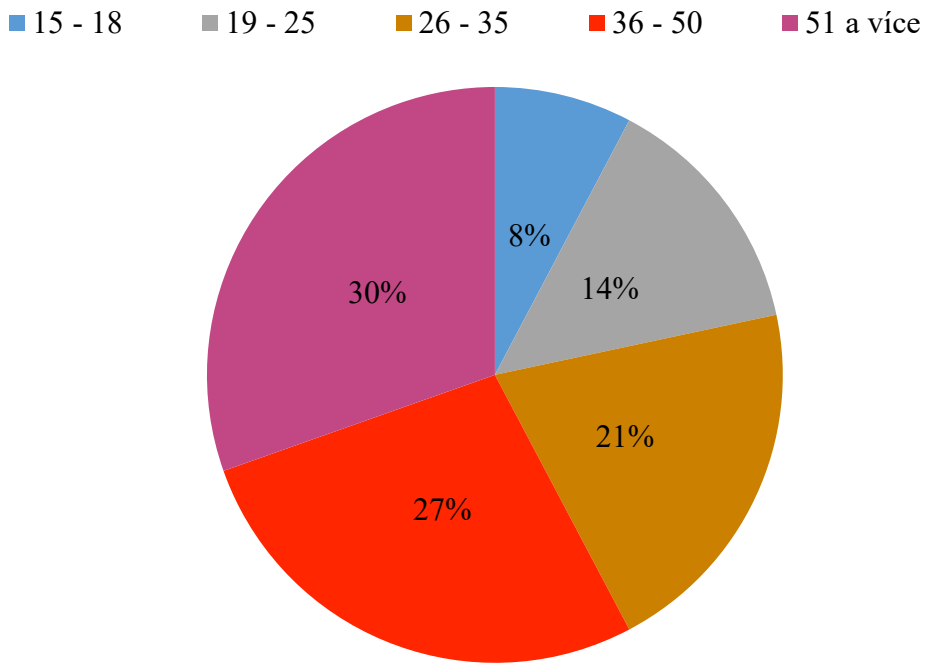
Graf č. 1: Pohlaví?



Zdroj: vlastní zpracování

Na otázku odpovědělo 96 mužů, tj. 49% a 98 žen, tj. 51%. Dotazníkové šetření tak bylo vyvážené a ani jedno pohlaví nebylo ve velké převaze.

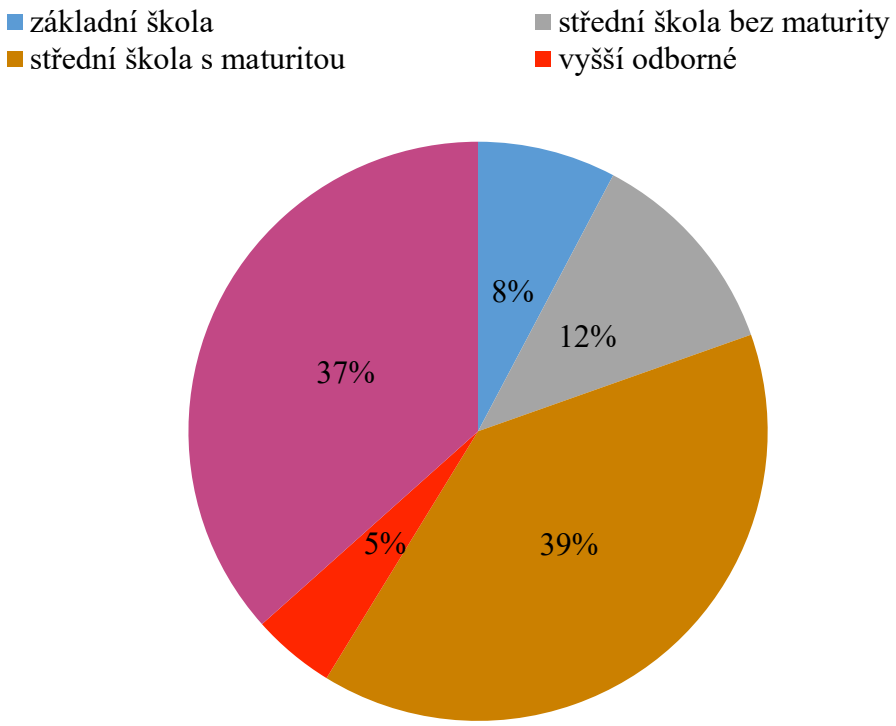
Graf č. 2: Jaký je Váš věk?



Zdroj: vlastní zpracování

Tato otázka byla zvolena, aby se ukázalo, jak se jednotlivé věkové skupiny chrání před počítačovou kriminalitou. Nejvíce odpovědí, 30%, bylo získáno od respondentů ve věkové kategorii 51 a více let, dále 27% tvořila věková kategorie 36 - 50 let, 21% odpovědí bylo získáno od skupiny ve věku 26 - 35 let, 14% věková kategorie 19 - 25 let a 8% tvořili ti nejmladší ve věku 15 - 18 let. Odpovědi tak byly získány sestupně dle věku, čím byli respondenti starší, tím více odpovídali v dotazníkovém šetření.

