Vyšetřování počítačové kriminality

Lukáš Keňo

Bakalářská práce

2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš Keňo**
Osobní číslo:	**A13035**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Vyšetřování počítačové kriminality**
Téma anglicky:	**Cybercrimes Investigation**

Zásady pro vypracování:

1. **Definujte pojem pořítačová kriminality.**
2. **Rozdělte tento druh kriminality na jednotlivá odvětví.**
3. **Uveďte modelový protiprávní čin a popište způsob jeho spáchání.**
4. **Popište úskalí a výhody současné doby ve vztahu k počítačové kriminalitě.**
5. **Zvýrazněte nejčastější skupiny pachatelů a virtuální místo činu.**
6. **Rozveďte právní aspekty vyšetřování.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **PORADA, V. a kol. : Kriminalistika, nakl. CERM Brno 2001 ISBN 80-7204-194-0.**
2. **MUSIL, J., KONRÁD, Z., SUCHÁNEK, J. : Kriminalistika, 2. přeprac. vydání Praha C.H.Beck, 2004 ISBN 80-7179-878-9.**
3. **PORADA, V. : Teorie kriminalistických stop a identifikace Praha, Academia 1987.**
4. **NĚMEC, M. : Kriminalistická taktika pro policisty, Praha, Eurounion 2004, ISBN 80-7317-036-15.**
5. **KAŠPAR, K., : Kriminalistika (online), Dostupný z www: http://www.vsrr.cz/kriminalistika1.pdf**

Vedoucí bakalářské práce: **JUDr. Vladislav Štefka**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **23. února 2016**

Termín odevzdání bakalářské práce: **30. května 2016**

Ve Zlíně dne 16. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ Fakulta aplikované informatiky L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 27.5.2016

.....
podpis diplomanta

ABSTRAKT

Cílem bakalářské práce je seznámit s problematikou počítačové kriminality a základními pojmy související s ní včetně příslušných postihů za tuto činnost podle nového trestního zákoníku. Snaha bakalářské práce byla především přiblížit čitatelům hrozby dnešní doby a vývoj tohoto odvětví. Teoretická část je zaměřená hlavně na konkrétní pojmy a právní aspekty vyšetřování. V praktická část je potom zaměřená na konkrétní postup vyšetřování, včetně důkazů a výslechu, dále pak případy za uplynulý rok a struktura této kriminality v grafech.

Klíčová slova: počítačová kriminalita, kyberzločin, trestná činnost,

ABSTRACT

Bachelor's thesis is focused on problems connected with computer crime, basic words including their appropriate legal sanctions according to the new criminal code. Bachelor's thesis wants to approach readers to the threats of nowadays and their development. Theory part is focused mainly on specific terms connected with cybercrime and legal aspects. Practical part is focused on specific steps of investigating cybercrime and interrogation. Then cases in the previous year with graphs of computer crime's structure.

Keywords: computer crime, cybercrime, criminal activity

Tímto chci poděkovat svému vedoucímu bakalářské práce, JUDr. Vladislavu Štefkovi za odborné vedení, poskytnuté konzultace, cenné informace, rady a podnětné připomínky k této práci. Dále chci poděkovat svým rodičům a blízkým za podporu, které se mi dostávalo během celého studia.

OBSAH

Úvod **10**

TEORETICKÁ ČÁST **11**

1 počítač **12**

2 Počítačová kriminalita **13**

3 Historie počítačové kriminality **14**

3.1 60. léta **14**

3.2 70. léta **14**

3.3 80. léta **14**

3.4 90. léta **15**

3.5 21. století **15**

4 Rozdělení počítačové kriminality **16**

4.1 Trestná činnost s využitím počítače **16**

4.1.1 Phishing 16

4.1.2 Pharming 17

4.1.3 Hoax 18

4.1.4 Násilné projevy, nenávist a rasismus 19

4.1.5 Sdílení souborů a pirátství 19

4.1.6 Padělání a falšování 20

4.1.7 Krádež identity a narušení soukromí 21

4.1.8 Dětská pornografie 21

4.2 Trestná činnost proti počítači **22**

4.2.1 Odcizení výpočetní techniky 22

4.2.2 Hacking 22

4.2.3 Spam 23

4.2.4 Počítačové viry 24

5 Modelový protiprávní čin § 230 TZ **25**

5.1 Plánování a útok **25**

5.2 Způsoby páchání **25**

5.2.1 Sociální inženýrství 25

5.2.2 Fyzický přístup 26

5.2.3 Udělení přístupu (privilegií) 26
5.2.4 Trojský kůň 27
5.2.5 Muž uprostřed (Man in the middle) 27
5.2.6 Útok hrubou silou 27

6 Úskalí a výhody dnešní doby 28
6.1 Příležitosti 28
6.2 Obecné problémy 28
6.2.1 Spoleh na informační a komunikační technologie 28
6.2.2 Množství uživatelů 29
6.2.3 Dostupnost zařízení 29
6.2.4 Dostupnost informací 30
6.2.5 Nezávislost lokace a spáchání zločinu 30
6.2.6 Automatizace 31
6.2.7 Rychlost přenosu dat 31
6.2.8 Rychlost vývoje 31
6.2.9 Anonymita 32
6.2.10 Selhání tradičních vyšetřovacích metod 32
6.2.11 Šifrovací technologie 33

7 Nejčastější skupiny pachatelů 34
7.1 Skript kiddies/kiddiots 34
7.2 Příležitostný hacker 34
7.3 Profesionální hacker 34
7.4 Organizované skupiny pachatelů 34
7.4.1 Anonymous 34

8 Počítačová kriminalita ve virtuálním světě 35
8.1 Virtuální krádež 36
8.2 Virtuální znásilnění 37
8.3 Virtuální vražda 37

9 právní aspekty vyšetřování 38

Praktická část 40

10 Vyšetřování počítačové kriminality 41
10.1 Ohlášení činu 41

10.2 Přístup k situaci 42
10.3 Počátek šetření 42
10.3.1 Praktický případ 1 42
10.4 Identifikace možných důkazů 44
10.4.1 Fyzické důkazy 44
10.4.2 Digitální důkazy 45
10.5 Výslech 46
10.6 Obvinění a tresty - shrnutí 46
11 Největší případy v roce 2015 48
11.1 Leden 48
11.2 Únor 49
11.3 Březen 49
11.4 Duben 50
11.5 Květen 51
11.6 Červen 51
11.7 Červenec 52
11.8 Srpen 52
11.9 Září 53
11.10 Říjen 54
11.11 Listopad 54
11.12 Prosinec 55
12 Statistiky počítačové kriminality 56
12.1 Struktura počítačové kriminality v ČR v roce 2015 56
12.2 Počet počítačových zločinů za poslední roky v ČR 57
12.3 Nejčastější útoky počítačové kriminality 58
13 Závěr 59
Seznam použité literatury 60
Seznam použitých symbolů a zkratek 64
Seznam obrázků 65
Seznam tabulek A grafů 66

ÚVOD

Bakalářská práce upozorňuje a seznamuje s problémem počítačové kriminality, její masivní rozvoj a aktuální problém. V práci najdeme nejznámější pojmy v souvislosti s touto problematikou a také reálné případy.

Počítačová kriminalita je novým fenoménem, který přinesl až rozvoj informačních technologií. Počítače a internet se staly za poslední desetiletí prakticky nedílnou součástí našich životů a to ve všech směrech ať už je to práce, soukromý život, služby nebo společenské vztahy. Tato „závislost“ na technologiích otevírá zločincům vrátka pro páchání nových, dříve nepoznaných zločinů.

Pachatel za využití téměř bezmezné anonymity, kterou internet nabízí napadne oběť, která se může nacházet naprosto na jiném kontinentu. Vyšetřování takového zločinu je potom mnohdy až nemožné a je zapotřebí mezinárodní spolupráce.

Počítačová kriminalita může postihnout osobní i společenský život. Pachatelům nejde vždy jenom o finance, ale i cenné dokumenty, osobní údaje nebo uspokojení sebe samého.

Orgány činné v tomto trestním řízení musely zavést nové metody vyšetřování, protože běžné metody selhávají. Rapidní rozvoj také přináší nevýhodu, že prakticky každým dnem vznikají nové technologie a vyšetřovatelé tak musí být neustále na pozoru a být na ně připraveni ať už se jedná o zavedení nové legislativy nebo nových vyšetřovacích prostředků.

V teoretické části je krátce shrnuta historie počítačové kriminality, definované hlavní pojmy týkající se týkající se tohoto problému včetně jejich rozdělení do kategorií, dále potom rozvinuty typické způsoby páchání zločinu trestného podle §230 TZ. Nedílnou součástí je také zaměřené se na výhody a problémy dnešní doby ve vztahu k počítačové kriminalitě. Na konci se zaměříme na právní aspekty při vyšetřování zločinu.

Praktická část je krátce zaměřena na konkrétní postup vyšetření včetně nejvíce významných reálných případů v roce 2015. Dále pak statistika této kriminality včetně struktury a nejčastějších protiprávních činností v grafech.

I. TEORETICKÁ ČÁST

1 POČÍTAČ

"Zařízení nebo stroj na realizaci výpočtů nebo řízení operací vyjádřitelných číselnými nebo logickými výrazy." [1] Počítače se skládají z komponentů, které vykonávají částkové, dobře definované funkce. Komplexní vztahy mezi takovými funkcemi dávají počítačům schopnost zpracovávat informace. Pokud je správně nakonfigurovaný, většinou programováním, je možné počítač použít na reprezentaci aspektu problému nebo části systému. Počítač se řadí do kategorie výpočetní techniky, která patří k nejnovějším informačním a komunikačním technologiím. [2]

V souvislosti s počítačem se taky vážou dva pojmy – software a hardware. Software znamená programové vybavení počítače, zajišťující jak samostatný běh systému, tak podpůrné vývojové programy. Hardware je opozitum softwaru a znamená fyzickou součást počítače, hmatatelnou a z větší části jsou to součástky počítače nezbytně nutné k fungování.

Dnešní doba, kdy počítač už neznamená jenom obrovský stroj rozměrově roven menší místnosti. Pokrok, který dostal počítače na stoly našich obývacích pokojů a počítače se staly osobními (PC – personal computer, osobní počítač). Internet, který propojil naše životy a přinesl svět blíže každému uživateli nemusí být nutně velkou výhodou. Žijeme v době, ve které tvoříme a budujeme naše životy kolem drátových a bezdrátových sítí. V dnešní době je výpočetní technika začleněna do všech sfér naší společnosti. Stále vzrůstající číslo lidí, kteří objevují jeho rychlost a pohodlí, kterou nabízí. Nové trendy vznikají dnes a denně. Objevuje se však i negativní stránka spojená s širokým užitím počítačů - počítačová kriminalita. [3]

2 POČÍTAČOVÁ KRIMINALITA

Trestný čin při kterém je hlavním aktérem počítač a internet. Počítačová kriminalita, též kybernetická kriminalita nebo kyberzločin, je označení ilegálního jednání za využití výhod, které nabízí počítačová síť. Počítač může být použit ke spáchání zločinu jako jsou podvody, obchody s dětskou pornografií a duševním vlastnictví, krádež identity a nebo také počítač může být cílem.

Více a více zločinců objevuje jeho anonymitu, která nezná prakticky žádnou hranici. V minulosti byla počítačová kriminalita páchána pouze jednotlivci nebo skupinami, dnes již můžeme vidět vysoce komplexní zločinecké sítě s cílem poškodit oběť za co nejkratší čas a vytěžit co nejvyšší zisk. Nelegální páchání, kde nemusí být cílem pouze jednotlivec, ale také celý stát. Díky brzkému rozšíření počítačů a Internetu v USA byla většina pachatelů a obětí Američani. Od 21. století však nezůstala žádná vesnička bez dotyku aspoň nějakého druhu kyberzločinu. [4]

Počítačová kriminalita je momentálně největší hrozbou, která kdy byla díky množství lidí a zařízení připojených k internetu. Nucené potlačování tohoto zločinu má za následek spíše rozvoj. Počítač v podstatě neumožní a není konstruován k páchání tohoto protiprávního činu, avšak díky dostupným technologiím, které nabízí, jej může pachatel využít k sabotáži, krádeži, stalkingu nebo zneužití. Všechny tyto aktivity existovali již před tímto fenoménem, avšak počítač a internet přispěl k rozšíření kriminálního jednání včetně nových prvků. [6]

Většina útoků počítačové kriminality je na jednotlivce, korporace nebo na vládu. Ačkoli útoky neproběhnout na fyzickém těle, ale na virtuálním těle společnosti, což je sada informačních atributů, které definují lidi a firmy. Jinými slovy, v digitálním světě, je naše virtuální identita základním prvkem našeho života - jsme svazek čísel a identifikátorů v několika počítačových databázích, které vlastní korporace nebo vláda.

Důležitým aspektem počítačové kriminality je její nelokální charakter: místo a čin se může lišit. To představuje vážný problém při vymáhání práv, protože je zapotřebí mezinárodní spolupráce. Například pokud osoba přistupuje k dětské pornografii umístěné na počítači v zemi, kde tento čin zakázaný není, avšak přistupoval k těmto materiálům v zemi, kde je to nezákonné, těžko se posuzuje místo činu. [5]

3 HISTORIE POČÍTAČOVÉ KRIMINALITY

Zločinné zneužívání informačních technologií a nezbytné právní aspekty jsou diskutovány již od samotného zavedení těchto technologií. V průběhu posledních 50 let, byla různá řešení realizována na národní a regionální úrovni. Jedním z důvodů, proč toto téma zůstává problematické je neustálý technický vývoj, stejně jako měnící se metody a způsoby páchání zločinu. [6]

3.1 60. léta

V 60. letech 20. století byly zavedeny počítačové systémy na bázi transistoru, které byly menší a levnější než než stroje na bázi vakuové trubice. Toto vedlo ke zvýšení využívání počítačových technologií. V této počáteční fázi se zločiny spíše zaměřovaly na fyzické poškozování počítačových systémů a uložených dat. Jeden takový větší incident byl v roce 1969, kdy student zapříčinil požár, který zničil počítačová data na univerzitní půdě.

3.2 70. léta

Počítačové systémy se rozvíjejí stále více. Na konci dekády je odhadovaný počet 100 000 sálových počítačů jenom ve Spojených státech. S poklesem cen jsou počítačové technologie využívány široce v administrativě a podnicích. 70. léta jsou charakterizována jako posun od tradičních majetkových trestních činů, která dominovala v 60. letech, k počítačovým. Zatímco fyzické poškozování proti počítačovým systémům pokračovalo, objevily se také nové formy zločinu. To zahrnovalo nezákonné používání počítačových systémů a manipulace s daty. Změna z manuálních transakcí na počítačově ovládané vedla k další nové trestné činnosti - počítačový podvod. Již v této době byly mnoha milionové ztráty a počítačový podvod byl velkou výzvou pro donucovací orgány, které dostávaly do rukou stále více a více případů. Aplikování stávajících legislativ bylo problematické, takže v různých částech světa byla zahájena debata na toto téma.

3.3 80. léta

V 80 letech se stávají osobní počítače populárnější. S tímto vývojem a zvýšeným počtem

počítačových systémů se také zvýšilo číslo potenciálních cílů pro zločince. Poprvé, cíle zahrnovaly širokou škálu kritických infrastruktur. Jedním z vedlejších účinků šíření počítačových systémů byl rostoucí zájem o software, což vedlo ke vzniku prvních forem softwarového pirátství a trestné činnosti vztahující se k patentům. Propojení počítačů přineslo nové typy zločinů. Sítě umožnily pachatelům vstoupit do počítačového systému, aniž by byl přítomen majitel. Kromě toho možnost distribuce softwaru prostřednictvím sítí umožnil pachatelům šíření škodlivého softwaru a objevovaly se i počítačové viry. Státy začaly proces aktualizací právních předpisů, tak aby splňovaly všechny rychle se měnící zločiny.

