Odhalování počítačové kriminality

Detection of computer crime

Jan Mrázek

Bakalářská práce 2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

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

Jméno a příjmení:	**Jan MRÁZEK**
Osobní číslo:	**A08359**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Odhalování počítačové kriminality**

Zásady pro vypracování:

1. **Práci zpracujte jako edukační materiál pro výuku v předmětu Kriminalistické technologie a systémy.**
2. **Charakterizujte základní způsoby páchání počítačové kriminality.**
3. **Popište druhy neoprávněných přístupů k datům a jejich následky.**
4. **Charakterizujte pachatele této trestné činnosti a jejich motivy.**
5. **Naznačte prevenci před počítačovou kriminalitou pro potřebu soukromých bezpečnostních složek.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **PORADA, V, a kol.: Kriminalistika. Brno : CERM, 2001. ISBN 80-7204-194-0.**
2. **STRAUS, J, a kol.: Kriminalistická metodika. Plzeň : Aleš Čeněk s.r.o., 2006. ISBN 80-86898-66-0.**
3. **MUSIL, J; KONRÁD, Z; SUCHÁNEK, J.: Kriminalistika. Praha : C.H.BECK, 2001. ISBN 80-7179-362-0.**
4. **SMEJKAL, V., SOKOL, T., VLČEK, M.: Počítačové právo. Praha: C. H.BECEK, SEVT, 1995 .ISBN 80-7049-101-9.**
5. **ŠIMOVČEK, I., a kol.: Kriminalistika. Bratislava : Akademia policejného sboru, 1999. ISBN 80-85981-117-5.**

Vedoucí bakalářské práce: **Ing. Petr Skočík**
Ústav elektroniky a měření

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **25. května 2012**

Ve Zlíně dne 24. února 2012

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Cílem této bakalářské práce je seznámit čtenáře s problematikou počítačové kriminality a rozdílem mezi jednotlivými typickými útoky pachatelů. Vysvětleny jsou zde i jednotlivé způsoby, kterými se pachatelé dopouští počítačové kriminality, která je označována za trestní čin. Část práce je zaměřena na rozdělení, popsání typů pachatelů a je i doplněna statistickými údaji a prevencí, jak se vyvarovat počítačové kriminalitě.

Klíčová slova:

Počítačová kriminalita, autorské práva, trestné činy, druhy počítačové kriminality, bezpečnost, počítačové útoky, hacking, cracking, prevence.

ABSTRACT

The goal of this bachelor's work is introduction of the problem with computer criminality and differences between typical offender's attacks. This work also explains individual methods how offenders commit computer criminality. In this case we can talk about crime. A section of this work is focused on separation, description of offender's types, statistic data and prevention of avoiding computer criminality.

Keywords: computer criminality, copyright, crime, types of computer criminality, security, computer attack, hacking, cracking, prevention

Poděkování

Chtěl bych na tomto místě poděkovat svému vedoucímu práce, panu Ing. Petrovi Skočíkovi, za jeho velmi cenné rady a veškerý čas, který mi věnoval při zpracování této práce a vedl mě tím nejlepším směrem.

Další velké díky patří celé mojí rodině, která mě podporovala po všech stránkách a dodávala mě hodně energie při psaní této práce.

V poslední řadě musím taky poděkovat svým zaměstnavatelům a kamarádům, kteří mě vždycky povzbudili, když to bylo nutné.

Diogenes

„Kdo toho hodně sní, není zdravější než ten, kdo sní, co potřebuje, a stejně nelze pokládat za vzdělance toho, kdo toho přečetl nejvíc a kdo se nejvíc naučil, ale kdo přečetl a naučil se věci užitečné.“

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně dne 25.5.2012 …….…….

podpis diplomanta

OBSAH

ÚVOD

Má práce bude pojednávat o problematice v počítačové kriminalitě. V dnešní době je počítač součástí prakticky každé domácnosti. Narazit můžeme taktéž na lidi, kteří počítač doma nemají a myslí si, že s počítačovou kriminalitou se vůbec nemůžou setkat, ale opak je pravdou. Ať už jde člověk v dnešní době kamkoliv, narazí na každém místě minimálně na jeden počítač. Počítač dokáže v dnešní době řídit prakticky náš svět. Za pomocí počítačů si člověk šetří nejen práci, ale slouží v každém oboru pro dobrou věc. Stejně jak nám je počítač prospěšný a vidíme na něm převážně jen ty klady, tak narazíme taky i na zápory, které se snažíme za každou cenu přehlížet. Jde o napadení počítače nebo data v něm uložené ať už přímo na daném počítači nebo za pomocí počítače.