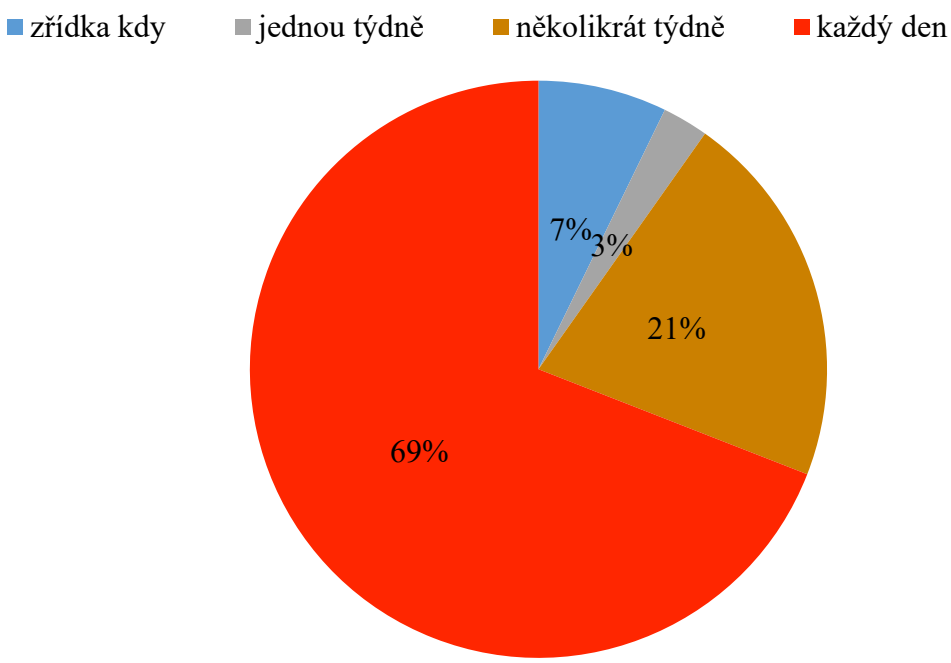
Graf č. 3: Jaké je Vaše nejvyšší dosažené vzdělání?



Zdroj: vlastní zpracování

Nejvíce odpovídali respondenti se středoškolským vzděláním zakončeným maturitou 39%, poté s vysokoškolským vzděláním 37%, 12% dotazovaných získalo středoškolské vzdělání bez maturity, 8% základní vzdělání a zbylých 5% vyšší odborné vzdělání.

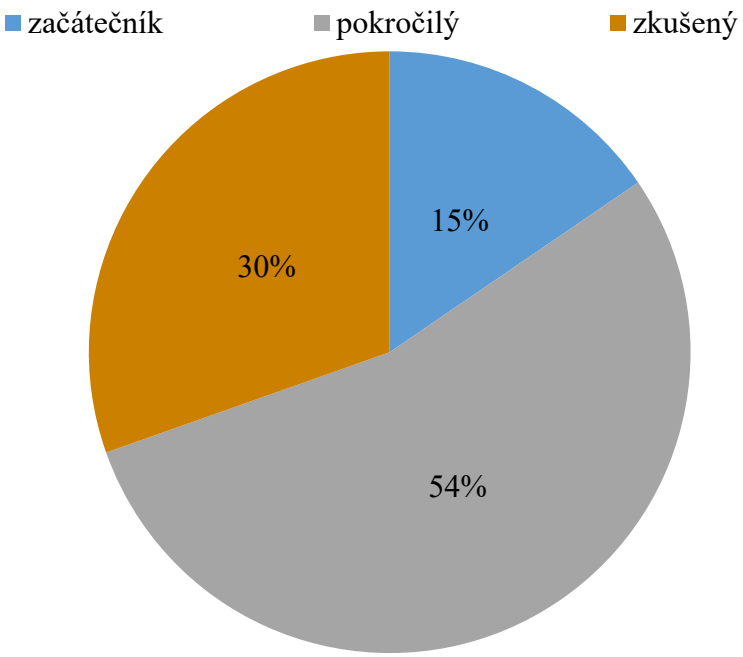
Graf č. 4: Jak často trávíte na počítači svůj čas?



Zdroj: vlastní zpracování

Denně tráví na počítači svůj čas 69% dotazovaných, 21% stráví svůj čas u počítače několikrát do týdne, 7% respondentů odpovědělo, že jsou na počítači zřídka kdy a zbylé 3% odpovědělo, že jsou na počítači jednou týdně.

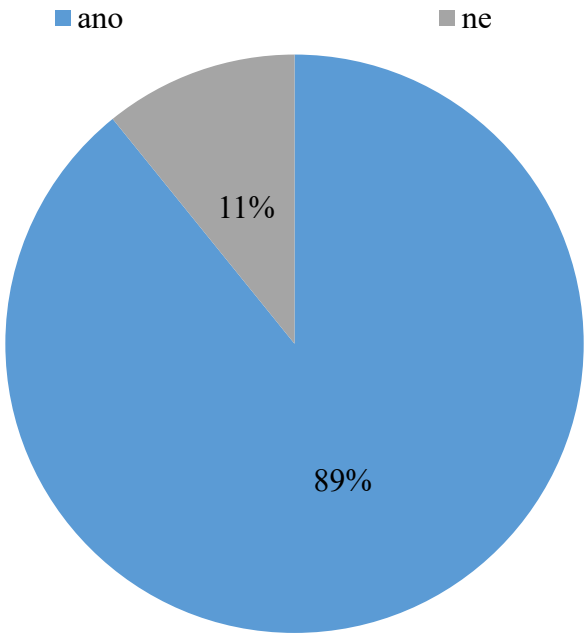
Graf č. 5: Jaká je Vaše schopnost pracovat na počítači?