3.4 90. léta

Zavedení grafického rozhraní („WWW“) v 90. letech, který způsobil rapidní růst počtu uživatelů internetu. Informace legálně zpřístupněné v jedné zemi vedly k dispozici všem po celém světě a to i v zemích, kde publikování takových informací bylo trestáno. Dalším problémem jsou online služby, které se ukázaly obzvlášť náročné při vyšetřování přeshraničních trestných činu kvůli rychlosti výměně informací. Šíření dětské pornografie se přesunulo z fyzické výměny knih a pásek k online distribuci prostřednictvím webových stránek a internetových služeb. Zatímco počítačové zločiny byly obecně místního mínění, na internetu se obrátilo v mezinárodní trestnou činnost. Výsledkem se stalo to, že mezinárodní společenství začalo řešit problémy mnohem intenzivněji.

3.5 21. století

Stejně jako předchozí desetiletí, nové trendy v oblasti počítačové kriminality a počítačové trestné činnosti se nadále rozšiřují v 21. století. První desetiletí nového tisíciletí bylo ovládáno novými, vysoce sofistikovanými metodami páchání trestné činnosti jako je „phishing“. Vzrůstající využití technologií, které je mnohem obtížnější pro vymáhání práva při vyšetřování. Nejenom se změnily metody, ale také dopad. Pachatelé jsou schopni útok automatizovat a počet trestných činů vzrostl. Regionální a mezinárodní organizace dávají reakcím na počítačovou trestnou činnost vysokou prioritu.

4 ROZDĚLENÍ POČÍTAČOVÉ KRIMINALITY

Způsobů dělení počítačové kriminality najdeme v literatuře spousty avšak většinou jsou si velmi podobné. Podle prof. Porady lze z kriminalistického hlediska lze rozdělit trestnou činnost rozdělit do dvou skupin: [3]

1) Trestná činnost s využitím počítače
2) Trestná činnost proti počítači

4.1 Trestná činnost s využitím počítače

Jedná se o trestnou činnost, kde v hlavní roli může být výpočetní technika, která v rukou pachatele může být prostředkem k spáchání tohoto protiprávního činu. Jedná se například o padělání peněz, kdy pachatel využívá výpočetní techniky.

4.1.1 Phishing

Akt zasílání emailů uživatelům, klamně se prohlašující za legitimní společnost, za cílem podvést uživatele, aby zadali své soukromé informace, které budou použity ke krádeži identity. Phishing je odvozen od anglického slova “fishing”, tedy rybaření.

Phishingový email je podvod většinou obsahující odkaz, který směřuje uživatele k návštěvě webové stránky, kde jsou požádáni o aktualizaci svých osobních údajů, například hesel, čísel kreditních karet nebo čísla bankovních účtů. Webové stránky mohou vypadat věrohodně a mnohdy až k nerozeznání od pravých, ale s tím rozdílem, že falešné se pokouší ukrást veškeré vložené informace, které uživatel na stránce zadá.

Jedním z takových větších případů phishingu byl v roce 2003, kdy uživatelé obdrželi emaily údajně z eBay s tvrzením, že uživatelský účet bude pozastaven, pokud uživatel neklikne na webový odkaz v emailu a neaktualizuje informace o své kreditní kartě, které originální eBay měl. Vzhledem k tomu, že je poměrně jednoduché, aby webová stránka vypadala jako legitimní díky napodobení HTML kódu, mnoho lidí opravdu přesvědčilo o tom, že jej kontaktuje eBay a následně na svých stránkách aktualizovali informace.

Hlavní elementy v emailu, který obsahuje phishing:

1. Pole odesílatel se zdá být legitimní společnost, avšak je velmi důležité si uvědomit, že políčko odesílatel je možno snadno změnit v každém emailovém klientovi během několika sekund.
2. Email obvykle obsahuje loga nebo obrázky pravděpodobně zkopírované z webu společnosti na kterou se email odkazuje.
3. Email obsahuje klikající odkaz s textem, který navádí ke kliknutí a ověření in-formací. Tento odkaz však nevede na legitimní stránky odkazované společnosti.

Navíc si v emailu můžeme všimnout mnoha prvků, které jsou na první pohled pochybné. Například logo přesně neodpovídá logu společnosti, pravopisné chyby, procento přihlášení následované číslem, náhodné jména nebo emailové adresy v těle textu a nebo dokonce v hlavičce mailu, které nemají nic co do činění s uvedenou společností. [7]

Lidé, kteří stojí za těmito emaily rozesílají miliony takových podvodných mailů v naději, že se aspoň pár z nich nachytá a poskytne své osobní a finanční informace. Každý kdo je vlastníkem emailové adresy je v nebezpečí, že bude cílem phishingu. Každá emailová adresa, která byla zveřejněna na internetu (příspěvkem na fóru, v diskuzních skupinách nebo na jiných webech) je náchylnější na phishing, tato emailová adresa je snadno vyhledatelná útočníky. To je také důvod proč je phishing tak výhodný pro podvodníky - mohou snadno a levně přistupovat k milionům emailovým adresám, kde mohou tyto podvodné emaily zaslat.

4.1.2 Pharming

Podvodná praktika ve které je škodlivý software nainstalován do PC nebo serveru, který přesměrovává uživatele na podvodné weby bez jejich vědomí, či souhlasu. Pharming je nazývám jako “phishing bez návnady”. Pharming vznikl ze slova “farming”, tedy farmaření.

Při phishingu pachatel zasílá emaily, které vypadají legitimně a zdá se, že pocházejí z některého z nejpopulárnějších webových stránek ve snaze o získání osobních a finančních informací od příjemců těchto mailů. Při pharming může být napadeno větší množství uživatelů, protože není nutné, aby byl zaměřen na jedince jeden po druhém a není nutná žádná akce na straně oběti.

V jedné formě pharmingového útoku kód zaslaný emailem upraví lokální hosts soubory v PC. Hosts soubory převedou adresy URL do řetězců, které počítač používá k přístupu k webovým serverům. Počítač s napadenými soubory je přesměrován na podvodné webové stránky i přesto, že uživatel zadá správnou internetovou adresu nebo klikne na záložku.

Další a zvláště nebezpečnou formou je tak zvaná “otrava” doménových adres ve kterém je název domény v systémové tabulce na serveru upraven tak, že přesměrovává na podvodné webové stránky. Při této metodě nemusí být jednotlivé hosts soubory v počítači poškozeny. Místo toho problém dochází na DNS serverech, který se stará o tisíce nebo miliony požadavků uživatelů na URL. Oběť skočí na podvodnou stránku bez jakéhokoliv zbystření.

Poté co uživatel zadá na podvodnou stránku osobní informace jako jsou čísla kreditních karet, bankovních účtů nebo hesla, podvodníci mohou vesele ukrást vaši identitu. [8]

4.1.3 Hoax

Hoax je zkráceně poplašná, nepravdivá zpráva. Nejenom, že je matoucí, ale může být i potenciálně škodlivá. Falešné zprávy začaly jako e-maily a nápad byl stejný jako řetězové zprávy. V současné době jsou tyto zprávy nejvíce aktivní na sociálních sítích, jako je Facebook. Oproti emailům sociální sítě dopomáhají k mnohem rychlejšímu šíření. Hoax může poznat podle nejhlavnějších, které jsou pro tyto zprávy typické: [9]

- Úspěšný hoax se pokusí zaujmou pozornost, potom pohrozí nějakým nebezpečím a požádá nás o to, abychom s tím něco udělali. Hrozba může být zaměřena na osobu nebo počítač, popřípadě útočí na to, abychom se cítili špatně pokud tuto příležitost nevyužijeme.
- Vyřešení této hrozby vždy vyžaduje poslání dalším lidem.
- Specifický datum, kdy se něco stalo nebo kdy je potřebná akce proti tomu není většinou zmíněna.
- Zdroj této zprávy není nikdy zmíněn nebo pouze v nejasných zmínkách jako je „Adobe pracuje na řešení tohoto problému“ nebo „Fox News napsalo, že to bylo hrozné“

Další věcí, kterou můžeme udělat je zkopírovat a vložit důležitý odstavec zprávy do vyhledávače a ověřit tak pravdivost. Cílem hoaxů je pouze sranda a obelhání osob, ovšem pokud zpráva znepokojí větší počet lidí může se jednat o trestný čin šíření poplašné zprávy podle §357 TZ.

4.1.4 Násilné projevy, nenávist a rasismus

Radikálové používají masové komunikační systémy k šíření propagandy. Počet internetových stránek ukazujících rasistický obsah a nenávistné projevy vzrostl v posledních letech a to až o 25 procent meziročně.

Internet nabízí několik výhod pro pachatele jako jsou nižší náklady na distribuci a není potřeba žádného speciálního vybavení. Jako příklady podněcování nenávistí mohou být webové stránky, které obsahují pokyny pro vybudování bomb. Kromě propagandy používají internet také k prodeji určitého zboží jsou položky související s Nazi – vlajky, symboly, uniformy a podobně. Dále jsou to pak emaily a distribuování videoklipů skrze internetové služby jako je například Youtube.

Ne všechny země mají tuto činnost uznávanou jako trestní čin a v některých státech mohou být chráněny jako svoboda projevu. Názory se liší do jaké míry se dá svoboda projevu uplatnit. [10] V českém zákoníku se tím zabývá § 355 a 356 TZ.

4.1.5 Sdílení souborů a pirátství

Prodeje médií - CD jsou hlavním příjmem nahrávacích studií. Avšak pirátství, ilegální duplikace těchto materiálů chráněných autorským zákonem, byl vždy problémem, hlavně na východě. Množení nahrávek na universitách skrze levné počítače, které byly schopné této činnosti, zachytávání hudby z CD a dále sdílení přes vysokorychlostní připojení k Internetu se stala největší noční můrou nahrávacích společností. Při kopírování dochází k porušení autorských práv podle § 270 TZ.

Na začátku 21. století, vlastníci autorských práv, začali vycházet vstříc myšlence komerční digitální distribuce. Jako příklad lze uvést online prodej prostřednictvím iTunes Store (Apple inc.) a Amazon.com, kde byla k dispozici hudba, filmy a televizní pořady ke stažení. Navíc poskytovatelé několika kabelových a satelitních televizí, stejně jako elektronických herních systémů (Sony PlayStation a Microsoft Xbox) vyvinuli služby, které umožňují zákazníkům stahovat filmy a pořady pro okamžité sledování nebo pozdější znovu přehrání.[11]

obr. 1: Logo iTunes Store [49]

4.1.6 Padělání a falšování

Sdílení souborů duševního vlastnictví je pouze jedním aspektem problému s kopírováním. Dalším je možnost použití digitálních zařízení k vytvoření dokonalé kopie materiálových artefaktů jako jsou peníze. Tímto tradičním zločinem je padělání. Až do nedávné doby, vytvoření měny vyžadovalo značné množství dovedností a přístup k technologiím, které jednotlivci většinou nevlastnili, a tím jsou tiskařské lisy, gravírovací desky a speciální barvy. Nástupem levných, vysoce kvalitních barevných kopírek a tiskáren přineslo padělání pro masy. V roce 1997 inkoustové tiskárny produkovaly kolem 19 procent padělaných peněz. Držení obdobných padělatelských náčiní je trestáno dle §236 TZ. Kvůli rozsáhlému rozvoji a využití výpočetní techniky donutilo americké ministerstvo financí k změně designu papírové měny, tak aby zahrnovala celou řadu technologií proti padělání.

Měna Evropské unie, tedy euro, má tento bezpečnostní design navrhnut už od začátku. Zvláštnosti jako hologramové folie, speciální pásky a papír byly navrženy tak aby udělaly padělání, co nejvíce obtížné. Konkrétně jsou tyto prvky čtyři. Ve skutečnosti přechod na euro přitáhl ojedinělou příležitost pro padělatele již existující národní měny. Lidé neznali pravý design euro měny a vznikl strach lidí, že padělané eura budou smíchány s pravými. I přes obavy k tomu naštěstí nedošlo.

Měna není jenom jediným cílem kopírování. V dnešní době se také hodně rozmohlo kopírování a falšování imigračních dokumentů, které patří mezi nejcennější dokumenty a jsou také mnohem jednodušší ke kopírování. [12]

Trestní zákoník obsahuje ustanovení o padělání a pozměnění peněz v § 233 TZ, padělání a pozměňování známek v § 246 TZ, padělání a pozměnění předmětů k označení zboží pro daňové účely a předmětů dokazujících splnění poplatkové povinnosti v § 245 TZ a padělání a pozměnění veřejné listiny v § 348 TZ.

obr. 2: Bezpečnostní prvky Euro bankovky [50]

4.1.7 Krádež identity a narušení soukromí

Kyberzločin může postihnout člověka jak virtuálně, tak fyzicky. S krádeží identity se setkáváme už od samého počátku lidstva. V dnešní době se trochu změnila podoba a díky internetu se tento fenomén obohatil o další možnosti. Namísto pouze fyzického se vydávání za někoho jiného je možno i z hlediska virtuálního. Za citlivé osobní údaje se považuje kromě jména a příjmení také rodné číslo, bydliště, čísla kreditních karet a další jiných dokladů, které pachatel využije ke krádeži identity. Získá-li pachatel osobní údaje mohou vzniknout dva různé efekty:

Například mohou použít údaje k vytvoření obrovského dluhu vedoucí k obrovským ztrátám nebo mohou prodat informace jiným, kteří je použijí podobným způsobem. Typickým způsobem může být krádež občanského průkazu, kdy v dnešní době pouze na základě tohoto dokladu je možné vytvořit půjčku. Původní majitel může zůstat v nevědomosti až do doby, kdy ho banka nekontaktuje kvůli vysokému dluhu.

Zadruhé mohou použít údaje k vytvoření nové identity pro jiné osoby. Například pachatel může kontaktovat vydávající banku při krádeži kreditní karty, tuto krádež ohlásit telefonicky ve jménu původního majitele a požádat o změnu emailové adresy účtu. Dále pak pachatel může získat jméno a čísla z dalších dokumentů a vytvořit pro sebe tyto dokumenty nové, s údaji původního majitele, avšak použije svoji fotku. [13]

Z hlediska správního práva připadá v úvahu zákon č. 101/2000 Sb., o ochraně osobních údajů, který obsahuje i případné sankce za neoprávněné nakládání s osobními údaji. Podle trestního zákoníku je v § 180 TZ trestný čin neoprávněného nakládání s osobními údaji.

4.1.8 Dětská pornografie

S příchodem skoro všech nových mediálních technologií byla pornografie buď jejich "zabiják" nebo řídila celý počáteční rozvoj technických inovací s účelem hledání zisku.

Internet nebyl výjimkou, ale je tu i nelegální stránka věci - dětská pornografie, která nemá v souvislosti s legální pornografií zaměřenou na dospělé nic společného. Vlastnictví dětské pornografie, příkladem jsou obrázky dětí mladších 18 let při sexuálních aktech, je v Spojených Státech, Evropské Unii a mnoho dalších státech ilegální problémem, který do dnešní doby nemá žádné lehké řešení. Problém je šíření materiálu z oblastí jako jsou státy bývalého Sovětského svazu a Jihovýchodní Asie, které chybí zákony k počítačové kriminalitě. Právníci se domnívají, že dětská pornografie reprezentuje průmysl s obratem 90 miliard korun ročně s více než 10 tisíci internetovými lokacemi umožňujícími k nim přístup.

Internet také poskytuje pedofilům bezprecedentní příležitost spáchat kriminální akt skrze takzvané "chatovací místnosti", kde si najdou a navnadí oběť. Zde se virtuální a hmotné světy protínají mimořádně nebezpečným způsobem.
V mnoha zemích se státní orgány vydávají na chatech za děti, i přes rozšířené povědomí o této praxi mezi pedofily se i nadále snaží o udržení kontaktu s dětmi a trvají na setkání reálně, tedy mimo virtuální realitu. To, že takové setkání je vysoce riskantní a vede k okamžitému zatčení ale pedofily neodrazuje. [14] V trestním zákoníku najdeme ustanovení o dětské pornografii ve § 192 TZ.