Téma odhalování počítačové kriminality jsem si vybral z důvodu každoročního zvyšování počtu trestních činů, které budí pozornost ve společnosti. Můžeme toto téma označit za problematiku, kterou veřejnost sleduje a budí u nich patřičné obavy. Odhalování počítačové kriminality není tak jednoduché jak u jiných kriminalit, protože pachatelé mají anonymní identitu, která se velice obtížně odhaluje a tak je policie často krátká aby dopadla pachatele a následně jej mohla usvědčit ze spáchaného trestního činu.

Preventivní opatření proti počítačové kriminalitě většina lidí zanedbává, což vede ke zvyšování počtu spáchaných těchto trestních činů. Při nedostatečné prevenci přímo napomáháme těmto pachatelům a následně pozorujeme následky. Z finančního pohledu není prevence až tak nákladná, aby si ji lidé nebo firmy nemohli dovolit. Mnohdy i malá investice do levných softwarů je dostačující, přitom jde o částku, která se nejčastěji platí na rok. Pomocí prevence nejen ztížíme pachatelům přístup, ale taky pachatele často odradíme od těchto útoků.

I. TEORETICKÁ ČÁST

1 POČÍTAČOVÁ KRIMINALITA

O počítačové kriminalitě můžeme v dnešní době slyšet na každém rohu. Počítačová kriminalita se rozvíjí závratnou rychlostí stejně jako informační a telekomunikační technologie. Počítačovou kriminalitu bychom měli hlavně dělit podle toho, jestli je daný počítač připojen nebo nepřipojen k internetu, který se stal v dnešních domácnostech nepostradatelným prvkem. V této vyspělé době,se jeví domácnosti bez internetu jako nemoderní, i když díky možnosti nepřipojení se k internetu jsou jejich počítače, pokud je zrovna vlastní, neporovnatelně bezpečnější než počítače, které jsou připojeny k internetu a nabízí tak velké možnosti pro páchání trestních činů přes internet nebo přes vlastní počítač. Stejně jak se vyvíjí náš život, tak se vyvíjí taky internetový svět, který nazýváme virtuálním světem a mnozí z nás v něm žijí i svůj virtuální život. Každý z nás má tajemství v obou světech a určitě by byl nerad, aby jeho tajemství a další jiné osobní věci mohl znát každý člověk připojený k internetu kdekoliv na světě. Proto je nezbytnou nutností být opatrný k údajům, které zveřejňujeme nejen o sobě ale také o svých blízkých aby nebyly později jakkoliv zneužity.

Přesná definice počítačové kriminality, na které se dohodnuly státy Evropské Unie a Evropského parlamentu zní následovně:

„Jsou to nemorální a neoprávněná jednání, která zahrnují zneužití údajů získaných prostřednictvím informačních a komunikačních technologií.“ [1]

Obrázek 1 – Počítačová kriminalita

1.1 Rozdíl mezi počítačovou a kybernetickou kriminalitou

V literaturách nejčastěji narazíme na dva různé názory od autorů. Při studování této literatury jsem se často setkával s názorem, že počítačová a kybernetická kriminalita jsou totožná. Určitě záleží na tom, z jakého pohledu se na to člověk v danou chvíli dívá a jakou literaturu s touto nebo případně podobnou problematikou právě dočetl. Zastávám názor, že se nejedná o stejnou problematiku. Přikláním se k názorům, které tvrdí, že kybernetická kriminalita je pouze určitá část počítačové kriminality. Jde o část, která se odehrává v internetovém světě a patří sem celá řada trestních činů, která se odehrává pomocí internetu.