Zdroj: vlastní zpracování

K této otázce byly přiřazeny odpovědi začátečník, pokročilý a zkušený. Respondenti tak měli možnost ohodnotit své dovednosti na třístupňové škále odpovědí. Začátečník se svými znalostmi tak nemusí vědět o možných hrozbách, kterými kyberprostor disponuje a také nemusí vědět, jak těmto hrozbám předcházet. Pokročilým byl myšlen běžný uživatel počítače, ten by měl vědět, jak se chránit, ale mohlo by ho něco překvapit. Zkušeným byl myšlen ten, kdo se v počítačích vyzná na úrovni např. IT technika apod. Toho by nemělo "nic" překvapit, a měl by vědět o možných rizicích a umět se jim vyvarovat a v případě napadení počítače virem, by si měl poradit s odvirováním svého počítače. Za pokročilého uživatele se považuje 54% dotazovaných, za zkušeného 30% a 15% odpovědělo, že je na úrovni začátečníka v ovládání funkcí počítače.

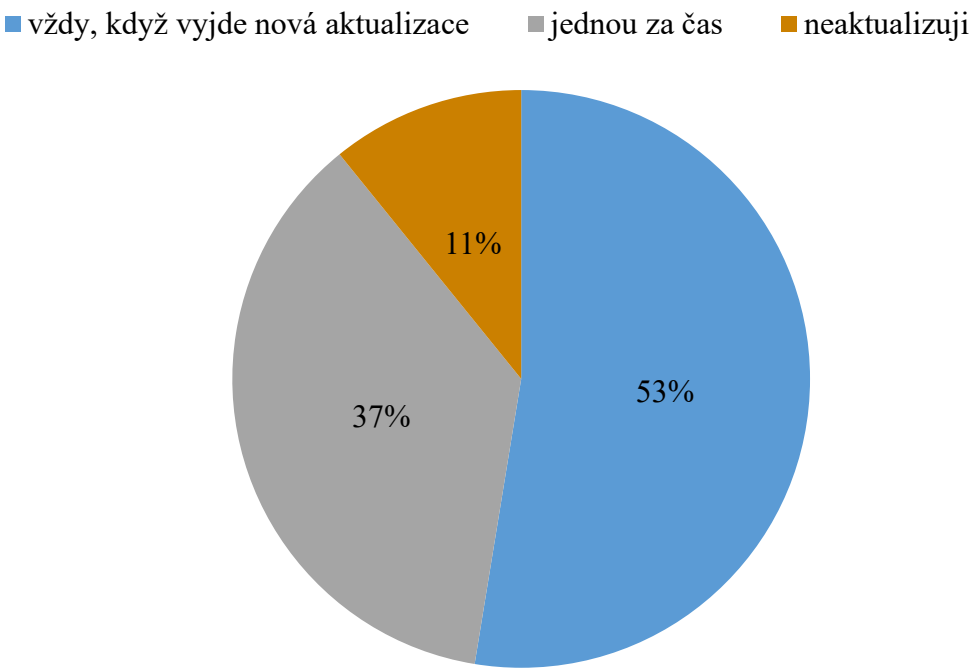
Graf č. 6: Používáte na Vašem počítači antivirový program?



Zdroj: vlastní zpracování

Cílem bylo zjistit, zda se dotazovaní chrání před možným napadením, tímto nejmenším krokem, jako je nainstalování antivirového systému. Naprostá většina, 89% dotazovaných, odpovědělo, že na svém počítači nainstalovaný antivirový systém mají a zbylých 11% odpovědělo, že antivirový program nemají.

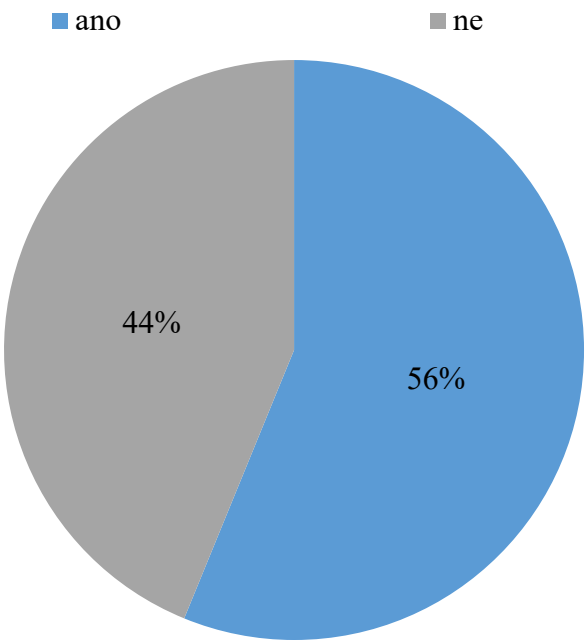
Graf č. 7: Jak často aktualizujete svůj operační systém?