4.2 Trestná činnost proti počítači

Přestupky v této kategorii jsou namířeny aspoň na jedno ze tří právních zásad - důvěrnost, integritu a dostupnost. Popřípadě zájmem pachatele je právě krádež této techniky či nosiče informací.

4.2.1 Odcizení výpočetní techniky

V souvislosti s počítačovou kriminalitou je tato kategorie jenom okrajová. Pokud se jedná o odcizení počítače, popřípadě souvisejícího hardwaru, můžeme tady hovořit o trestné činnosti dle § 205 TZ.

4.2.2 Hacking

Příběh hackování sahá do 50. let 20. století, kdy skupinka bláznů začala odnášet části světových telefonních sítí, vytvářet neoprávněné meziměstské hovory, zřizovat linky pro další telefonní nadšence. [14] v pozdních 70. letech, se začali tito lidé shromažďovat do organizovaných skupin, které povýšili od hackování obyčejných telefonních sítí k hackování korporátních a vládních počítačových sítí.

Ačkoli termín "hacker" předchází počítačům a byl používán již v polovině roku 1950 v souvislosti s fandy elektroniky, první záznam o použití v souvislosti s počítačovými programátory, kteří byli zběhlí v psaní nebo "hackování" počítačového kódu byl článek v roce 1963 ve studentských novinách na univerzitě *Massachusetts Institute of Technology* (MIT). Po prvních počítačových systémech, které byly propojeny s více uživateli telefonními linkami v raných 60. letech, hacker se odkazoval na jednotlivce, který získal neoprávněný přístup do počítačových sítí, buď z jiné počítačové sítě nebo přímo z počítače, který je právě volný a nesledovaný a použije jeho vlastní systém. Většina hackerů nebyli zločinci s cílem

vyhledávat vandalismus nebo nezákonně nabýt finanční odměny. Místo toho většina těchto lidí bylo mladých s velkou zvědavostí a hodně z nich se chtělo stát počítačovými architekty v oblasti bezpečnosti. Hackeři zejména začínali s vlámáním se do počítačových systému a potom chlubením se navzájem svými činy a pak sdílením ukradených dokumentů jako svých trofejí. Tyto činy nezůstávali jenom u vlámání se do počítačů, ale také převzetí kontroly nad korporátními a vládními počítačovými sítěmi. Podle nového trestního zákoníku je tento zločin trestán jako neoprávněný přístup k počítačového systému a nosiči informací dle §230 TZ.

Jedním takovým zločincem byl Kevin Mitnick, první hacker, který to dotáhl na list nejvíce hledaných americkým FBI. Kevin se údajně naboural do počítače Amerického letecké obrany - *North American Aerospace Defense Command* (NORAD) v roce 1981, když mu bylo pouhých 17 let, čin, který vnesl do popředí závažnost takové hrozby narušením bezpečnosti, který následně vedl k přepracování zákona ve Spojených státech ve spojitosti s počítačovou kriminalitou v roce 1984.

Rozsah hackerských zločinů je jedním z nejtěžších k posouzení, protože oběti nehlásí napadení hackerem - kvůli rozpačitosti nebo strachu z dalšího narušení bezpečnosti. Oficiální odhad je však ten, že hackování stojí světovou ekonomiku miliardu dolarů ročně. Útok hackera není vždycky jenom z "vnějšku", ale také přímo zaměstnanci v rámci korporace nebo vládní byrokracie s úmyslem pozměnit databázové systémy za cílem zisku nebo z politických důvodů. Největší ztráty jsou z chráněných informací, které jsou někdy původem vydírání majitele těchto informací, aby mu byla data vrácena. [15]

4.2.3 Spam

Email vyplodil jednu z nejznámějších forem kyberzločinu a tím je spam nebo také nevyžádané reklamy na výrobky a služby. Odborníci odhadují, že tento spam je více než 90 procent emailů kolujících na Internetu. Spam je zločin vůči všem uživatelům Internetu, protože zabírá jak místo, tak kapacity internetového providera a také je často urážlivý. Navzdory různým pokusům o vytvoření legislativy související s odstraněním tohoto problému, stále zůstává nejisté jak spam smazat aniž by byla porušena svoboda projevu v liberálním demokratickém zřízení. Na rozdíl od nevyžádané pošty, která něco stojí, spam je pro pachatele téměř zdarma a není rozdíl mezi odesláním deseti nebo milionu zpráv.

Jedním z nejtěžších problémů jak odstavit spammery (osoba odesílající tyto spamy) zahrnuje jak jejich, tak počítače jiných, nakažených viry a bezvědomky rozesílajících tyto spamy. Mnohdy se několik počítačů připojených k Internetu nakazí virem nebo trojským

koněm, který dává spammerovi tajnou kontrolu. Takové nakažené stroje zaplavují Internet spamy. Odborníci odhadují, že pouze v USA je 4-8 milionů nakažených počítačů odesílajících spamy a jsou původem téměř jedné třetiny této nevyžádané pošty. [16]

Email slouží také jako nástroj pro tradiční zločince a teroristy. Zatímco liberálové chválí využití kryptografie pro zajištění soukromí při komunikaci, zločinci a teroristé mohou také používat tyto kryptografické prostředky k skrytí svých plánů. Úředníci uvádějí, že některé teroristické skupiny vkládají instrukce a informace do obrázků přes proces známý jako steganografie. Sofistikovaná metoda, která skrývá informace před běžným pohledem na obrázek.

Steganografie - věda, která se zabývá ukrýváním zprávy. Cílem ukrytí zprávy je aby celá přenášená zpráva zůstala v tajnosti a nikdo o ní nevěděl, že je vůbec přenášena. Ukrytá zpráva nebudí pozornost, takže nemusí být ani šifrována. Pro větší bezpečí je možné ji zašifrovat za použití kryptografie. [17]

Kryptografie - nauka o utajování zprávy převodem do podoby nečitelné bez speciálních znalostí. Zpráva je zašifrována tak, aby jí rozuměl pouze příjemce a nikdo další.

4.2.4 Počítačové viry

Záměrné uvolňování škodlivých počítačových virů je další typ kyberzločinu. V listopadu roku 1988, student počítačové vědy jménem Robert Morris na Cornellské univerzitě v USA, uvolnil softwarového "červa" na Internet. Červ byl experimentem, počítačovým programem, který měl za úkol replikovat sám sebe, využít chyb v některých emailových protokolech a rozeslat mezi lidi. Vzhledem k chybě v jeho programování, místo kopií sebe sama do ostatních počítačů, tento software stále dokola replikoval sebe na každém infikovaném systému dokud nezaplnil celou paměť počítače. Než byla nalezena "léčba" tohoto červa, stihl prolézt do 6 000 počítačů (jedna desetina internetu v té době). Náklady na nalezení léčby stály ekonomiku několik milionu dolarů. Morrisův otec byl hlavou počítačové bezpečnosti pro USA v tisku uvedl, že tato hrozba je spíše high-tech, čili vzácnost než předzvěst příchodu obdobných věcí v budoucnu. Mýlil se a od té doby začali přicházet další a další z různorodých oblastí jako jsou Filipíny, Pákistán nebo Bulharsko. [18]

Hodně počítačů zastaví viry ještě před jeho zaútočením, avšak nové, doposud neznámé typy se objevují stále na které není počítač připravený. Počítačový virus může poškodit nebo smazat data v počítači, použít email k dalšímu rozšíření nebo smazat všechno na disku. [19]

Tato protiprávní činnost je trestána dle §232 TZ.

5 MODELOVÝ PROTIPRÁVNÍ ČIN § 230 TZ

V novém trestním zákoníku § 230 TZ v přesném znění „Neoprávněný přístup k počítačovému systému a nosiči informací“ se zabývá nejčastěji páchaným počítačovým zločinem. Sem se řadí různé druhy hackingů, crackingů a dalšímu zneužití počítačových systémů. Nemusí dojít přímo ke krádeži ale už jenom samotný neoprávněný přístup je trestný – například prolomení hesla do systému. [20]

5.1 Plánování a útok

První věcí, kterou bude pachatel vyhledávat a zvažovat je oběť, tedy cíl útoku. To můžou být společnosti i individuální lidé. Avšak vždy je tu nějaký motiv uspokojení.

Typické příklady motivů pro útok:

- Peníze – finanční zisk
- Emoce – hněv, zlost, láska, teroristické hrozby, nespokojený zaměstnanec
- Sexuální impulz – pedofilové, násilníci, sexuální sadisti
- Politika/náboženství – názory, přesvědčení
- Pro zábavu – zvědavost, uspokojení

Po vytipování správného cíle je tu sbírání informací, zjišťování slabin. To vyžaduje rozsáhlé znalosti o systému. V další fázi je konečný útok. [21]

5.2 Způsoby páchání

Způsobů jak spáchat tento protiprávní čin je mnoho a další vznikají každým dnem avšak níže uvedené jsou pravděpodobně ty nejtypičtější pro daný čin. [22]

5.2.1 Sociální inženýrství

Zjednodušeně je to umění manipulovat s lidmi aby poskytli své důvěrné informace. Typy informací, které pachatelé potřebují se mohou lišit, ale při útoku na jedince se většinou snaží přimět k poskytnutí hesel, údajů o bankovnictví nebo přístup k počítači, kde nainstalují software, který jim poskytne další přístup a dá nad počítačem kontrolu k získání informací.

Pachatelé používají taktiku sociálních inženýrství, protože je to obvykle nejsnadnější způsob. Mnohem snadnější je přesvědčit někoho aby vydal své heslo než hackování hesla (tedy pokud heslo není velmi slabé).

Každý bezpečnostní odborník řekne, že nejslabším článkem v bezpečnosti je člověk. Nezáleží na tom kolik máte zámků. hlídacích psů, poplašných systémů, plotů a ostnatých drátů, pokud uvěříte, že osoba vydávající se za rozvoz pizzy a vy ho bez kontroly pustíte dovnitř, jsou vám zámky k ničemu.

5.2.2 Fyzický přístup

Při získání fyzického přístupu k počítači je snadné počítač hacknout. Pachatel může začít používat operační systém a získá přístup k datům. Fyzický přístup otevře pachateli obrovské možnosti hackování. Tento přístup umožňuje nainstalování různého typu softwaru, přečtení nešifrovaných dat na disku a podobně.

5.2.3 Udělení přístupu (privilegií)

Nezáleží na tom jak moc se bezpečnostní experti snaží ochránit systém před hackery, vždy si najdou cestu. Jedna taktika je použití neoprávněného přístupu do sítě známé jako udělování přístupu. Udělení přístupu dá hackerům privilegia, která normální uživatelé nemají. Typicky je to využití chyb nebo mezer v kódu nebo systému. Používají dva typy - horizontální a vertikální.

Oba spoléhají na aspekt počítačového programování známý jako privilegia. Privilegia jsou bezpečnostní funkce většiny programů a operačních systémů, omezují přístup uživatelů k souborům a kódům. Čím více privilegií uživatel má, tím více může měnit nebo komunikovat se systémem nebo aplikacemi.

Chceme-li zabránit neoprávněným uživatelům v přístupu k pokročilým operacím - jako změna kódu, mazání souborů nebo prohlížení citlivých dat - vývojáři obvykle využívají princip nejmenších privilegií. Jinými slovy, každý program a uživatel má nejmenší možní privilegia potřebné k provedení práce v rámci programu. Když hacker chce větší privilegia než typický uživatel musí najít způsob jak tento bezpečnostní prvek obejít.

Ve vertikálním útoku na přístup se útočník pohybuje nahoru na žebříčku privilegií, takříkajíc udělí si nejvyšší privilegia vyhrazena pro uživatele. Typický útok je takový, že se hacker přihlásí na uživatelský účet s nejnižšími, který má nejnižší privilegia a využití mezer v systému si privilegia zvýší a to mu následně umožní síťové aktivity, vytvoření nových uživatelů a podobně.

V horizontálním udělování přístupu je útočník obyčejný uživatel, který má přístup k ostatním běžným uživatelům. Jinými slovy, útočník nezíská žádné pokročilé privilegia,

prostě vezme identitu někoho jiného aby získal přístup. Například v případě, že se hacker přihlásí ke svému bankovnímu účtu a pak najde chybu v bankovní aplikaci, kterou je schopen získat přístup k účtu jiného uživatele se tímto dostal k horizontálnímu útoku. [23]

5.2.4 Trojský kůň

Trojan nebo trojský kůň je typ malwaru, který se často vydává za legitimní software. Trojani jsou využíváni hackery k získání přístupu k počítačovému systému. Uživatelé jsou obvykle obelhání nějakým typem sociálního inženýrství aby spustili trojského koně v jejich operačním systému. Díky spuštěnému trojanovi potom pachatel může získat přístup k citlivým datům a může s nimi dál nakládat - například: [24]

- Mazat data
- Blokovat data
- Modifikovat data
- Kopírovat data
- Narušit chod počítače a internetové sítě

5.2.5 Muž uprostřed (Man in the middle)

Útok proběhne tak, že se pachatel dostane mezi odesílatele a příjemce k získání informací a odposlouchává odesílané informace. V některých případech uživatelé mohou zasílat nešifrované data, které jsou pro muže uprostřed snadno získatelné. V dalších případech může pachatel získat zašifrované data, ale musí je první pomocí dešifrovacích metod dešifrovat a poté může přečíst. [25]

5.2.6 Útok hrubou silou

Nejjednodušší pokus o získání přístupu do systému. Útok hrubou silou se snaží přijít zkoušením na uživatelské jméno a heslo stále dokola dokud ho neuhodne. Tato metoda může být velmi jednoduchá při použití typických uživatelských jmen a hesel. [26]

6 ÚSKALÍ A VÝHODY DNEŠNÍ DOBY

Vývoj v oblasti informačních a komunikačních technologií nejenže vyústil v nové zločiny a nové kriminální metody, ale také nové metody vyšetřování počítačové trestné činnosti. Pokroky v informačních a komunikačních technologiích značně rozšířila schopnosti donucovacích orgánů. Pachatelé využívají nové nástroje k zabránění identifikace a brzdí vyšetřování.

6.1 Příležitosti

Donucovací orgány nyní mohou využívat narůstající výkon počítačových systémů a komplexní forenzní software k urychlení vyšetřování a automatizaci procedur.

Zatímco vyhledávání klíčového slova v ilegálním obsahu může být jednoduché, identifikace nelegálních obrázků už je problematičtější.

Forenzní software je schopen automaticky vyhledávat dětské pornografické obrázky porovnáváním souborů na pevném disku podezřelého s informací o známých obrázcích. Například na konci roku 2007 úřady našly řadu obrázků sexuálního zneužívání dětí. Aby se zabránilo identifikaci, pachatel digitálně upravil část snímků ukazující jeho tvář před publikováním snímků na internet. Počítačový forenzní experti byli schopni tyto modifikované snímky rozpoznat a zrekonstruovat obličej podezřelého. Ačkoli úspěšné vyšetřování jasně demonstruje potenciál počítačové forenzní analýzy, tento případ není žádným důkazem průlomu ve vyšetřování dětské pornografie. V případě, že by pachatel zakryl svou tvář prostou bílou skvrnou, identifikace by byla nemožná. [27]

6.2 Obecné problémy

6.2.1 Spoleh na informační a komunikační technologie

Veškeré každodenní komunikace jsou závislé na informačních a komunikačních technologiích a internetových službách. Tyto technologie jsou nyní odpovědné za kontrolní a řídící funkce v budovách, autech a službách letectva. Dodávky energie, vody a komunikační služby na nich závisí také. Další integrace informačních a komunikačních technologií budou s největší pravděpodobností pokračovat. Tato rostoucí závislost dělá systémy a služby náchylnější k útoku proti kritickým infrastrukturám. I krátká přerušení dopravy by mohla způsobit obrovské finanční škody.