1.2 Pojem počítačová kriminalita

Pojem počítačové kriminality není přesně vymezený, protože neexistuje jednotná definice pro tento trestní čin. Důvodem proč vymezení této problematiky je složité, se stal rozvoj informačních technologií a jejich neustálé používání i při běžných činnostech. Vystačit si s obecným vymezením, kdy počítačová kriminalita je protiprávní jednání, která je spojována s počítačem nelze. Nutné je myslet i na to, že počítač může byt cílem pachatele nebo za pomocí počítače může být tento trestní čin páchán. Pachatelův čin je spojen s výpočetní technikou. [5] [31]

1.3 Typické útoky počítačové kriminality

1.3.1 Trestné činy porušující soukromí

Jako soukromí se v tomto trestním činu bere důvěrnost, dostupnost nebo taky formu uložení počítačových dat a operačních systémů. Do této trestní činnosti spadá:

- Narušování dat
- Narušování systémů
- Nezákonný přístup
- Nezákonné odposlouchávání
- Zneužití prostředků

Mezi odposlouchávající a sledovací druhy patří např. carding, hacking, phreaking, sniffing, sparing apod.

a) Carding

Pod tímto názvem se nemůže schovávat nic jiného než zneužití platební karty. Od doby co karty vznikly, tak zaznamenaly během posledních 10let velké rozšíření mezi lidmi a tak se tento trestní čin stává čím dál rozšířenější. Mezi nejlehčí zneužití platební karty patří zaručeně její odcizení nebo také krádež čísla platební karty. Mezi nejnovější metody zneužívání platebních karet patří tzv. „skimming“ což znamená kopírování platebních karet pomocí speciálního zařízení. Přístroj je nutné vložit přímo do zařízení bankomatu a tam snímá informace při zasouvání karty do bankomatu. Nezbytnou součástí při tomto činu je také kamera, která musí zachytit pin kód, který majitel platební karty zadává pro přihlášení na účet.

Obrázek 2 – Platební karty

b) Hacking

Činnost, která se provádí v síti internetu a může být opět legální nebo nelegální. S legálním hackingem se můžeme setkat vyjimečně, když si člověk zkouší nabourávat vlastní počítač nebo server. Nelegální hacking je již kapitola sama o sobě, kdy si pachatel zvolí cíl, ze kterého se pokouší získat či odcizit informace nebo data k zneužití. První myšlenka při stvoření hackingu nebyla za úmyslem poškodit systém, ale naopak poukázat na chyby v bezpečnosti systému a případně k odstranění těchto chyb. Slovo hacking tedy znamená proniknutí do systému jinou cestou než normálním přihlášením ale zároveň se dostává za rámec bezpečnosti napadeného systému. [19]

c) Phreaking

Tímto pojmem nazýváme činnost, která není přímo definována. Dochází k zneužívání telekomunikačních služeb, aniž by došlo k zaplacení této služby. Jedná se o případy, kdy osoby neoprávněné užívají telekomunikační služby lidí, kteří o tom vůbec nevědí do doby, než jim dojde účet za tyto služby, které musí uhradit. Zpočátku se jednalo o nabourání do telefonních linek, které umožňovalo bezplatné volání do kterékoliv části země, v závažnějších případech odposlouchávání některých telefonních hovorů. Později však došlo k nabourávání počítačových systémů prostřednictvím těchto telekomunikačních prostředků. [2] [17]

d) Sniffing

V překladu sniffing znamená čichat nebo šňupat. Jedná se o činnost, kdy komunikace na internetu je monitorována subjektem, který není adresátem této komunikace. Tento subjekt získává důležité informace, které mu následně slouží k páchání dalších trestních činů. Převážně jde o e-maily, hesla, soubory atd., které pachateli napomáhají například k průniku do cizího systému nebo také k získání financí z cizího účtu. Proti těmto neoprávněným zásahům se lze bránit pomocí šifrování elektronické komunikace. Záznamy o provozu sítě a ostatní záznamy umožňující identifikovat osobu jsou chráněny podle telekomunikačního zákona a zákona na ochranu osobních údajů. Správce sítě může tyto údaje poskytnout pouze PČR (Policii České Republiky) nikoliv však třetím osobám aby nedošlo ke zneužití. [2] [18]

e) Spamming

Spamming je nevyžádané masově šířené sdělení (nejčastěji reklamní) pomocí internetu. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging. [3]