Zdroj: vlastní zpracování

Aktualizace operačního systému je důležitá z důvodu, že autoři operačních systémů v aktualizacích odstraňují chyby, které se naskytly v předchozích verzích. Aktualizací se tak zabrání možnému využití chyb a napadení počítače. Svůj počítač aktualizuje vždy, když vyjde nová aktualizace 53% dotazovaných, 37% aktualizuje operační systém jednou za čas a 11% neaktualizuje operační systém na svém počítači dle své odpovědi vůbec.

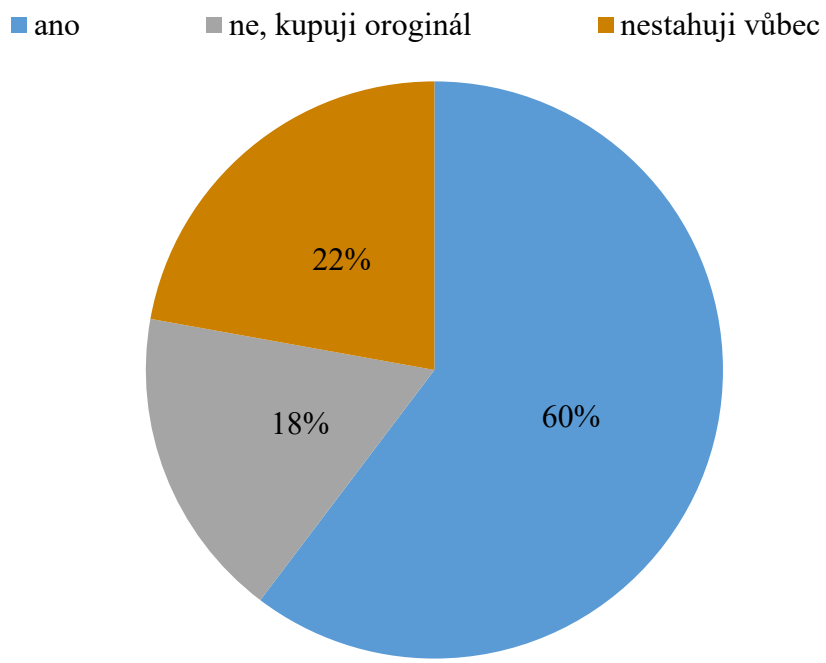
Graf č. 8: Máte obavu, že byste se mohl/a stát obětí počítačové kriminality?



Zdroj: vlastní zpracování

Otázka byla položena z důvodu, zda respondenti přemýšlejí či si uvědomují možné riziko spojené s používáním počítače či chováním na počítači. 56% uvedlo, že obavu mají, 44% uvedlo, že tuto obavu nemá.

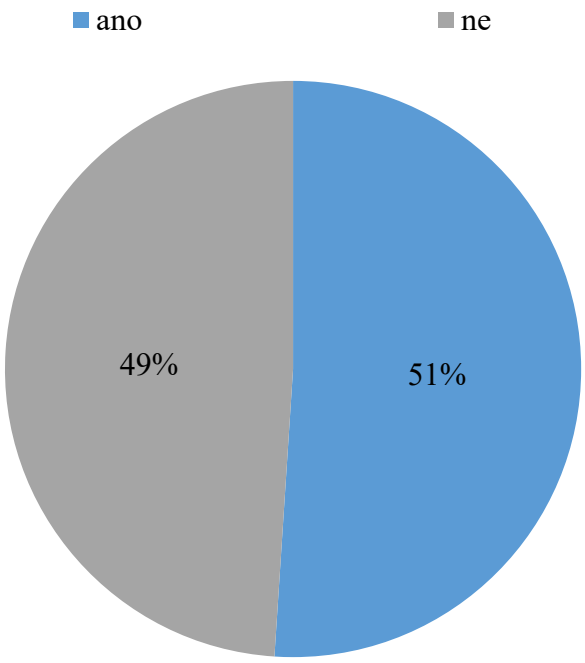
Graf č. 9: Stahujete z internetu filmy, hudbu aj. zadarmo?



Zdroj: vlastní zpracování

Respondenti, kteří odpověděli, že ano, se dobrovolně vystavují riziku, že jejich počítač může být infikován virem. I přes možné riziko majoritní část respondentů, 60%, na tuto otázku odpovědělo, že stahuje výše zmíněné zadarmo, tudíž porušují autorský zákon a dopouštějí se tak trestné činnosti. 18% respondentů si za tyto služby platí a hudbu, filmy a jiné si kupuje nebo pouze propůjčuje za peníze, a tak chrání svůj počítač před možným stažením viru. Možnost v odpovědích byla i "nestahuji vůbec", tuto možnost zvolilo 22% dotazovaných.