Stávající technické infrastruktury mají řadu slabých míst jako je monokultura a homogenita operačních systémů. Mnoho soukromých uživatelů a malých, či středních podniků používá operační systém od Microsoftu a tak pachatelé mohou navrhnout efektivní útok soustřeďující se na jeden konkrétní systém. [28]

6.2.2 Množství uživatelů

Popularita internetu a jeho služeb rychle roste a nyní je více jak 2 miliardy uživatelů. Počítačových firem a poskytovatelů internetových služeb se zaměřením na rozvojové země mají největší potenciál pro růst. V roce 2005, počet uživatelů internetu v rozvojových zemích předčil číslo v průmyslových zemích. Vývoj levného hardwaru a bezdrátových přístupů umožní ještě více lidem přístup k internetu.

S rostoucím počtem lidí připojených k internetu vzrůstá také počet cílů a pachatelů. Je obtížné odhadnout kolik lidí používá internet k nelegální činnosti. Dokonce i když jen 0,1 procent uživatelů spáchá počítačový trestný čin bude více než milion pachatelů. Ačkoli míra využití internetu v rozvojových zemích je nižší, propagace kybernetické bezpečnosti není jednodušší, protože se pachatelé mohou dopustit trestného činu z jiné země. [29]

6.2.3 Dostupnost zařízení

Pouze základní vybavení je potřeba ke spáchání počítačové trestné činnosti - hardware, software a přístup k internetu.

S ohledem na hardware, výkon počítačů roste. Existuje celá řada iniciativ, které umožní lidem v rozvojových zemích aby využívali informační technologie více. Pachatelé se mohou dopustit závažného počítačového zločinu pouze s levnou bazarovou výpočetní technikou - znalost je důležitější než zařízení.

Posledním důležitým prvkem je přístup k internetu. Přestože náklady k přístupu na internet je ve většině rozvojových zemí vyšší než v průmyslově vyspělých není velkým problémem. Pachatelé se většinou nezaregistrují do internetové služby u kterých není potřebná identifikace. Typický případem může být hledání nezabezpečených bezdrátových sítí. [30]

Donucovací orgány podnikají kroky k omezení nekontrolovaného přístupu k internetové síti aby se zabránilo trestnímu zneužívání těchto služeb. Například v Itálii a Číně je k využívání veřejných internetových terminálů vyžadována identifikace. Existují však i odpůrci těchto identifikačních metod. Přestože omezení přístupu by mohlo předcházet trestné

činnosti a usnadnit vyšetřování donucovacích orgánů, mohla by tato právní úprava narušit další rozvoj informačních technologií.

Toto omezení přístupu k internetu by mohlo porušovat lidská práva, například Evropský soudní dvůr rozhodl v řadě případů, že právo na svobodu projevu se vztahuje nejen na obsah informací, ale také způsob jeho přenosu nebo příjmu. [31]

6.2.4 Dostupnost informací

Internet má miliony webových stránek. Každý, kdo publikuje nebo jen udržuje webovou stránku je zahrnut. Jedním z příkladů úspěchu je uživatelsky generovaná platforma Wikipedia, online encyklopedie, kde může každý přispívat.

Úspěch internetu závisí také na výkonných vyhledávacích nástrojích, které umožňují uživatelům prohledávání několika milionů webových stránek během pár vteřin. Tato technologie může být použita pro legitimní a kriminální účely. Například se pachatelé mohou zaměřit na hledání nezabezpečených systémů. Pachatel, který plánuje útok může také najít na internetu podrobné informace jak postavit bombu za pomoci pouze chemických látek, které jsou k dispozici v běžných supermarketech. I když takové informace byli k dispozici ještě před rozvojem internetu bylo mnohem těžší se k nim dostat.

Zločinci mohou také využít vyhledávač k analýze cílů. Příručka pro výcvik byla nalezena v průběhu vyšetřování proti členům teroristické skupiny a ukazuje tak, jak je užitečný internet pro šíření informací. Pomocí vyhledávačů mohou také pachatelé shromáždit veřejně dostupné informace (například plány ve veřejných budovách), které značně pomohou při jejich přípravě. [32]

6.2.5 Nezávislost lokace a spáchání zločinu

Pachatel nemusí být přítomen na stejném místě jako cíl. Umístění může být zcela odlišné od místa zločinu a mnoho útoků je nadnárodních. Zločinci se snaží vyhnout zemím se silnou legislativou pro počítačovou kriminalitu.

Prevence je jedním z klíčových výzev v boji proti kyberkriminalitě. Rozvojové země, které doposud nezavedly právní předpisy mohou být náchylné k zranitelné k útoku, protože si pachatelé mohou zvolit sami, kde si postaví svoji základnu. Závažné trestné činy mají vliv na oběti na celém světě a může být obtížné je zastavit vzhledem k nedostatečné legislativě v zemi, kde jsou umístěni pachatelé. To může vést k nátlaku, aby země přijala potřebné zákony. [33]

6.2.6 Automatizace

Jedna z největších výhod informačních a komunikačních technologií je schopnost automatizovat určité procesy. Automatizace má několik významných důsledků - zvyšuje rychlost procesů, jakož i rozsah a dopad procesů a nakonec omezuje počet zapojených lidí.

Automatizace snižuje potřebu na pracovní síly, což umožňuje poskytovatelům nabízet služby za nižší ceny. Pachatel lze pomocí automatizace zvýšit své aktivity - několik milionů nevyžádaných spamů. Zprávy mohou být rozesílány automaticky. Hacking útoky jsou často také automatizované s 80 miliony útoků každý den díky používání příslušného softwaru. Automatickým procesem může pachatel hodně získat když navrhne podvody, které jsou založeny na vysokém počtu útoků s relativně nízkou ztrátou pro každou oběť. Čím nižší je ztráta, tím vyšší je pravděpodobnost, že oběť nebude trestný čin hlásit. [34]

6.2.7 Rychlost přenosu dat

Přenos emailu mezi jednotlivými zeměmi trvá jen několik sekund. Tento krátký časový úsek je jedním z důvodů pro úspěch internetu, email odstranil potřebu fyzické přepravy zprávy. Nicméně tento rychlý přenos dává málo času donucovacím orgánům vyšetřit nebo nashromáždit důkazy. Tradiční vyšetřování tak trvá déle.

Jedním z příkladů je výměna dětské pornografie. V minulosti byly pornografické videa přepravovány ke kupci, což bylo možné snadno vyšetřit. Když pachatelé použijí internet filmy mohou být vyměněny během několika sekund.

Pro sledování a identifikaci podezřelého, potřebují vyšetřovatelé mít přístup k údajům, které mohou být odstraněny krátce po přenosu. Velmi krátká odezva vyšetřovacími orgány je často životně důležitý pro úspěšné vyšetřování. Bez odpovídajících právních předpisů a nástrojů, díky kterým mohou vyšetřovatelé reagovat okamžitě a zabránit odstranění dat, může být boj proti počítačové kriminalitě nemožný. [35]

6.2.8 Rychlost vývoje

Internet se neustále rozvíjí. Vytvoření grafického rozhraní www zaznamenal prudkou expanzi, protože předchozí služby založené na příkazech nebyly moc uživatelsky příjemné. Donucovací orgány se snaží udržet krok.

Online hry jsou stále více populární, ale doposud není jasné zda je možné úspěšně vyšetřovat a stíhat trestní činy v tomto virtuálním světě. [36]

Nové hardwarové zařízení se síťovou technologií se také vyvíjí. Nejnovější systémy umožní zapnout TV s přístupem k internetu. USB paměťová zařízení také zaznamenala pokroky a byly začleněny do hodinek, per a kapesních nožů. Donucovací orgány musí vzít v úvahu tento vývoj - nutno vzdělávat se v oblasti počítačové kriminality nepřetržitě.

Další výzvou je používání bezdrátových přístupových bodů. Rozšíření bezdrátového připojení k internetu v rozvojových zemích je příležitost, stejně jako problém. Pachatelé využívají bezdrátové přístupové body, které nevyžadují přihlášení a proto je náročnější dohledat pachatele.

6.2.9 Anonymita

Určování původu komunikace může být často velmi klíčovým prvkem ve vyšetřování. Nicméně, distribuovaná povaha sítě, jakož i dostupnost některých internetových služeb, které vytvářejí nejistotu původu, je obtížné identifikovat pachatele.

Příklady takových služeb, které mohou být i kombinované, jsou: [37]

- Veřejné internetové terminály (internetové kavárny, letiště..)
- Bezdrátové sítě
- Předplacené telefonní služby, které nevyžadují registraci
- Uložiště, které nevyžadují registraci
- Anonymní komunikační servery

Pachatelé mohou skrývat svou identitu například prostřednictvím falešné emailové adresy. Mnozí poskytovatelé nabízejí bezplatné emailové adresy. Tam, kde je třeba zadat osobní údaje, nemusí být ověřována jejich správnost, takže uživatelé mohou registrovat emailové adresy aniž by odhalili svoji identitu. Anonymní emailové adresy mohou být užitečné pokud se například uživatelé chtějí připojit k politické diskusní skupině bez identifikace. Anonymní komunikace může vést k antisociálnímu chování, ale může také umožnit uživatelům jednat volněji. [38]

6.2.10 Selhání tradičních vyšetřovacích metod

Vyšetřování a stíhání počítačové trestné činnosti vyžaduje specifické nástroje a prostředky, které umožní příslušným orgánům provádět vyšetřování. V této souvislosti nástroje k identifikaci pachatele a shromažďování důkazů potřebných pro trestní řízení je nezbytné. Tyto nástroje mohou být stejné jako ty, které se používají v tradičním teroristickém vyšetřování a

nesouvisí s výpočetní technikou. S rostoucím počtem případů souvisejících s internetem nejsou tradiční nástroje dostatečné. [39]

6.2.11 Šifrovací technologie

Dalším faktorem, který může komplikovat vyšetřování počítačové trestné činnosti je šifrovací technologie, která chrání informace před přístupem neoprávněných osob a je klíčovým technickým řešením v boji proti kyberkriminalitě. Šifrování je technika převedení obyčejného textu pomocí algoritmu. Stejně jako anonymita, šifrování není nic nového, ale výpočetní technika ho trochu pozměnila.

Všeobecná dostupnost snadno použitelných softwarových nástrojů a integrace šifrovacích technologií v provozních systémech nyní umožňuje šifrovat data z počítače pouhým kliknutím myši. Není ovšem jisté do jaké míry pachatelé používají šifrovací technologie k zamaskování jejich aktivit. Jeden průzkum o dětské pornografie poukazuje, že pouze 6 procent zatčených pachatelů dětské pornografie používalo šifrování, ale odborníci upozorňují na zvyšující se hrozbu.

Současný šifrovací software daleko přesahuje šifrování jednotlivých souborů. Nejnovější verze operačních systémů od Microsoftu umožňují například šifrovat celý pevný disk. Uživatelé mohou snadno instalovat šifrovací software. Ačkoli se někteří odborníci na forenzní analýzu domnívají, že je tato funkce nijak nebrzdí, může dostupnost této technologie vézt k širšímu využívání.

Techniky mohou být také kombinovány. Použitím softwarových nástrojů může pachatel šifrovat zprávu a převést ji do obrázku - technologie zvaná steganografie. Pro vyšetřovatele je obtížné rozpoznat jestli se jedná o fotky z dovolené nebo fotky, které v sobě skrývají šifrovanou zprávu. [40]

7 NEJČASTĚJŠÍ SKUPINY PACHATELŮ

Od nejméně znalých útočníku až po rozsáhlé organizace.

7.1 Skript kiddies/kiddiots

Také nazýván jako skiddie nebo bažant v hackování. V hackerském kultuře je to někdo, kdo používá software vytvořený někým jiným k útoku na počítačové systémy nebo sítě. Běžně jsou to pachatelé, kteří mají jenom velmi malé znalosti k napsání sofistikované programu ke spáchání zločinu. Jejich motivem bývá obvykle jenom ukázat se před kamarády a získat jejich ocenění. Termín nesouvisí s věkem, ale odvíjí se od znalostí v oblasti hackování. [41]

7.2 Příležitostný hacker

Sem se řadí také ti, kteří získali přístup k něčí práci nebo soukromým emailům, nebo našli cestu jak se dostat k účtům na sociálních sítích. Většina z nich to dělá ze srandy, nemluvíme tady o finančních ztrátách. Je to také hlavně zvědavost v soukromém životě někoho jiného a podobně. [42]

7.3 Profesionální hacker

Někdo, kdo žije počítačem, ví o nich vše a dokáže s nimi udělat cokoliv. Dokáží najít slabiny v systému i napsat vlastní program k útoku.

7.4 Organizované skupiny pachatelů

S růstem hackování se mnoho velkých hackerů spojilo a vytvořili alianci, která vzbuzuje pozornost celého světa. Velké organizované skupiny mají výhodu v páchání zločinů. Skupiny jsou schopny vybudovat velké komplexní systémy zaměřené na kradení peněz nebo citlivých dat. Spousta těchto skupin dosáhlo technického vybavení na úrovni národního. [43]

7.4.1 Anonymous

Populární organizace díky jejich mstivým útokům proti ISIS. Anonymous je otevřená skupina, která má působení všude ve světě. Jsou známi díky útokům na Pentagon, Visa, PayPal, MasterCard nebo shozením webů ISIS. Mnoho lidí ze zemí jako je Nizozemsko, USA, Velká Británie, Austrálie, Španělsko nebo Turecko bylo zatčeno kvůli údajnému působení v Anonymous. [44]

8 POČÍTAČOVÁ KRIMINALITA VE VIRTUÁLNÍM SVĚTĚ

Vývoj online počítačových her a interakce se rozrostl od internetového boomu v polovině devadesátých let. V dnešní době vytvoření online virtuálních světů vtahuje miliardy registrovaných uživatelů po celém světě všech věkových skupin a demografických údajů. Virtuální svět je prostě definován jako "trojrozměrné počítačové prostředí" ve kterém jsou uživatelé reprezentovaní na obrazovce jako oni sami a mohou komunikovat s ostatními v reálném čase.

Některé z nejpopulárnějších online relací jsou Second Life, World of Warcraft, Gaia online, Runescape a další. Pro lepší představu - Second Life umožňuje svým "obyvatelům" vytvořit plnou reprezentaci sebe sama a možnost komunikovat s dalšími miliony uživatelů, kterým pomáhají vytvářet nové položky a obsahy a v podstatě žít jiný život s neomezenými možnostmi. Kromě toho je možné nakupovat, prodávat kusy země, vytvářet vlastní položky, zakládat podniky a obchody s virtuální měnou, která může být převedena do skutečné měny a opačně. Prakticky anonymní povaha, virtuální trh a různé další prvky, které tvoří tyto digitální světy může vést ke všem druhům počítačové kriminality, včetně krádeží a podvodů.

Výskyt kyberkriminality týkajících se virtuálních světů se objevil již v roce 2003 a je považován za zvyšující se hrozbu v celém světě. Například v Jižní Koreji více něž polovina počítačových zločinů mělo něco dočinění s online hrami. Číslo momentálně není známo, avšak určitě je vysoké. Evropská Unie (EU) rovněž přijala oznámení a mnozí volají po nové legislativě k vypořádání se s krádeží a podvody ve virtuálních světech. Ve jedné zprávě bylo prohlášeno, že roční obrat virtuálních peněz obchodováním s virtuálním zboží se odhaduje na téměř 1,5 miliardy eur. Stejná zpráva také prohlašuje, že 70% uživatelů, kteří ztratili něco cenného jako důsledek trestné činnosti má velmi malou šanci na nápravu z důvodu obtížnosti sledování zdrojů a nedostatek právních předpisů týkajících se těchto aktů. Bohužel pachatelé jsou nepotrestáni.