Mezi charakteristické znaky spammingu nepatří pouze hromadný charakter zprávy ale také její nevyžádaná složka. Lidé, kteří tento spam rozesílají, se nazývají spameři a jsou mezi uživateli internetu velice neoblíbení. V tuto chvíli existuje nespočet programů, které tuto nevyžádanou poštu dokážou filtrovat, ale bohužel i spameři si najdou cestičky, jak tyto bezpečnostní programy obejít aby svůj cíl zasypali spamem.

f) Jiné druhy odposlouchávání a sledování

Mezi jiné druhy odposlouchávání a sledování patří průmyslová špionáž, která se dělí na:

- Legální – Tuto průmyslovou špionáž provádí převážně skupina zaměstnanců, kteří mají za úkol shromažďovat veškeré legální informace z článků, časopisů, novin a různých prezentací o jejich konkurenci a tak vykonávat legální odposlouchávání nebo sledování konkurence.
- Nelegální – Tyto informace je možné získat mnoha metodami za účelem získání nových technologií nebo potřebných informací o činnosti případného soupeře na trhu.

g) **Elektronická pomluva, msta, útoky na čest**

Pomluva je jeden z nejstarších trestních činů nejen u nás. S vývojem informačních technologií dostala nový rozměr. Tohoto trestního činu se může dopouštět každá osoba, ktera má přístup k internetu ať už doma,v práci nebo v internetových kavárnách kam může dnes opravdu každý člověk. Kromě jednoduchosti tohoto činu jde spíše o anonymitu jednání, kterou pachatel využívá. Mnozí lidé, kteří tento čin spáchají, si neuvědomují, že i když tento čin páchají anonymně, tak můžou být zjistitelní nebo postižitelní, ale opak je pravdou. Každý trestní čin se trestá, ať jde i o „pouze“ elektronickou pomluvu. Pokud podáváme zkreslené nebo nepravdivé osobní údaje můžeme poškodit jak vlastní osobu, tak osobu v profesním životě, která může vést až k nenapravitelným útokům na čest, pomluvám a nenávratném úsudku o poškozeném člověku.