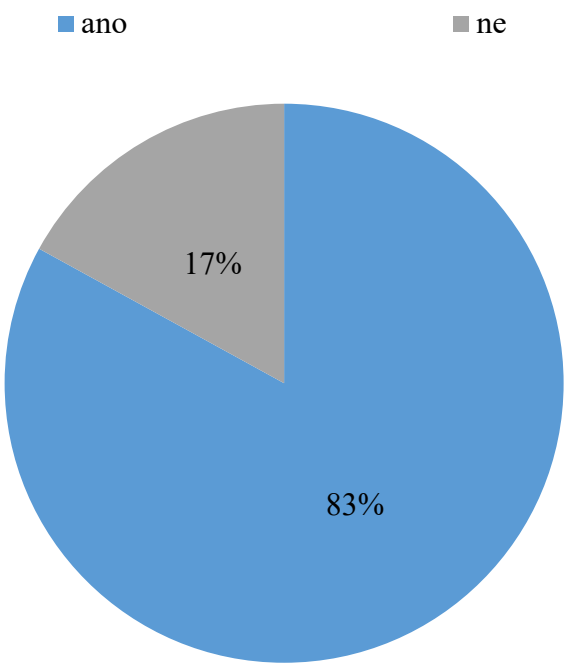
Graf č. 10: Byl někdy Váš počítač nakažen virem?



Zdroj: vlastní zpracování

Otázka byla položena z důvodu zjištění, zda se respondenti s počítačovou kriminalitou v minulosti již setkali, 51% uvedlo, že jejich počítač již někdy v minulosti nakažen virem byl a 49% dotazovaných uvedlo, že se s virem v počítači ještě nesetkalo.

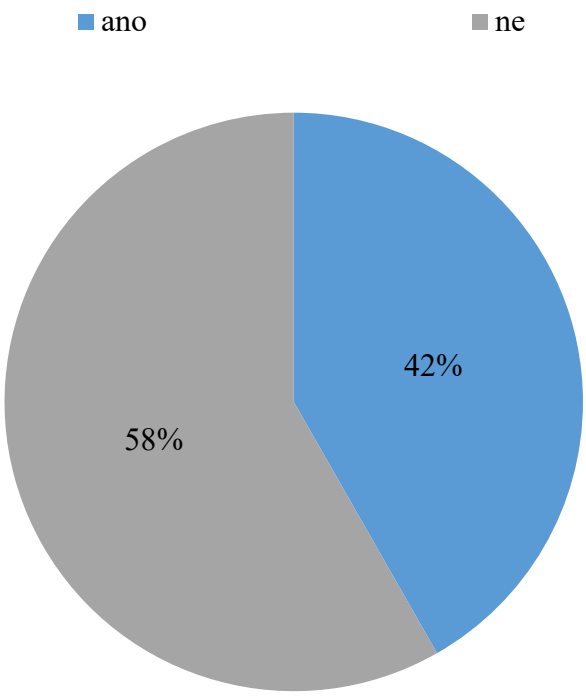
Graf č. 11: Používáte bezpečná hesla? (více než 8 znaků, kombinace malých a velkých písmen, čísla…)



Zdroj: vlastní zpracování

Tato otázka měla prověřit, zda si své účty dotazovaní chrání bezpečným heslem, či si raději nastavují zapamatovatelná a tím také lehce uhodnutelná hesla. Své účty si bezpečnými hesly chrání 55% a zbylých 45% odpovědělo, že bezpečná hesla nepoužívá.

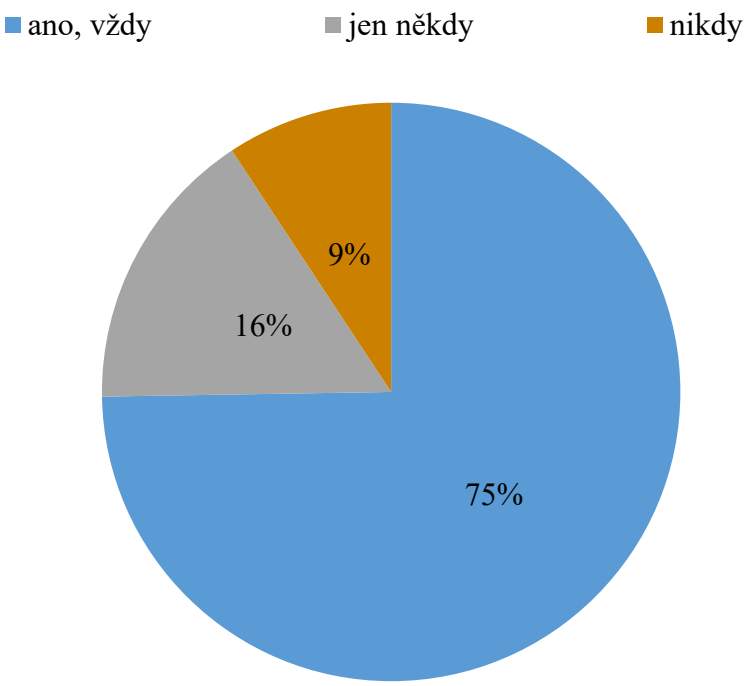
Graf č. 12: Přihlašujete se ke svým účtům (e-mail, internetové bankovnictví apod.) i na jiných počítačích, než na vlastním?



Zdroj: vlastní zpracování

42% respondentů se přihlašuje ke svým účtům i na jiných počítačích. V tomto případě je důležité, aby neukládali své údaje na cizích počítačích. To znamená, aby nezaškrtávali při přihlašování políčko “přihlásit se trvale”, „uložit údaje”, „zůstat přihlášený”, „pamatovat si mě” apod. Tato otázka úzce souvisí s otázkou následující, a to, zda se respondenti odhlašují ze svých účtů. V případě, že se ke svým účtům respondent přihlašuje i na jiném počítači, než vlastním, je také důležité nezapomenout se odhlásit. Uložení přihlašovacích údajů či neodhlášení by mohlo mít za následek zneužití daného účtu ve prospěch útočníka. Většina, 58%, se ke svým účtům na jiných počítačích nepřihlašuje.