Jedním z hlavních problémů, které obklopují problematiku podvodu, krádeže nebo jiných počítačových zločinů ve virtuálním světě je jejich význam. V závislosti a situaci snaha vysvětlit a přesvědčit policii a soudce, že skutečný zločin proběhl a zahrnuje předměty jako jsou zbraně z online hry, nehmotné zboží nebo "zlato" z virtuálního světa může být velmi obtížné. Online avatary, hry sociálních sítí, virtuální světy jako je Second life ještě nejsou znalostí většiny úředníků. Ti nemusí pochopit význam těchto položek pro některé lidi, kteří strávili týdny nebo možná měsíce získáváním těchto položek.

Situace se zhoršuje, když uživatel ve virtuálním světě nakupuje položky za reálnou

měnu. V případě některých virtuálních světů, uživatelé provozují legitimní podnikání, kde vytvářejí a budují jedinečný obsah a prodávají třetím osobám za účelem výdělku. Někteří tak mají značný vysoký zisk a považují ho za živobytí.

Je také dobře známo, že tito zločinci, kteří prodávají virtuální měnu za skutečné peníze využívají různé hackerské metody, podvody a další činy, které ve virtuálním světě objeví. Všechny jsou porušením smluvních podmínek a dohod téměř ve všech online hrách a virtuálních světech.

Je potřeba poznamenat, že mnoho hráčů nakupující virtuální předměty není starších osmnácti let a nemá přístup ke své vlastní kreditní kartě. Rodiče jim buď umožní používat své prostředky nebo peníze zasílají fyzicky poštou na vlastní pěst. Craig Sherman, ředitel společnosti Gaia Online řekl, že jejich společnost zaměstnává 3 lidi, kteří mají za úkol přebírat pouze klasickou poštu s penězi, kvůli velkému množství takových zásilek. [45]

8.1 Virtuální krádež

Jedná se v podstatě o klasickou krádež avšak zasazenou do virtuálního světa. Virtuální svět může vytvářet velkou ekonomiku s virtuální měnou a majetkem, který uživatelé získávají hraním mnohdy i několika stovek hodin. Těžko zločin proti tomuto majetku dokazovat avšak vysoké číslo jedinců se obrací na policii, protože cítí újmu způsobenou krádeží. S velkým rozvojem virtuálních světů a jejich obchodování vzniká potřeba regulace, který by se vztahovala na virtuální vlastnictví. Legislativní orgány začínají toto brát vážně avšak stále neexistuje žádné přesné vymezení.

Ve virtuálních světech vzniká silná ekonomika s velkými transakcemi a vždycky se naskytuje šance, že se druhá strana zachová nečestně. Transakce probíhají podobným způsobem jako v reálném světě - nakupují předměty, pozemky, komodity. U těchto transakcí hraje velkou roli důvěra obou stran a problém nastane tehdy, kdy se prodávající rozhodne předem zaplacené zboží nepředat. Nejlehčím způsobem je obrátit se na administrátora tohoto virtuálního světa, avšak ne vždy je jednoduché krádež dokazovat.

Dalším krádeží může být krádež virtuálního charakteru nebo celého účtu, což je nejefektivnější způsob přístupu k virtuálnímu majetku. Přístup k takovému účtu může získat pachatel už známými způsoby jako je hacking, phishing, pharming a podobně.

Virtuální majetek nemá stanovený právní status v legislativě a proto je často odmítnut z obtížného dokazování hodnoty a způsobení škody, obvykle pachatel není obviněn z krádeže majetku, avšak z neoprávněného přístupu k počítačového systému. [46]

8.2 Virtuální znásilnění

Vymezení tohoto zločinu je mnohem obtížnější v porovnání s virtuální krádeží. Je zřejmé, že virtuální znásilnění neobsahuje jednu důležitou věc a tou je fyzický kontakt. Uživatel, který se setká z násilníkem v tomto virtuálním světě může činnost vždy ukončit prostým odpojením se a této činnosti zabránit. Někteří lidé avšak nepovažují pohlavní styk za nezbytně nutný ke znásilnění a nemusí být přítomna žádná fyzická těla.

I když virtuální znásilnění postrádá prvek fyzického kontaktu může zahrnovat aspekty pro znásilnění typické. Velké citové i psychické investice jedinců do virtuálních světů může vést k jejich rozhořčení a mohou se cítit napadeni. Virtuální znásilnění je tedy spíše duševního než fyzického stavu. Sexuální aktivita způsobená ať už obrazově nebo textově může vést k traumatickým zkušenostem.

Virtuální znásilnění působí podvratně. Škodí uživatelům a oběti mohou zažívat emocionální újmy nebo také nedůvěru k virtuálnímu světu. Popřípadě negativně ovlivňuje virtuální svět a jeho kulturu. I přesto by tento útok neměl podléhat právní regulaci jako reálný sexuální útok, většina právních teoretiků se jím zabývá a zkoumá jejich dopad. [47]

8.3 Virtuální vražda

Vraždou se rozumí smrt jiného člověka. Pojmou však vraždu z hlediska virtuálního světa je mnohem obtížnější a není jednoznačné. Ve virtuálním prostředí je běžné setkávat se s aktem napodobujícím vraždu v reálném světě. Jedná se však pouze o simulaci a nikoli fyzický čin. Pokud hráč za pomoci svého virtuálního charakteru zabije jiného hráče jedná se většinou o produkt hry, která má s virtuálním světem nějakou souvislost. Charaktery jsou reprezentovány různými bytostmi, které s dalšími bojují.

Jsou tady také i hry mírumilovného charakteru, kde zabíjení dalších hráčů je spíše nečestnou praktikou. Zabíjení charakterů není přímo cílem hry a může přinášet zcela jiný pohled na situaci. Vražda není fyzická a oběť neprožívá žádnou bolest ani utrpení je tedy spíše emocionálních následků. Vzniká však otázka zda-li tato násilná činnost může mít opravdu vliv na psychiku hráčů bez ohledu na to, že není fyzického dopadu. Ačkoli existuje spousta studií, které zkoumají vliv her na agresivitu a emoce není negativní vliv přímo dokázán.

Obvinění z vraždy virtuálního charakteru mnohdy u policie neuspěje, ale v budoucnu bude možná šance vyšší až se dostane do povědomí. Obviněním z neoprávněného přístupu je mnohonásobně větší šance na úspěch. [47]

9 PRÁVNÍ ASPEKTY VYŠETŘOVÁNÍ

Vyšetřování je rozsáhlý proces úkonů hlavně v prvních stádiích trestního řízení. Činnost orgánů trestního řízení je základním předpokladem pro dosažení účelu trestního řádu, přesněji odhalení pachatele a trestního činu. Poté je teprve možné pokračovat do dalších fází a tím je potrestání pachatele. Právní aspekty jsou čerpány z aktuálního Zákonu o trestním řízení (trestní řád) č. 141/1961 Sb. [48]

Hlavním cílem vyšetřování v počáteční fázi je získat co nejvíce důkazů, které umožní další poznání skutečností a důležitá rozhodnutí. Problematika důkazních prostředků je v § 89 TŘ, konkrétně v druhém odstavci ve znění, že jako důkaz může může sloužit cokoliv, co přispěje k objasnění situace a tím jsou i výslechy svědků, obviněných, znalecké posudky a listiny důležité pro řízení a ohledání. Trestní řád mluví o důkazech velmi obecně. Při vyšetřování počítačové kriminality budou mimo klasické důkazy potřeba i jiné důkazy, specifické pro tuto oblast.

Policie ČR podniká nezbytné kroky pro zajištění důležitých důkazů pro trestní řízení jako jsou počítače, datové nosiče a další materiál, kterým mohou být například různé písemnosti. Takové sbírání důkazů probíhá obvykle na místě, kde byl spáchán trestní čin a tím bývá doma nebo v sídle společnosti. Domovní prohlídku je možné nařídit až poté, kdy je splněno vymezení v ustanovení § 82 TŘ. První odstavec hovoří o tom, pokud je důvod a podezření na trestní čin v bytě nebo jiných prostorech na bydlení a nebo se tam nachází osoba důležitá k trestnímu řízení. Druhý odstavec potom hovoří o stejném důvodu avšak v prostorech, které nejsou určeny k bydlení, kde spadají i pozemky a další neveřejně přístupné prostory. Domovní prohlídka je jedním z největších zásahů do domovní svobody. Při vyšetřování počítačové kriminality je toto však nesmírně nezbytné, protože výpočetní technika se zde nachází prakticky vždy.

Podle § 83 odst. 1 TŘ musí být domovní prohlídka vydána písemně a musí být odůvodněna. Oprávnění pro nařízení domovní prohlídky má předseda senátu a také soudce. Prohlídku tedy bez tohoto povolení není možné policejními orgány provést a to ani v neodkladném případě.

Za určitých okolností v ustanovení § 83c TŘ může do obydlí policejní orgán vstoupit pouze tehdy, pokud je to nezbytné pro ochranu života a zdraví osob nebo ochranu jiných práv a svobod. Při vyšetřování počítačové kriminality to může mít význam například při

hrozícím teroristickém útoku a je nutné neprodleně jednat a útoku zabránit. Avšak při běžných prohlídkách je potřeba vždy souhlas předsedy senátu, popřípadě soudce.

Další možností podle § 83a odst. 3 TŘ je možné provést prohlídku bez předchozího příkazu a to pokud majitel bytu nebo prostor písemně prohlásí souhlas je vstupu policejních orgánů. Tato varianta však není v praxi běžná. V případě nelegálního páchání by se tak majitel de facto sám udal.

Při vyšetřování mohou být zajištěny jak kompletní počítačové systémy, tak jejich části jako důkazový materiál. Ust. § 78 TŘ v prvním odstavci říká, že pokud má kdokoliv u sebe důležitý materiál k trestnímu řízení je povinen jej na vyzvání soudci nebo policejnímu orgánu a pokud tak neudělá je potřeba jej upozornit, že dotyčnému může mu být věc odňata. Navazující ustanovení § 79 TŘ potom hovoří o odnětí této věci a pokud ji dotyčný nevydá bude policejním orgánem na příkaz státního zástupce odebrána.

Při vyšetřování je také nutné posoudit jak velkou část výpočetní techniky je potřeba zajistit, jestliže je možnost spokojit se pouze s mediálními nosiči, zajištění celé výpočetní techniky by bylo v rozporu s ustanovením § 2 odst. 4 TŘ, kdy by nebyl postup zabavení kompletních systémů přiměřený a zasahoval by do práv osob.

Počítačové protiprávní činy jsou většinou páchány úmyslně a často vyžadují odposlechu kvůli závažnosti tohoto činu. Předpoklady pro použití tohoto úkonu jsou v § 88 TŘ. V prvním odstavci je stanoveno, že pokud je čin závažný, může státní zástupce nařídit odposlech a záznam telekomunikačního provozu, pokud je předpokládané usnadnění trestního řízení.

Kriminalistickou metodou, která je bezpochyby nejdůležitější je výslech podezřelého nebo obviněného. Tato metoda se řadí k nejstarším a charakter výslechu je zcela individuální podle situace. Průběh výslechu je v trestním řádu v ustanoveních § 91 - 95 TŘ. Pokud osoba vyslýchaná je svědkem, potom jsou to ustanovení § 97-104 TŘ.

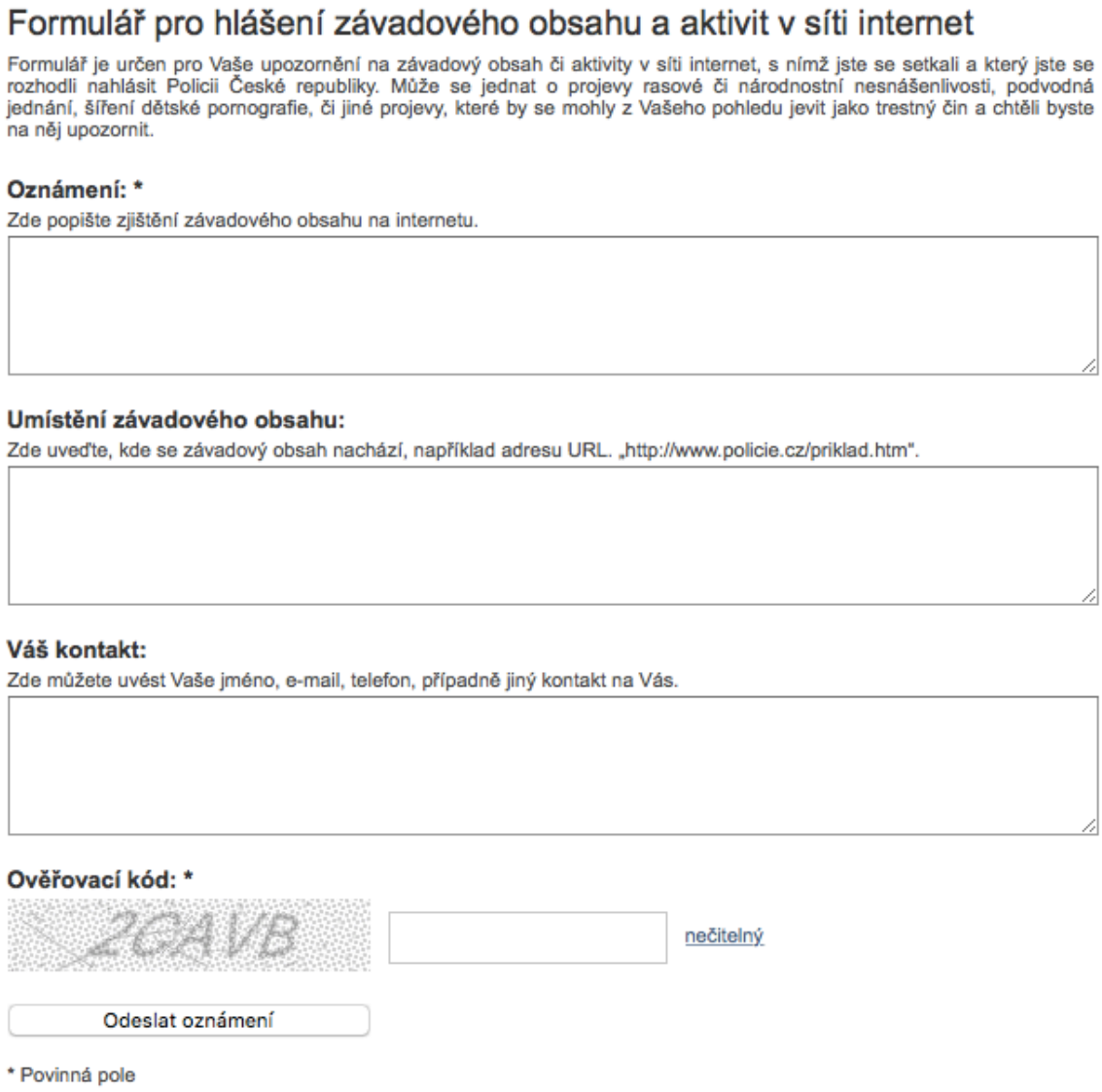
Výslech má za cíl získat věrohodné nebo úplné poznatky vyšetřované události a v nejlepším případě k doznání podezřelého. Je nutné při výslechu předpokládat vysokou inteligenci pachatele, který může reagovat na kladené otázky velmi rychle. U protiprávního činu, který spadá do počítačové kriminality je nutná přítomnost odborníka nebo znalce. Podle § 55 TŘ musí být celý průběh výslechu zaznamenán do protokolu. [20]

II. PRAKTICKÁ ČÁST

10 VYŠETŘOVÁNÍ POČÍTAČOVÉ KRIMINALITY

10.1 Ohlášení činu

Vyšetřování kyberzločinu většinou předchází nějaké oznámení o činu, toto oznámení může být podáno elektronicky nebo přímo na příslušných orgánech jako je Policie ČR. Níže příklad elektronicky podávaného oznámení.



Formulář pro hlášení závadového obsahu a aktivit v síti internet

Formulář je určen pro Vaše upozornění na závadový obsah či aktivity v síti internet, s nímž jste se setkali a který jste se rozhodli nahlásit Policii České republiky. Může se jednat o projevy rasové či národnostní nesnášenlivosti, podvodná jednání, šíření dětské pornografie, či jiné projevy, které by se mohly z Vašeho pohledu jevit jako trestný čin a chtěli byste na něj upozornit.