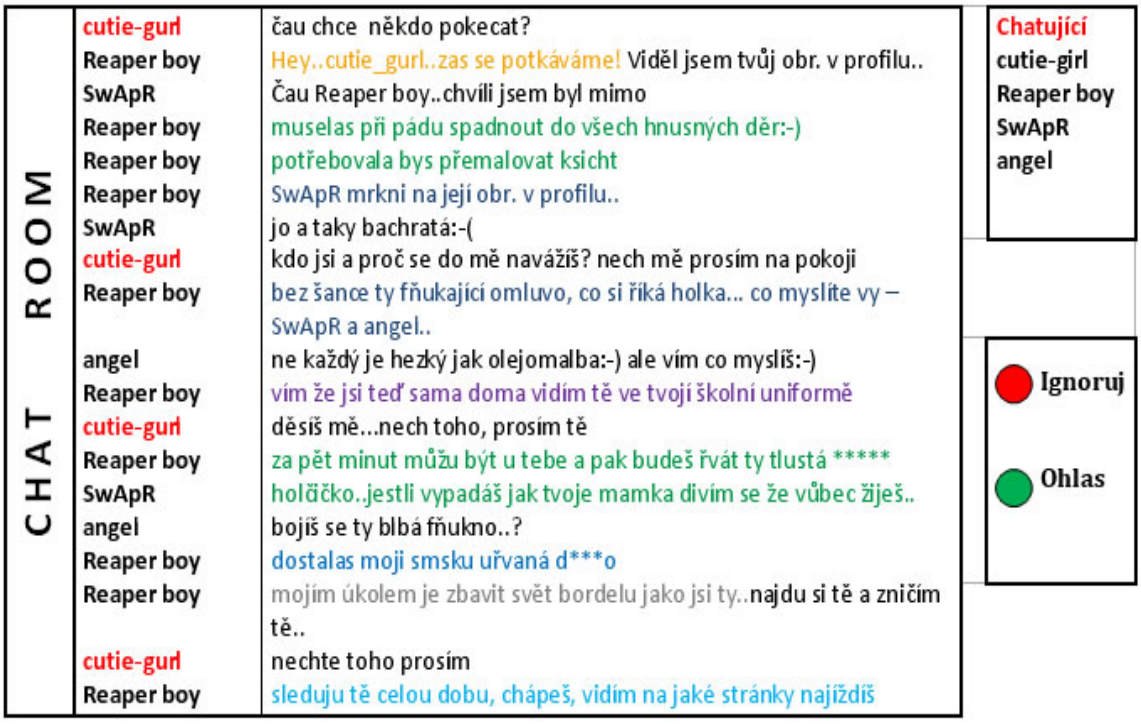
h) **Hoax**

Hoax překládáme nejčastěji jako falešnou a poplašnou zprávu, která se nešíří samovolně ale skrytě jako počítačové viry nebo trojské koně. Nejčastěji jde o žerty, poplašné zprávy, novinářské kachny nebo podvody které se šíří pomocí e-mailů. Nejbezpečnější formou hoaxu je pro uživatele kategorie podvodů, které mají za cíl vylákat od uživatelů za každou cenu peníze za různé služby, zboží nebo také pomoc. Hoaxy nás dokáží vždycky zaujmout, ať už jde o neuvěřitelný objev, nepublikovaná novinka, mediální zpráva. Často se také můžeme setkat s tím, že hoax obsahuje i výzvy k dalšímu rozeslání mezi přátele, popřípadě další uživatele. [15]

i) Cyberstalking

Tímto jevem označujeme zneužívání online komunikace k nabízení nepožadovaných služeb a věcí, virtuální pronásledování, obtěžování a zastrašování vybraných uživatelů nebo jejich blízkých osob pomocí internetu. Toto pronásledování se bere jako úmyslné, zlovolné pronásledování a obtěžování jiné osoby, které snižuje kvalitu života jejího nebo osobám jim blízkým. Cyberstalking snižuje kvalitu života a ohrožuje bezpečnost. [12]

Cyberstalking může zahrnovat zasílání nevyžádaných e-mailů a zpráv (které obsahuje pro adresáta nepříjemný obsah), posílání zpráv prostřednictvím chatů a blogů, různé způsoby šíření pomluv prostřednictvím internetu, posílání spamů a další různé druhy útoků zasahující počítač oběti nebo osobám jim blízkým. [12]



Obrázek 3 - Typický příklad chování při cyber stalkingu [12]

Stupeň 1: Chování	Motivace
- Pronásledování a trvalé zaměření se na jednotlivce online, tj. nejméně při dvou a více příležitostech. - Nabádání ostatních, aby zastrašovali a uráželi oběť. - Nazývání jménem a nechtěné a/nebo oplzlé pokusy o sblížení. - Zastrašující nebo obtěžující chování. - Může zahrnovat vyjádření emocionálních nebo hrubě vyjádřených názorů ve formě osobního napadení. - Urážky a posměch chatující oběti se může rozšířit na e-mail, mobilní telefon a pravděpodobně i do skutečného světa. - Vyhrožování vyhledáním oběti ve skutečném světě. - Může zahrnovat pokusy o zničení počítače zasláním škodlivého programu do počítače oběti, např. počítačového viru.	- Jedinec může věřit tomu, že si získá věhlas mezi chatujícími účastí v těchto aktivitách a tímto chováním. - Může považovat tyto aktivity za jakýsi druh sportu a často si zvolí jednoduché „cíle“, které poníží a tím vyvolá ještě větší strach. - K zastrašení a kontrole oběti. - Kontrolní cvičení využívající způsoby, jak naplánovat kontakt s obětí. - Snaha o vyvolání strachu u oběti – dává jednotlivci pocit síly a moci. - Maximální množství kontroly nad obětí, vštěpující maximální strach.

Obrázek 4 – Ukázka chování a motivace spojené s cyber stalkingem. Barevné oblastí v této tabulce se vztahují z komunikace v Obrázku 1 výše. [12]

j) **Padělání**

Padělání se rozšířilo spolu s rozvojem informačních technologií. Tuto trestní činnost jsem zmínil v počítačové kriminalitě, protože k padělání dochází za pomoci počítačového hardwaru a softwaru, které napomáhají k dokonalejším padělkům.