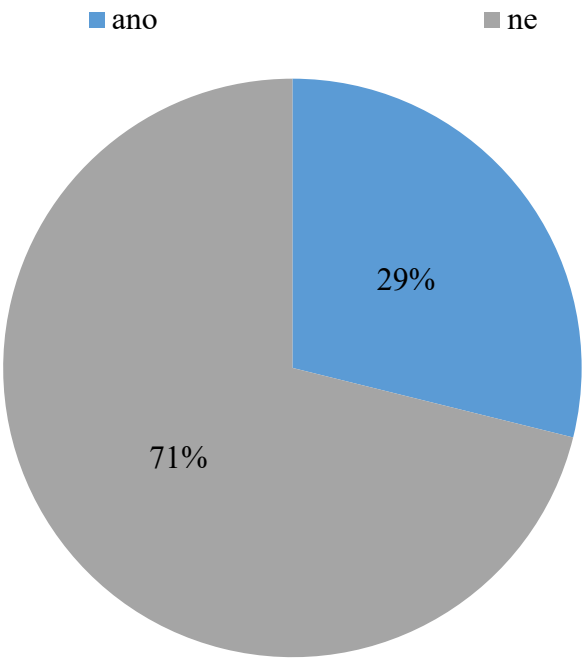
Graf č. 13: Odhlašujete se ze svých účtů?



Zdroj: vlastní zpracování

Otázka navazující na předchozí, v případě přihlašování i na jiných počítačích, než vlastních, je odhlašování nezbytné. Odhlašovat by se ale mělo i na vlastním počítači. V případě napadení by útočník mohl napadnout přihlášená okna. Bezpečné není ani ukládat své přihlašovací údaje a nechávat je počítačem vyplňovat automaticky. Některé systémy tak nabízí tzv. „klíčenky“, které jsou zabezpečeny heslem, kde se uloží a sdruží jakékoli přihlašovací údaje. 58% dotazovaných se odhlašuje vždy, 30% jen někdy a zbylých 12% se dle své odpovědi neodhlašuje nikdy.

Graf č. 14: Pracujete na počítači, který je připojen k veřejné Wi-Fi, s citlivými údaji, jako je např. internetové bankovnictví?



Zdroj: vlastní zpracování

29% dotazovaných se dobrovolně vystavuje riziku, že někdo zneužije jejich údajů. Není rozumné využívat veřejnou Wi-Fi, kdy spravovatelem může být kdokoli a může tak zneužít citlivých údajů. Pro pracování s citlivými, osobními údaji, jako je např. internetové bankovnictví by se měla využít síť, kterou uživatel zná či si je jist, že je bezpečná. Většina respondentů, 71%, se ke svým účtům na veřejné Wi-Fi síti nepřihlašuje.

10.3 Shrnutí výsledků dotazníkového šetření

Nejvíce odpovědí bylo získáno od respondentů ve věkové kategorii 51 a více let (59) se středoškolským vzděláním zakončeným maturitou (76) a nejvíce odpovídaly ženy (98).

Na otázku zda byl jejich počítač již někdy nakažený virem, jich 99 odpovědělo, že ano a všech 99 respondentů také odpovědělo, že stahuje z internetu hudbu, filmy aj. zadarmo. Je tak velice pravděpodobné, že si vir do svého počítače mohli stáhnout spolu se soubory.

81 respondentů se ke svým osobním účtům přihlašuje i na jiných počítačích, než na vlastním a pouze 32 z nich se ze svých účtů vždy odhlašuje. Ze zbylých 49 se jich 31 odhlašuje jen někdy a 18 z nich odpovědělo, že se neodhlašují vůbec a vystavují se tak riziku napadení jejich účtů.

Podle celkových výsledků vyplývajících z vyplněných dotazníků si respondenti z pohledu bezpečnostní gramotnosti nevedli špatně a dalo by se říci, že svými odpověďmi překvapili. Naprostá většina používá na svém počítači antivirový program (173), používá bezpečná hesla (161), ze svých osobních účtů se vždy odhlašuje (145) a také nepracuje s citlivými údaji na veřejné Wi-Fi (138). Nadpoloviční většina aktualizuje svůj operační systém vždy, když vyjde nová aktualizace (102) a přihlašuje se ke svým účtům pouze na vlastním počítači (113). Negativně z tohoto pohledu vyšla pouze otázka, zda respondenti stahují hudbu filmy aj. zadarmo, kdy takto odpovědělo více jak polovina (117).

10.4 Vyhodnocení hypotéz

H1: Uživatelé provádí základní operace k ochraně svého počítače. Pro tuto hypotézu byly stanoveny otázky „*Používáte na Vašem počítači antivirový program?"* a „*Jak často aktualizujete svůj operační systém?*" Tato hypotéza se potvrdila, neboť 89% dotazovaných antivirový program na svém počítači používá a 53% svůj operační systém pravidelně aktualizuje spolu s novou verzí.