Oznámení: *

Zde popište zjištění závadového obsahu na internetu.

Umístění závadového obsahu:

Zde uveďte, kde se závadový obsah nachází, například adresu URL. „http://www.policie.cz/priklad.htm".

Váš kontakt:

Zde můžete uvést Vaše jméno, e-mail, telefon, případně jiný kontakt na Vás.

Ověřovací kód: *

2CAVB nečitelný

Odeslat oznámení

* Povinná pole

obr. 3: Trestní oznámení

10.2 Přístup k situaci

Po předložení stručných informací o zločinu jsou důležité další kroky důležité k vyšetřování počítačové kriminality jako je identifikaci potenciálních důkazů a další práce s nimi.

Stejně jako u jiných protiprávních případů musí příslušník orgánu určit konkrétní prvky trestného činu a zda mají zákony v jeho stíhání pravomoc. Dalším faktorem může být zvážení globální povahy zločinu, který se pak dále konzultuje se státním zástupcem.

10.3 Počátek šetření

Při vyšetřování počítačové kriminality jsou také důležité běžné vyšetřovací metody. Dotazování se kde, kdy, jak, proč jsou stále nezbytné. Tato fáze má za cíl zjistit potenciálního pachatele a místo činu. Vyšetřovatel si ještě pokládá následující otázky:

- Kdo je potenciální podezřelý?
- Co za zločin bylo spácháno?
- Kdy byl zločin spáchán?
- Jsou tyto zločiny v rozporu se zákonem?
- Existují nějaké důkazy?
- Kde mohou být umístěny fyzické nebo digitální důkazy?
- Je potřeba aby byl nějaký důkaz neodkladně vyfotografován/zachován?
- Jak je možné zachovat důkazy po dobu soudního řízení?

10.3.1 Praktický případ 1

Občan tvrdí, že při surfování po internetu narazil na web, který by měl být vyšetřen. Občan uvede adresu webové stránky například: www.seznam.cz.

Prvním krokem je získat z webové adresy IP adresu. Existuje mnoho komerčních softwarových nástrojů a také veřejných webových stránek, které dokáží vyšetřovatelům tento problém snadno vyřešit. Jako nejznámější český web je možno uvést www.paranoia.cz, který obsahuje funkci WHOIS.

Další zahraniční webové stránky umožňující tuto funkci.

- www.geektools.com
- www.dnsstuff.com

Funkce WHOIS - nástroj, který prochází databázi obsahující domény, IP adresy a také kontaktní informace jako jsou jména, poštovní adresy a telefonní čísla.

```
domain: seznam.cz
registrant: SB:SEZNAM-CZ-AS
admin-c: SB:SEZNAM-CZ-AS
nsset: SEZNAM-NAMESERVERS
registrar: REG-IGNUM
status: Sponsoring registrar change forbidden
status: Update forbidden
registered: 07.10.1996 02:00:00
changed: 23.01.2008 18:51:04
expire: 29.10.2016

contact: SB:SEZNAM-CZ-AS
org: Seznam.cz, a.s.
name: Seznam.cz, a.s.
address: Radlická 3294/10
address: Praha 5
address: 15000
address: CZ
e-mail: domeny@firma.seznam.cz
registrar: REG-IGNUM
created: 10.08.2001 22:13:00
changed: 17.06.2013 12:21:03

nsset: SEZNAM-NAMESERVERS
nserver: ans.seznam.cz (77.75.74.80, 2a02:598:3333::3)
nserver: ams.seznam.cz (77.75.75.230, 2a02:598:4444::4)
tech-c: SB:SEZNAM-CZ-AS
registrar: REG-IGNUM
created: 18.10.2007 18:01:01
changed: 11.12.2014 11:08:04
```

obr. 4: Výsledek WHOIS webu paranoia.cz

Obrázek ukazuje typické údaje, které WHOIS zobrazí. Tento konkrétní případ je zaměřen na seznam.cz a informace obsažené z paranoia.cz.

Vyšetřovatelé musí mít na vědomí, že vyšetřování na těchto stránkách může být monitorováno a zaznamenáváno. Je důležité tyto citlivé dotazy z počítače provádět tak, aby nebylo možné vyšetřovatele zpětně vysledovat.

Díky IP adrese, data a času (včetně časového pásma) může většina providerů internetu identifikovat registrovaného uživatele k přiřazené IP adrese, což může vyšetřovatelům pomoct k doplnění potřebných informací jako jsou aktivity konkrétní IP adresy v různých časech. Avšak vyšetřovatel bude možná také potřebovat tradiční vyšetřovací metody k identifikaci osoby. V tomto případě je tedy důležitá případná spolupráce s internetovým providerem dotyčného podezřelého.

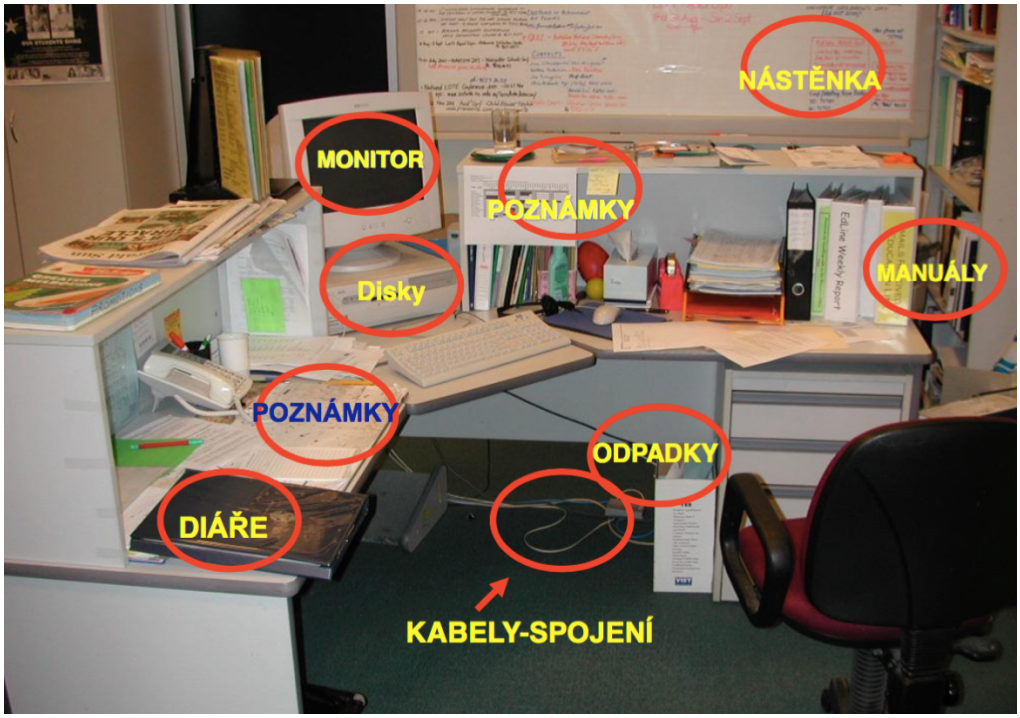
10.4 Identifikace možných důkazů

Cílem je zajistit co nejvíce možných důkazů, které jsou nezbytně nutné k dalším právním rozhodnutí v trestním řízení. Problematiku důkazního materiálu najdeme v §89 odst. 2 TŘ, který mluví o tom, že za důkaz lze považovat vše, co může přispět k objasnění situace, hlavně výpovědi svědků a obviněných. Identifikaci důkazů předchází prohlídka místa činu, kde se fyzicky nachází předmět, který protiprávní jednání způsobil – například počítač. Tento zásah do soukromí v podobě domovní prohlídky nalezneme v §82 TŘ. Domovní prohlídku lze nařídit předsedou senátu a v přípravném řízení na návrh státního zástupce soudce. Příkaz musí být odůvodněn a vydán písemně. Na místě činu, které bylo označeno jako možné spáchání počítačového zločinu obsahuje většinou důkazy, které se dají řadit do dvou kategorií:

1) Fyzické důkazy
2) Digitální důkazy

10.4.1 Fyzické důkazy

Fyzické důkazy nejsou pouze fyzická elektronická zařízení jako například počítače, ale je možno sem řadit i různé diáře, sešity, poznámky. Fyzické důkazy pak přímo směřují k důkazům digitálním.



obr. 5: Fyzické důkazy [51]

10.4.2 Digitální důkazy

Digitální důkazy mohou být různých typů souborů a velikostí. Dále mohou být důkazy šifrovány, chráněny, skryty a podobně. Pokud orgán nemá prostředky, nástroje nebo zvláštní odborné znalosti potřebné k identifikaci a shromáždění těchto důkazů je potřeba zvážit spolupráci s více vybavenými organizacemi. Také je potřeba myslet na to, že téměř každá digitální stopa může být důkazem a proto je nutné v této oblasti dbát zvlášť velké pozornosti.

Ve většině případech mohou vyšetřovatelé zabavit fyzické elektronická zařízení bez povolení, ale pokud chtějí dále v zařízení hledat, pak už povolení potřebují. Někdy je potřeba i více povolení pokud je určité zařízení spojeno s více trestnými činy.

Nejběžnější elektronické zařízení obsahující digitální důkazy:

Zařízení	**Potenciální digitální důkazy**
Fotoaparát/kamera	Obrázky Videa
Telefon	Obrázky Videa Audio nahrávky Zprávy Záznamy o hovorech Lokace
Počítač	Obrázky Videa Emaily Zprávy a příspěvky na sociálních médích Historie prohlížení (Internet) Dokumenty
Tablet	Totožné jako počítač
Herní konzole	Obrázky Videa Dokumenty

Tabulka 1: Zařízení a digitální důkazy

10.5 Výslech

Nejdůležitější metodou je výslech podezřelých a obviněných nebo případných svědků. Výslech může být zcela individuální a závisí na charakteru a závažnosti zločinu. Cílem by mělo být získání dalších důkazů nebo úplného doznání pachatele. Vyslýchající by měl mít připravenou řeč – seznam otázek a být plně seznámen se situací a mít na paměti, že podezřelý může dosahovat vysoké inteligence. U výslechu musí být přítomen znalec nebo odborník na počítačovou kriminalitu.

Výslech většinou probíhá ve třech fázích – úvod, monolog, dialog.

Úvod – navazování kontaktu s osobou vyslýchanou a zjištění základních osobních dat.

Monolog – vyslýchaná osoba vyličuje bez přerušení všechny skutečnosti, které by chtěl sdělit. Tento monolog je důležitý s psychologického hlediska, kde vyslýchaná osoba může udat i takové informace, na které by se vyslýchající neptal. Může také vypovídat pravdivěji.

Dialog – Znalec je klíčovou osobou, počítačová kriminalita je natolik odborná, že by vyslýchající osoba nemusela správně skutečnosti chápat a nemusel by otázky správně pokládat.

Celý průběh výslechu musí být zaznamenán do protokolu podle ustanovení §55 TŘ.

10.6 Obvinění a tresty - shrnutí

Krátké shrnutí možných trestů podle trestního zákoníku č. 40/2009 Sb. [48]

Neoprávněné nakládání s osobními údaji §180 TZ

Odnětí svobody na 1 až 8 let, peněžitý trest nebo zákaz činnosti.

Výroba a jiné nakládání s dětskou pornografií §192 TZ

Odnětí svobody na 2 až 8 let a propadnutí majetku.

Neoprávněný přístup k počítačovému systému a nosiči informací §230 TZ

Odnětí svobody na 6 měsíců až 5 let, zákaz činnosti, propadnutí věci, peněžitý trest.

Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti §232 TZ

Odnětí svobody až na 2 léta, zákaz činnosti nebo propadnutí věci.

Padělání a pozměnění peněz §233 TZ

Odnětí svobody na 1 až 12 let, propadnutí majetku.

Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi §233 TZ

Odnětí svobody na 6 měsíců až 8 let, zákaz činnosti nebo propadnutí majetku.

Šíření poplašné zprávy § 357

Odnětí svobody na 1 až 8 let nebo zákaz činnosti.

11 NEJVĚTŠÍ PŘÍPADY V ROCE 2015

Všechny informace pochází z internetového portálu www.novinky.cz, případy se zaměřují na hlavní kybernetické zločiny a problémy v roce 2015.

11.1 Leden

Pachatelé využívají povánočních výprodejů za využití podvodných emailů, které informují o objednávce zboží za tisíce korun. Emaily obsahují přílohu, která by měla obsahovat fakturu, avšak místo toho obsahuje vir.

Phishing zaměřený na Českou spořitelnu, email obsahuje odkaz na podvodnou stránku, která vyžaduje zadání citlivých údajů. Česká spořitelna se od těchto emailů distancuje a upozorňuje, že nikdy nevyžaduje aktualizaci informací internetového bankovnictví.

obr. 6: Logo České spořitelny [52]

Útoky hackerů na 19 tisíc francouzských webů. Mimo stránky vojenských útvarů jsou to také školy, ústavy i pizzerie. Útoky však nezpůsobily žádné velké kromě nedostupnosti těchto stránek v době útoku. Pravděpodobnými pachateli byla hackerská skupina, která podporuje islámské extremisty.

Napadení twitterových účtů New York Post a UPI na kterých bylo hackery umístěny falešné ekonomické a bezpečnostní informace. V těchto informacích byla mimo jiné i citace papeže, který prohlašuje, že začala třetí světová válka.

11.2 Únor

Podnikatel přišel o statisíce v důsledku phishingových emailů, podnikatel otevřel emailovou přílohu, která obsahovala vir, který v počítači vysledoval údaje do internetového bankovnictví.

Organizovaná skupina napadla více než 100 bank ve 30 zemích se ziskem více než 20 miliard korun. Hackeři nevyužívají účty klientů, avšak finance přímo z vnitřních systémů. Hackeři využili špionážní software k přehledu o klíčových zaměstnancích. Po získání potřebných informací začali banku okrádat způsobem, tak sofistikovaným, že bylo těžko rozpoznatelné, že tyto převody nepřichází od zaměstnanců.

Národní bezpečnostní agentura (NSA) údajně infikovala nové počítačové komponenty sledovacími viry, které umožňovali nejen sledování počítačového systému, ale také přístup k libovolným datům v počítači. Výrobci počítačů nic nevěděli, avšak napadeni byli všichni největší hráči. Virus se vyskytoval nejméně v 30 zemích uvedla antivirová společnost Kaspersky.

Sleva 50% na pohonné hmoty při vyplnění jména a emailové adresy na podvodné stránce, kde jim bude sleva zaslána. Lidé koupí voucher, který jim například za 1000 Kč umožní natankovat pohonné hmoty v hodnotě 2000 Kč. Emaily se odkazují na legitimní společnost, avšak lidé, kteří za voucher zaplatí, nic nedostanou.

11.3 Březen

Miliony počítačů jsou ohroženy chybou zabezpečení komunikace. Sem se řadí jak počítače s operačním systémem Windows, tak Android, iOS a MacOS X. Bezpečnostní chyba umožní pachateli zaútočit na počítače připojené k webu a pachatel tak může bez problému sledovat komunikaci a také nakazit počítač škodlivým softwarem.

Americké spisy naznačují, že výzkumníci vlády Spojených států vytvořili pozměněnou verzi XCode od Applu, což je hlavním vývojovým softwarovým balíčkem, který Apple používá. Pozměněná verze by pak mohla agentům umožnit přístup do přístrojů a zmocnit se hesel a zpráv. CIA se k tomuto případu nevyjádřila a Apple nikdy s takovými složkami nespolupracoval na prolomení bezpečí.

Operační systémy Windows a webové prohlížeče od Microsoftu Internet Explorer obsahují chybu ve skriptovacím jazyku. Pachatelé mohou chybu využít k propašování jakéhokoliv návštěvníka. Chyby byly následně opraveny Microsoftem.

Přibývá tzv. skimmovacích zařízení, které snadno zkopírují kreditní kartu. Toto zařízení je umístěno na samotném bankomatu nebo na dveřích k bankomatu, které umožňují přístup i mimo pracovní hodiny. Kartu jsou tak schopni zkopírovat ještě dříve než je vložena do bankomatu. V případě vhodně umístěné kamery je možno vysledovat i PIN kód.

Pouhých 17 sekund stačilo hackerovi k prolomení ochranných prvků i webového prohlížeče Internet Explorer. Také ostatní webové prohlížeče neobstály dobře. Všechno bylo uskutečněno v rámci hackerské soutěže a vítěz získal finanční odměnu.

Podvodníci oprášili starý trik s emaily o doručování zásilky. Dříve se vydávali za Českou poštu, nyní za doručovací službu DHL. Emaily jsou psané v němčině i když adresovaní jsou tuzemští adresáti. Email obsahuje přílohu ve formátu ZIP, která stáhne do počítače trojského koně a umožní tak získání kontroly nad počítačem.

11.4 Duben

Podvodníci využívají nový trik s hláškou o chybné platbě. Počítač napadený virem zobrazí zprávu o chybné platbě, připsané na jeho účet, po přihlášení do internetového bankovnictví. Zpráva vyžaduje po uživateli vrácení připsané částky zpět jinak bude jejich bankovní účet zablokován. Formou odkazu na pokračování pro vrácení peněz se pachatel dostane k osobním informacím a získá peníze z účtu uživatele.

Pachatelé si podvodnými emaily přišli na statisíce. Zpráva vyzívá uživatele k uhrazení dlužné částky způsobené využíváním bankovních produktů. Zpráva obsahuje mnoho gramatických chyb a žádnou hlavičku legitimní společnosti, dále pak obsahuje přílohu ve které se nachází trojský kůň.

Ministr obrany USA oznamuje, že Pentagon odhalil útok ruských hackerů na armádní síť. Útok byl během 24 hodin odhalen a odvrácen. Tento útok napomáhá k rozšíření obraných kybernetických sil v USA.

11.5 Květen

Až padesát hackerů bylo zatčeno v Polsku, Španělsku a Itálii, kteří díky phishingovým útokům vytáhli z lidí několik milionů korun. Policisté prohledali na 58 míst při operaci zvané Triangle. Hackeři využívali metody „Muž uprostřed“ , která sledovala komunikaci mezi dvěma účastníky.

Společnost Starbucks čelila podvodným emailům, které vyzívali uživatele ke změnění svých uživatelských údajů. Tyto phishingové zprávy po zadání údajů získají přístup k účtu uživatele a mohou převést peníze s přiřazené kreditní karty na dárkové poukazy. Ty potom jednoduše prodají nebo poukazy odešlou na svoje osobní účty pro využití slev.

obr. 7: Logo Starbucks [53]

Hacker napadl systémy dopravního letadla a mohl ovlivnit i jeho směr letu. Hacker byl zatčen a byly mu zabaveny elektronická zařízení. Pachatel přepsal kód u jednoho z motorů v palubním počítači, což mu umožnilo vyslat příkaz k stoupání letadla.

11.6 Červen

Hackeři ukradli osobní data všech vládních zaměstnanců v USA. Podezřelá je Čína, ta však útok popírá. Ztráta osobních údajů se týká více než čtyř milionů zaměstnanců. Mezi získané údaje patří adresy, data narození, výše platů a informace o zdravotním nebo životním pojištění.

Pachatelů šířili viry pomocí velkých legitimních webů. Útočníkovi se podařilo využít chyb ve Flash playeru, která dopomáhala k zobrazování reklam na nejvíce navštěvovaných stránkách. V podstatě stačilo pouze zobrazení reklamy a do počítače se stáhl trojský kůň. Napadeny byli například weby CNN nebo i letiště Václava Havla.

V operačním systému iOS, který využívají iPhony a iPady se objevila velká chyba. Pokud si lidé nainstalovali určitou aplikaci, útočník bez problému získá přístup k citlivým datům uživatelů, konkrétně uložené hesla k jednotlivým službám.

Hackeři napadli polské letecké společnosti a útokem utrpělo na 1400 cestujících. Kvůli útoku muselo byt zrušeno 10 letů, protože společnost kvůli výpadku nemohla sestavit letecké plány. Hackeři se zaměřili hlavně na pozemní operační systémy aerolinek.

11.7 Červenec

Antivirová ochrana otevírala hackerům přístup do počítače. Chyba kterou antivirový program obsahoval umožnila útočníkovi číst měnit nebo mazat soubory v systému. Dále přístup k hardwaru jako je webkamera, mikrofon a skener. Postiženy byly antivirové programy od společnosti ESET.

Pachatelé využívají dobrého jména společnosti Penny. Rozesílají emaily ve kterých se soutěží o cenné výhry. Všechno, co pro to uživatel musí udělat je zadat svoje telefonní číslo a šířit dále po sociální síti. Důvěřivci, kteří zadají telefonní číslo souhlasí se zasíláním prémiových sms zpráv, které stojí 99 Kč, těchto zpráv může přijít i více na jedno číslo. Tento souhlas je uveden miniaturním písmem v podmínkách „soutěže“. Společnost Penny market nemá s tímto nic společného.

Hackerská společnost Hacking Team byla sama hacknuta. Společnost stojí za vývojem šmírovacích zařízení a nástrojů pro hackování. Mezi klienty této společnosti byli údajně i složky české policie. Pachatelé získali kompletní přístup k databázi a mohl si je z internetu stáhnout kdokoliv.

11.8 Srpen

Podvodníci cílí na klienty Fio banky. Emaily obsahující logo společnosti vyžadují po uživatelích přihlášení do internetového bankovnictví, kde dojde k zneužití osobních údajů.

obr. 8: Logo Fio banky [54]

Hackeři pod názvem Impact Team získali údaje o uživatelích mezinárodní diskrétní seznamky Ashley Madison. Tato seznamka slouží k seznámení zadaných lidí k nalezení milostného poměru. Pachatelé získali údaje o emailových adresách, erotický preferencích nebo detaily o platebních kartách. Podle informací hackeři odeslali tyto údaje na skryté servery.

Patnáctiletý mladík organizoval internetové útoky za statisíce. Mladík vystupující jako lídr hackerské skupiny pod názvem Lizard Squad prodával za pár stovek korun internetové útoky DDoS. Platbu přijímali ve virtuální měně bitcoin, která se na internetu nedá dohledat. Hackeři mají na svědomí vyřazení celostátních médií, škol nebo online obchodů. Po několika měsícovém vyšetřování policie mladíky z Velké Británie dopadla, i přes obrovským škodám, které způsobili jim hrozí výjimečný trest kvůli nízkému věku.

11.9 Září

Útočníci zkouší nový trik v podobně nainstalování tlačítka do sociální sítě Facebook. Tlačítko chystá oficiální i Facebook avšak nebude potřeba žádné instalace. Důvěřivci, kteří toto tlačítko chtějí kliknou odkaz, který jim do počítače nainstaluje vir ke sběru citlivých informací.

obr. 9: Logo Facebook [55]

Po stažení aplikace vydávající se za didaktický test bylo nakaženo až 500 000 zařízení virem. Didaktický test s názvem BrainTest, který se nacházel v internetovém obchodě s aplikacemi Google Play byl nakažen škodlivým kódem.

Pachatelé vydávající se za zaměstnance České spořitelny nabízí hypotéky. Tento phishingový útok se však snaží pouze vylákat potvrzovací sms zprávu k vybrání peněz účtu uživatele. Trik funguje stejně jako drtivá většina těchto útoků. Počítač nakažený virem odkazuje na podvodné stránky, kde se nachází nabídka se super výhodou hypotékou, kde je potřeba provést pravost uživatele pomocí potvrzovací sms zprávy.

11.10 Říjen

Cílem hackerů se stala americká společnost T-mobile, kterým se podařilo získat údaje o 15 milionech zákazníků firmy. Údaje obsahují adresy, data narození, nikoli však finanční údaje o kartách. Zatím nejsou důkazy, že by byly údaje zneužity.

Čísla platebních karet byly ukradeny hackery při útoku na platební systém v sedmi mezinárodních hotelích amerického realitního magnáta a kandidáta na prezidenta Donalda Trumpa. Útočníci získali přístup k citlivých všech hostů hotelů a zákazníků v restauracích.

obr. 10: Donald Trump [56]

Poskytovatel telekomunikačních služeb a internetu TalkTalk sídlící v Britálnii se stal terčem útoku hackerů. Útok vedl ke krádeži osobních údajů více než čtyř milionů zákazníků. Není jasné jestli se jedná o jednotlivce nebo hackerskou organizovanou skupinu, avšak je to jedno z největších narušení bezpečnosti soukromí ve Velké Británii.

11.11 Listopad

Organizace hackerů pod názvem Anonymous se zaměřila na uvolnění osobních údajů Ku-klux-klanu na internet. Hackeři se k těmto údajům dostali prostřednictvím účtů na sociální síti Twitter. Anonymous je přesvědčen, že Ku-klux-klan je potřeba vnímat jako teroristickou organizaci.

Díky prolomení bezpečnostní chyby v novém operačním systému od Applu si hackeři přišli na milion dolarů. Hackerská skupina, která zůstává utajena prolomila operační systém

a zvítězila tak v soutěži vyhlášenou společností Zerodium a právě milion byl přislíben tomu, kdo bezpečností chybu jako první najde.

Útočníci využívají novou vyděračskou metodu, která cílí na uživatele operačních systémů Linux. Pokud uživatelé stáhnou tento virus, který jim zašifruje data na disku a pro dešifrování je potřeba zaplatit určitou částku. Samozřejmě po zaplacení částky se nic nestane. Tento vir však obsahuje chybu v podobně dešifrovacího klíče.

11.12 Prosinec

Útočníci se snaží využít Vánoc, kde žádají o zaslání drobné finanční částky do 50 Kč. Všechno začíná na Facebooku, kde se pachatel snaží pomocí zprávy oslovit klienta. Poté uživateli zašle odkaz na internetové bankovnictví pro zaplacení této částky, tento phishingový odkaz dostane z uživatelů citlivé údaje o bankovnictví a vede k dalšímu vybílení účtu.

Hackeři napadli seznamku pro HIV pozitivní jedince a zveřejnili jejich údaje. Byly zveřejněny údaje o datu narození, náboženském vyznání, počtu dětí a tělesných mírách.

Twitter zaznamenal řadu hackerských útoků o získání citlivých údajů uživatelů. Hacker zaútočil pouze na malou skupinku uživatelských účtů, ale žádný vážný dopad tohoto útoku nebyl zaznamenán. V podezření tohoto útoku je Čína a Severní Korea.

obr. 11: Logo Twitteru [58]

Hackeři se dostali do databáze vzdělávacích aplikací, her a elektronických učebnic. Ohroženo je až 5 milionů klientů, což se řadí mezi 4. Největší případ úniku citlivých dat. Útočníci se mohli dostat k obecným informacím o klientovi a zároveň IP adresám.

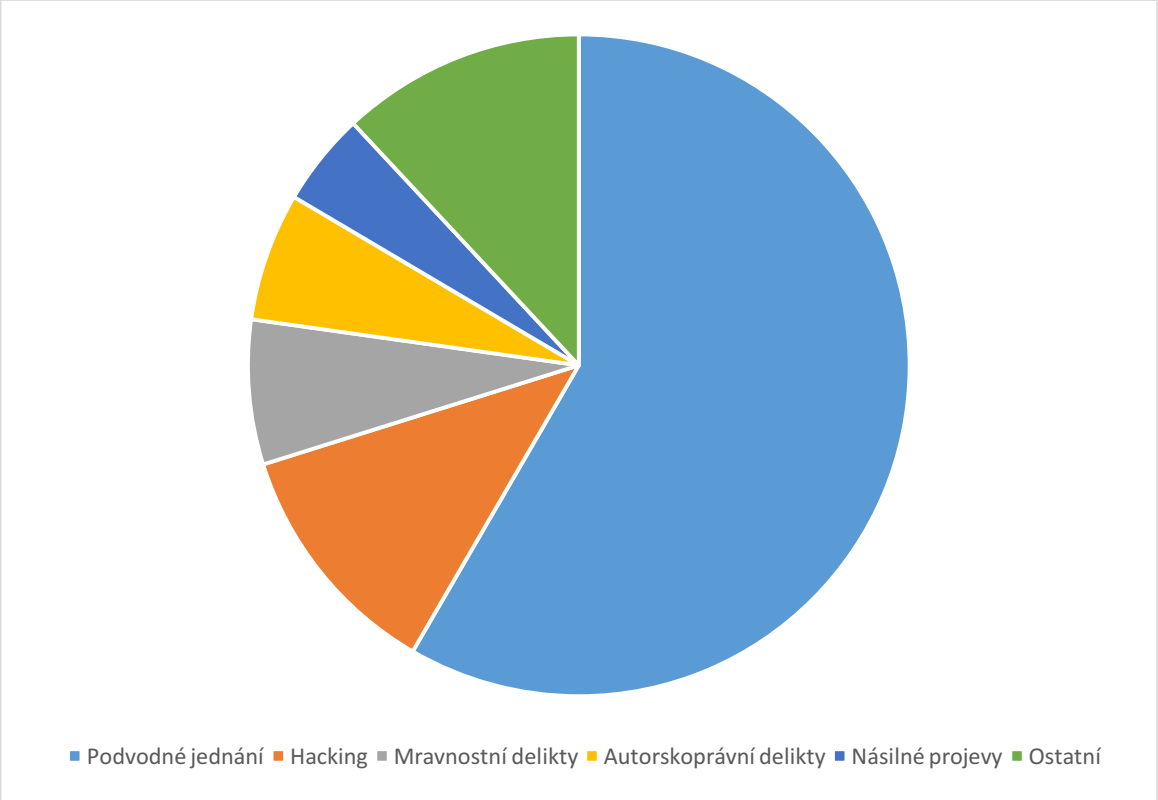
Britskému nejmladšímu dopadenému hackerovi je 12 let. Průměrný věk hackerů se neustále snižuje a již nyní je na hranici 17 let, o rok dříve však byl průměrný věk 24 let. Ke snižování snižování průměrného věku dochází v důsledku snadné dostupnosti nástrojů na internetu.