H2: Uživatelé, přesto, že si uvědomují hrozbu počítačové kriminality se nechovají v kyberprostoru obezřetně. Otázky pro tuto hypotézu byly: „*Máte obavu, že byste se mohl/a stát obětí počítačové kriminality?*", „*Stahujete z internetu filmy, hudbu aj. zadarmo?*" a „*Byl někdy Váš počítač nakažen virem?*" Tato hypotéza se taktéž potvrdila, 56% dotazovaných má obavu, že by se mohli stát obětí počítačové kriminality, 60% stahuje filmy, hudbu aj. zadarmo a 51% již někdy mělo ve svém počítači vir.

H3: Uživatelé nenakládají se svými osobními údaji bezpečně. Otázky pro tuto hypotézu byly „*Používáte bezpečná hesla? (více než 8 znaků, kombinace malých a velkých písmen, čísla…)*“, „*Přihlašujete se ke svým účtům (e-mail, internetové bankovnictví apod.) i na jiných počítačích, než na vlastním?*“, dále *„Odhlašujete se ze svých účtů?*“ a „*Pracujete na počítači, který je připojen k veřejné Wi-Fi, s citlivými údaji, jako je např. internetové bankovnictví?*“ Tato hypotéza se nepotvrdila. Bezpečná hesla používá 83%, ke svým účtům se 58% přihlašuje pouze na svém počítači, 75% se z těchto účtů poctivě odhlašuje a s citlivými údaji na veřejné Wi-Fi nepracuje 71%.

Závěr

Cílem práce bylo analyzovat stav bezpečnostní gramotnosti zkoumaného vzorku prostřednictvím dotazníkového šetření a stanovených hypotéz. Tento cíl byl naplněn a zhodnocen v praktické části. Vedlejším cílem bylo objasnit pojmy týkající se počítačové kriminality, ten byl naplněn v teoretické části.

Z práce lze vyvodit některé možné příčiny počítačové kriminality. Jednou z hlavních příčin je sám uživatel počítače. Svým chováním v kyberprostoru či na internetu a zacházením s citlivými daty může z větší části ovlivnit, zda se stane její obětí, či nikoliv. Z tohoto důvodu je nutné podotknout, že prevence a osvěta formou šíření do povědomí společnosti o počítačové trestné činnosti je nezanedbatelná. Prevence zejména formou vzdělávání se či zabezpečení svého počítače (viz některé příklady v kapitole 7).

Další příčinou je kyberprostor, jeho neomezenost a to, že nikdy nebude stoprocentně zajištěn. Útočník se v prostředí kyberprostoru může neomezeně pohybovat, měnit svou polohu či obměňovat svou identitu.

Jednou z příčin může být také msta bývalému zaměstnavateli či vidina snadného zisku.

Další možnou příčinou může být fakt, že než vývojáři vytvoří ochranu proti jedné formě počítačové trestné činnosti, vznikne mezitím další. Útočníkům se tak daří vytvářet stále nové formy počítačové trestné činnosti, ať už z existujících forem, tak úplně nové.

Další příčinou, navazující na předchozí, může být ta, že určitá část uživatelů útok ani neohlásí, čímž zůstane útok utajen a nevytvoří se tak ochranné opatření anebo zůstane útočník nepotrestán.

Nicméně žádným ochranným opatřením nelze počítačové kriminalitě stoprocentně zabránit, lze jimi pouze snížit pravděpodobnost možných hrozeb a rizik či počet útoků anebo minimalizovat ztráty.

Seznam použitých zdrojů

Literární zdroje

1. BÍMOVÁ, Alena. *Počítačová kriminalita a naše doba.* Praha: IDG Czechoslovakia, 1990. 137 s. ISBN 80-900872-2-1.
2. GŘIVNA, Tomáš, POLČÁK, Radim, ed. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
3. JIRÁSEK, Petr, NOVÁK, Luděk, POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. 200 s. ISBN 978-80-7251-436-6.
4. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 284 s. ISBN 978-80-247-1561-2.
5. KLIMEK, Libor, ZÁHORA, Jozef, HOLCR, Květoň. *Počítačová kriminalita v európskych súvislostiach.* Bratislava: Wolters Kluwer, 2016. 444 s. ISBN 978-80-8168-538-5.
6. KOHOUT, Roman, KARCHŇÁK, Radek. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. 68 s. ISBN 978-80-260-9543-9.
7. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. 522 s. ISBN 978-80-88168-15-7.
8. KOSTRECOVÁ, Eva, JÓKAY, Matúš, KOSTREC, Matej. *Počítačová kriminalita*. Bratislava: Nakladateľstvo STU, 2010. Edícia příručiek. 109 s. ISBN 978-80-227-3410-3.
9. KRČMÁŘ, Petr. *Linux: postavte si počítačovou síť*. Praha: Grada, 2008. Průvodce (Grada). 184 s. ISBN 978-80-247-1290-1.
10. *Kriminológia ako súčasť trestnej politiky: pocta prof. PhDr. Květoňovi Holcrovi, DrSc. k 80. narodeninám.* Praha: Leges, 2018. Teoretik. 324 s. ISBN 978-80-7502-279-0.
11. MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002. 106 s. ISBN 80-7226-419-2.
12. MCCARTHY, Linda, WELDON-SIVIY, Denise, ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, [2013]. 316 s. ISBN 978-80-904248-6-9.
13. PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014. Tajemství (Dialog). 248 s. ISBN 978-80-7424-066-9.

14. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). 309 s. ISBN 80-86898-38-5.
15. SKLENÁK, Vilém. *Data, informace, znalosti a Internet*. Praha: C.H. Beck, 2001. C.H. Beck pro praxi. 507 s. ISBN 80-7179-409-0.
16. SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. 640 s. ISBN 978-80-7380-501-2.
17. ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). 148 s. ISBN 978-80-7552-758-5.

Elektronické zdroje

1. BASTL, M., GRUBEROVÁ, Z. *Kyberprostor jako „pátá doména"?* [online]. 2013 [cit. 2019-03-20]. Dostupné z WWW: <http://vojenskerozhledy.cz/kategorie/kyberprostor-jako-pata-domena>.
2. POŽÁR, J. *Vybrané hrozby informační bezpečnosti organizace.* [online]. Praha : Fakulta bezpečnostního managementu PA ČR v Praze. [cit. 2019-02-25]. Dostupné z WWW: <https://www.cybersecurity.cz/data/pozar2.pdf>.
3. *Our mission* [online]. [cit. 2019-03-20]. Dostupné z WWW: <http://www.oecd.org/about/>.
4. *Evropská unie.* [online]. [cit. 2019-03-20]. Dostupné z WWW: <https://www.mvcr.cz/clanek/mezinarodni-organizace-a-vs-evropska-unie.aspx>.
5. *Sdělení komise evropskému parlamentu a radě.* Brusel : Evropská komise, 2017 [cit. 2019-03-20]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52017DC0476>.
6. *Rada Evropy (RE), anglicky Council of Europe (CoE).* [online]. 2015 [cit. 2019-03-20]. Dostupné z WWW: <http://www.radaevropy.cz>.
7. *Octopus Cybercrime Community*. [online]. [cit. 2019-04-05]. Dostupné z WWW: <https://www.coe.int/en/web/octopus/home>.
8. *Cíle organizace.* [online]. Praha [cit. 2019-03-20]. Dostupné z WWW: <https://www.osn.cz/osn/cil/>.
9. *Internet.* [online]. 2019 [cit. 2019-04-15]. Dostupné z WWW: <http://www.statistiky.wz.cz/?pg=internet>.

Seznam zkratek

aj. – a jiné

apod. – a podobně

atd. – a tak dále

CD – Compact Disc

DDoS – Distributed Denial of Service

DVD – Digital Versatile Disc

EU – Evropská unie

IT – informační technologie

ITU (International Telecommunication Union) - Mezinárodní telekomunikační unie

např. - například

OECD (Organisation for Economic Co-Operation and Development) – Organizace pro hospodářskou spolupráci a rozvoj
OSN – Organizace spojených národů

PDF – portable document format

SMS – Short Message Service

tj. – to jest

TZ – trestní zákoník

tzv. - takzvaný

Seznam tabulek a grafů

Přílohy

Příloha 1: Dotazníkové šetření

Vážení respondenti,

ráda bych Vás požádala o vyplnění dotazníku, který je součástí mé bakalářské práce na téma „Počítačová kriminalita a její příčiny".

Dotazník je zcela anonymní a výsledky budou využity pouze pro účely mé bakalářské práce.

Děkuji za Vaši ochotu a čas.

1. Pohlaví?
    - Muž
    - Žena

2. Jaký je Váš věk?
    - 15 – 18
    - 19 – 25
    - 26 – 35
    - 36 – 50
    - 51 a více

3. Jaké je Vaše nejvyšší dosažené vzdělání?
    - Základní škola
    - Střední škola bez maturity
    - Střední škola s maturitou
    - Vyšší odborné
    - Vysokoškolské

4. Jak často trávíte na počítači svůj čas?
    - Zřídkakdy
    - Jednou týdně
    - Několikrát týdně
    - Každý den

5. Jaká je Vaše schopnost pracovat na počítači?
    - Začátečník
    - Pokročilý
    - Zkušený

6. Používáte na Vašem počítači antivirový program?
    - Ano
    - Ne

7. Jak často aktualizujete svůj počítačový systém?
    - Vždy, když vyjde nová aktualizace
    - Jednou za čas
    - Neaktualizuji

8. Mátě obavu, že byste se mohl/a stát obětí počítačové kriminality?
    - Ano
    - Ne

9. Byl někdy Váš počítač nakažen virem?
    - Ano
    - Ne

10. Stahujete z internetu filmy, hudbu aj. zadarmo?
    - Ano
    - Ne, kupuji originál
    - Nestahuji vůbec

11. Používáte bezpečná hesla? (více než 8 znaků, kombinace malých a velkých písmen, čísla…)
    - Ano
    - Ne

12. Přihlašujete se ke svým účtům (e-mail, internetové bankovnictví apod.) i na jiných počítačích než na vlastním?
    - Ano
    - Ne

13. Odhlašujete se ze svých účtů?
    - Ano
    - Ne

14. Pracujete na počítači, který je připojen k veřejné Wi-Fi, s citlivými údaji, jako je např. internetové bankovnictví?
    - Ano
    - Ne