12 STATISTIKY POČÍTAČOVÉ KRIMINALITY

Nejdůležitější údaje a statistika k počítačové kriminalitě v roce 2015. [56]

12.1 Struktura počítačové kriminality v ČR v roce 2015

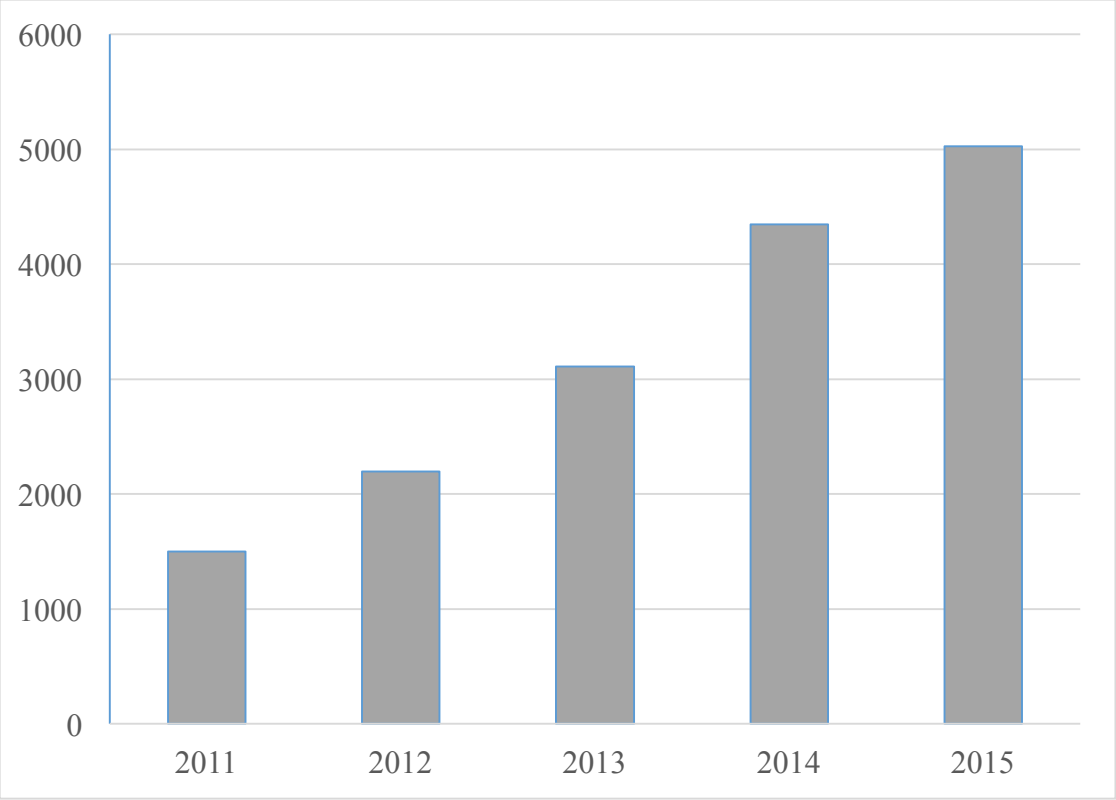
Podvodné jednání	2932	58%
Hacking	592	12%
Mravnostní delikty	355	7%
Autorskoprávní delikty	315	6%
Násilné projevy	229	5%
Ostatní	600	12%



Graf 1: Struktura počítačové kriminality v roce 2015

12.2 Počet počítačových zločinů za poslední roky v ČR

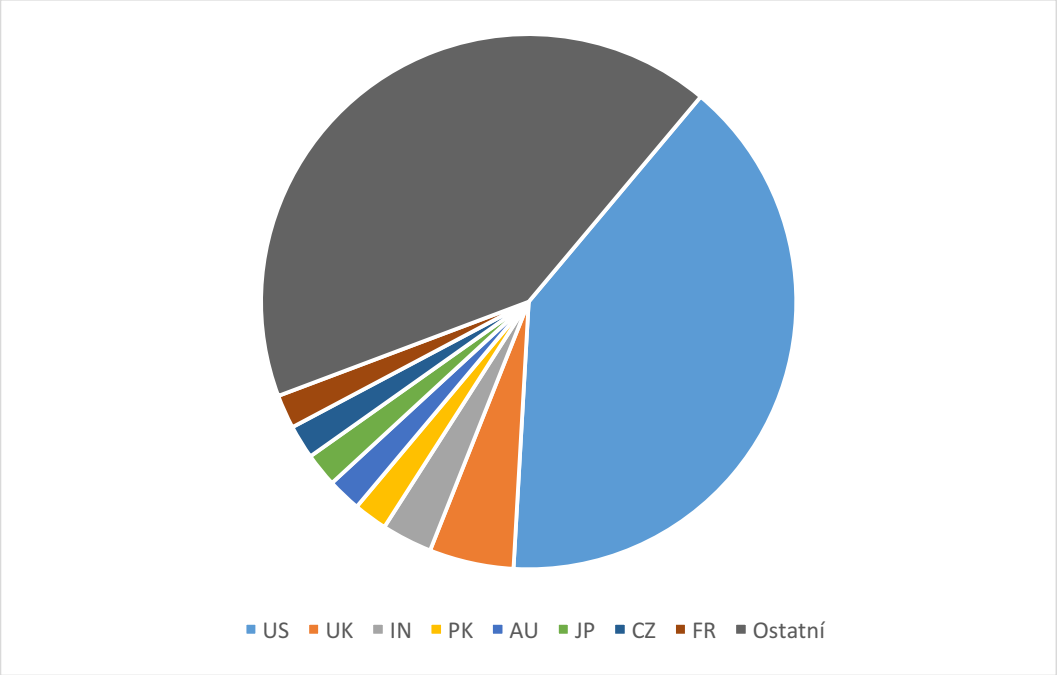
2011	1502
2012	2195
2013	3108
2014	4348
2015	5023



Graf 2: Počet počítačových zločinů v roku 2011 - 2015

12.3 Nejčastější útoky počítačové kriminality

US	39%
UK	5%
IN	3%
PK	2%
AU	2%
JP	2%
CZ	2%
FR	2%
Ostatní	41%



Graf 3: Útoky počítačové kriminality

13 ZÁVĚR

Jak už bylo v úvodu zmíněno, cílem bakalářské práce bylo seznámit s celou problematikou počítačové kriminality a s příslušnými právními aspekty. Počítačová kriminalita je záležitostí moderní doby a s neustálým rozvojem technologií se pouze stupňuje a na povrch se vyplavují nové hrozby. Pachatelé jsou sofistikovanější a přichází se stále novými nápady, které jsou jen těžko odhalitelné. Proto vyšetřovatelé musí být neustále ve střehu, toto dění v digitálním světě sledovat a připravit se na možné hrozby.

Vyšetřování počítačové kriminality nemá přesně stanovené postupy jak k ní přistupovat a je potřeba k ní vzhlížet trochu jiným způsobem než například k tradiční krádeži. Vychází se však ze zásad všeobecných pro protiprávní jednání. Důkazy jako takové stále existují i v tomto odvětví, avšak je potřeba se na ně dívat jako na možné křehké, snadno poškoditelné materiály. Při špatném přístupu k nim mohou být nenávratně ztraceny. Také pachatel mnohem snadněji dokáže sofistikovanými způsoby po sobě zamést stopy. Díky anonymitě, kterou internet nabízí může být pak vystopování pachatele nesmírně obtížným úkonem.

Staré kriminalistické prvky je také nutno použít při výslechu obviněných a svědků, v této fázi se nic moc nezměnilo, stále je to pokládání otázek a získání maximálního množství důkazního materiálu nebo přiznání.

Pokud se na počítačovou kriminalitu zaměříme z hlediska legislativy můžeme v České republice najít jisté mezery v tomto odvětví. Ve srovnání třeba s americkou jsme hodně pozadu, kde mají detailně popsané způsoby spáchání tohoto zločinu, kdežto u nás je to spíše obecné a proto trestání takových zločinců může být někdy opravdu velkým problémem a těžko stanovit, kdy zločin je vůbec v rozporu se zákonem. Příkladem může být spáchání tohoto zločinu nezáměrně s neznalostí této problematiky. V dnešní době každý stahuje a sdílí na internet, ale mnozí si ani neuvědomují závažnost tohoto činu.

Bakalářská práce by měla být přínosem těm, kteří mají v této oblasti ještě jisté pochybnosti a pro zájemce o problém počítačové kriminality včetně příslušného vyšetřování. Na každý případ je nutno se dívat jinak, proto postup rozhodně nesedí na každý čin. V této oblasti je nutná neustálá připravenost, obezřetnost, stále se učit novým věcem. Obecný postup pro vyšetřování počítačové kriminality, včetně konkrétních případů a rozbor minulého roku může být alespoň pro někoho začátkem při seznamování s celou problematikou.

SEZNAM POUŽITÉ LITERATURY

[1] Is.mendelu.cz [online]. [cit. 2016-03-18]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=21047

[2] Vyznam-slova.com [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-03-18]. Dostupné z: http://www.vyznam-slova.com/Poč%C3%ADtač

[3] PORADA, Viktor. Kriminalistika. Brno: CERM, 2001. ISBN 80-7204-194-0

[4] Britannica.com [online]. [cit. 2016-04-08]. Dostupné z: http://www.britannica.com/topic/cybercrime#toc235699

[5] Interpol.int [online]. [cit. 2016-04-08]. Dostupné z: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

[6] Itu.int [online]. [cit. 2016-05-09]. Dostupné z: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

[7] Webopedia.com [online]. [cit. 2016-04-08]. Dostupné z: http://www.webopedia.com/DidYouKnow/Internet/phishing.asp

[8] Techtarget.com [online]. [cit. 2016-04-10]. Dostupné z: http://searchsecurity.techtarget.com/definition/pharming

[9] Nobullying.com [online]. [cit. 2016-05-09]. Dostupné z: http://nobullying.com/hoax/

[10] Osce.org [online]. [cit. 2016-05-09]. Dostupné z: www.osce.org/documents/cio/2004/06/3162_en.pdf

[11] Americanassembly.org [online]. [cit. 2016-04-08]. Dostupné z: http://piracy.americanassembly.org/file-sharing-is-it-wrong/

[12] Britannica.com [online]. [cit. 2016-04-04]. Dostupné z: http://www.britannica.com/topic/cybercrime/Counterfeiting-and-forgery#toc235706

[13] Britannica.com [online]. [cit. 2016-04-04]. Dostupné z: http://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy

[14] Techtarget.com [online]. [cit. 2016-04-08]. Dostupné z: http://searchsecurity.techtarget.com/definition/cybercrime

[15] Britannica.com [online]. [cit. 2016-04-10]. Dostupné z: http://www.britannica.com/topic/cybercrime/Hacking#toc235708

[16] Britannica.com [online]. [cit. 2016-04-06]. Dostupné z: http://www.britannica.com/topic/cybercrime/Spam

[17] Is.mendelu.cz [online]. [cit. 2016-04-06]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7030

[18] Earchiv.cz [online]. [cit. 2016-04-05]. Dostupné z: http://www.earchiv.cz/b05/b0701002.php3

[19] Microsoft.com [online]. [cit. 2016-04-10]. Dostupné z: https://www.microsoft.com/en-us/security/pc-security/virus-whatis.aspx

[20] GŘIVNA, Tomáš a Radim POLČÁK (eds.). Kyberkriminalita a právo. Vyd. 1. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4

[21] Techrepublic.com [online]. [cit. 2016-05-09]. Dostupné z: http://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/

[22] Quora.com [online]. [cit. 2016-05-09]. Dostupné z: https://www.quora.com/How-is-actual-computer-hacking-done

[23] Tomsguide.com [online]. [cit. 2016-05-09]. Dostupné z: http://www.tomsguide.com/us/privilege-escalation,review-1983.html

[24] Kapersky.com [online]. [cit. 2016-05-09]. Dostupné z: https://usa.kaspersky.com/internet-security-center/threats/trojans#.VzBwPmN8agQ

[25] Computerhope.com [online]. [cit. 2016-05-09]. Dostupné z: http://www.computerhope.com/jargon/m/mitma.htm

[26] Wordpress.org [online]. [cit. 2016-05-09]. Dostupné z: https://codex.wordpress.org/Brute_Force_Attacks

[27] Nytimes.com [online]. [cit. 2016-05-03]. Dostupné z: http://www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=2&oref=slogin

[28] Hoover.org [online]. [cit. 2016-05-03]. Dostupné z: http://media.hoover.org/sites/default/files/documents/0817999825_69.pdf

[29] Cert.org [online]. [cit. 2016-05-03]. Dostupné z: http://www.cert.org/archive/pdf/counter_cyberwar.pdf

[30] Olswang.com [online]. [cit. 2016-05-03]. Dostupné z: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf

[31] Hoover.org [online]. [cit. 2016-05-03]. Dostupné z: http://media.hoover.org/documents/0817999825_1.pdf.

[32] Unodc.org [online]. [cit. 2016-05-03]. Dostupné z: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf

[33] 212cafe.com [online]. [cit. 2016-05-03]. Dostupné z: www.212cafe.com/download/e-book/A.pdf

[34] Utica.edu [online]. [cit. 2016-05-03]. Dostupné z: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8- 8B5F-450484589672E1F9.pdf.

[35] Mit.edu [online]. [cit. 2016-05-03]. Dostupné z: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

[36] Efl.edu [online]. [cit. 2016-05-03]. Dostupné z: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

[37] Cert.org [online]. [cit. 2016-05-03]. Dostupné z: www.cert.org/archive/pdf/ecrimesurvey06.pdf.

[38] Missingkids.com [online]. [cit. 2016-05-03]. Dostupné z: www.missingkids.com/en_US/publications/NC144.pdf.

[39] Georgetown.edu [online]. [cit. 2016-05-03]. Dostupné z: www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

[40] Utica.edu [online]. [cit. 2016-05-03]. Dostupné z: www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf

[41] Pctools.com [online]. [cit. 2016-05-09]. Dostupné z: http://www.pctools.com/security-news/script-kiddie/

[42] Currys.co.uk [online]. [cit. 2016-05-09]. Dostupné z: http://techtalk.currys.co.uk/gadgets/are-you-a-casual-hacker/

[43] Cyberdesensereview.org [online]. [cit. 2016-05-09]. Dostupné z: http://www.cyberdefensereview.org/2015/04/07/organized-cyber-crime/

[44] Hackread.com [online]. [cit. 2016-05-09]. Dostupné z: https://www.hackread.com/10-most-notorious-hacking-groups/

[45] Psu.edu [online]. [cit. 2016-05-03]. Dostupné z: https://wikispaces.psu.edu/display/IST432TEAM4/Theft+and+Cybercrime+in+Virtual+Worlds

[46] Inflow.cz [online]. [cit. 2016-05-03]. Dostupné z: http://www.inflow.cz/virtualni-zlocin-kyberkradez-kybervrazda-kyberznasilneni-cast-i

[47] Inflow.cz [online]. [cit. 2016-05-03]. Dostupné z: http://www.inflow.cz/virtualni-zlocin-kyberkradez-kybervrazda-kyberznasilneni-cast-ii

[48] Zakonyprolidi.cz [online]. [cit. 2016-05-08]. Dostupné z: http://www.zakonyprolidi.cz/cs/1961-141

[49] Archive.org [online]. [cit. 2016-05-15]. Dostupné z: https://archive.org/details/available-on-itunes-logo

[50] Narod.ru [online]. [cit. 2016-05-15]. Dostupné z: http://money-pix.narod.ru/E/Europe/Security/20a.jpg

[51] Cybersecurity.cz [online]. [cit. 2016-05-25]. Dostupné z: http://www.cybersecurity.cz/data/pozar3.pdf

[52] Jobs.cz [online]. [cit. 2016-05-15]. Dostupné z: http://csas.jobs.cz/wp-content/themes/default/images/logo_share_1500.png

[53] Uab.edu [online]. [cit. 2016-05-15]. Dostupné z: https://www.uab.edu/dining/images/NewLogos/starbucks_hz.png

[54] Fio.cz [online]. [cit. 2016-05-15]. Dostupné z: http://www.fio.cz/o-nas/media

[55] Adstage.io [online]. [cit. 2016-05-15]. Dostupné z: http://blog.adstage.io/wp-content/uploads/2014/07/facebook-logo.png

[56] Novinky.cz [online]. [cit. 2016-05-15]. Dostupné z: https://media.novinky.cz/218/512184-original1-urqns.jpg

[57] Policie.cz [online]. [cit. 2016-05-15]. Dostupné z: http://www.policie.cz/statistiky-kriminalita.aspx

[58] Britainfirst.org [online]. [cit. 2016-05-15]. Dostupné z: https://www.britainfirst.org/wp-content/uploads/2015/08/TWITTER-1.jpg

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

TZ Trestní zákoník

TŘ Trestní řád

DNS Doménové adresy

SEZNAM OBRÁZKŮ

obr. 1: Logo iTunes Store [49] 19
obr. 2: Bezpečnostní prvky Euro bankovky [50] 20
obr. 3: Trestní oznámení 41
obr. 4: Logo České spořitelny [51] 48
obr. 5: Logo Starbucks [52] 51
obr. 6: Logo Fio banky [53] 52
obr. 7: Logo Facebook [54] 53
obr. 8: Donald Trump [55] 54
obr. 9: Logo Twitteru [57] 55

SEZNAM TABULEK A GRAFŮ

Tabulka 1: Zařízení a digitální důkazy 45

Graf 1: Struktura počítačové kriminality v roce 2015 56
Graf 2: Počet počítačových zločinů v roku 2011 - 2015 57
Graf 3: Útoky počítačové kriminality 58