Nezákonná činnost, při které dochází k vytváření nelegálních kopií, které jsou od originálů skoro k nerozeznání. Jedna z mnoha možností kdy dochází k počítačové kriminalitě za vidinou zisku.

Padělání listin, bankovek a jiných veřejných listin bylo dřív poměrně složitou záležitostí. Postupem času jak se rozvíjela výpočetní technika a rozvíjela se neskutečnou rychlostí a modernizací, se stávalo padělání podstatně jednoduší, neboť sebou přinesla kvalitní grafické programy, kvalitní technologie tisku ale také i softwary, které zdokonalovali padělky k jejímu, čím dal menšímu rozeznání. [8]

Na druhou stranu nemohli zůstat pozadu ani pravé bankovky a jiné důležité dokumenty. Bylo nezbytně nutné opatřit bankovky různými ochrannými prvky, které nejen že

znemožňují, ale také ztěžují jejich padělání a tak snižují druh této kriminality. Mezi ochranné prvky bankovek patří například: [9] [10]

- Vodoznak – Značky nebo obrazce viditelné pouze proti světlu. [10]

Obrázek 5 - Vodoznak

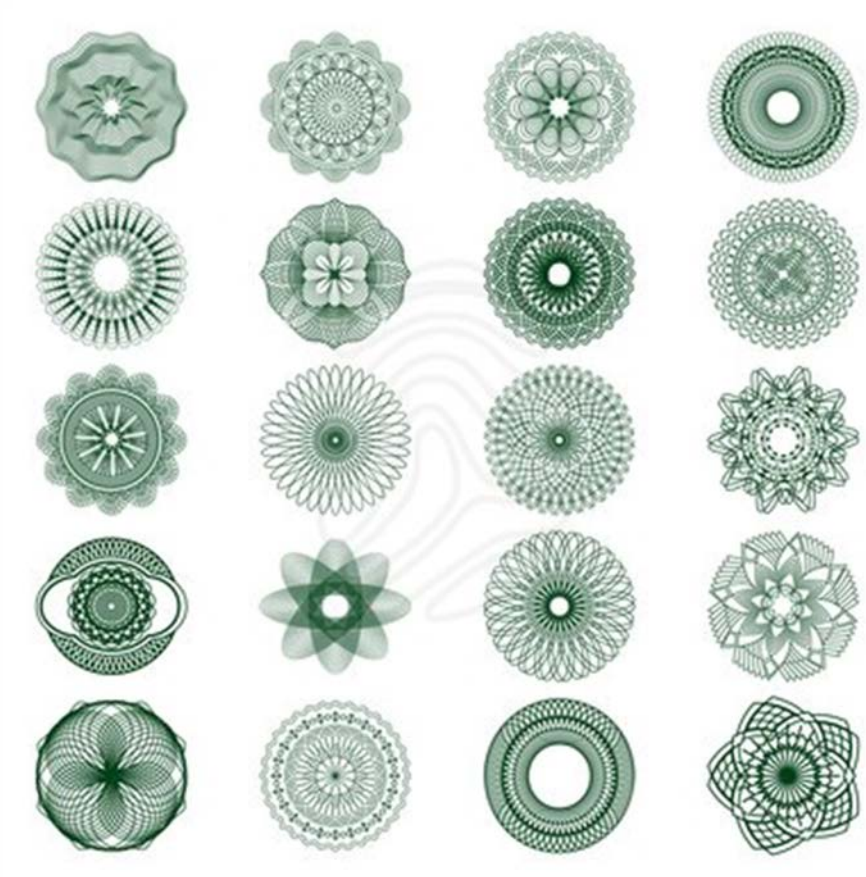
- Ochranný proužek – Plastový proužek, který je buď pokovený nebo kovový. Proužek často obsahuje i mikropísmo nebo hologram. Ochranný proužek je hodnocen jako vyšší stupeň ochrany. [10]

Obrázek 6 – Ochranný proužek

- Papír – Nejhmotnější část bankovek, určený k potisku. Samozřejmostí jsou náročnější požadavky než na obyčejný konzumní papír. Od obyčejného papíru se liší silou, strukturou a zabarvením. Musí mít tento papír větší pevnost a pružnost, odolnost při přehýbání nebo natržení. [10]
- Číslování a sériování – Slouží k tomu aby dvě bankovky neměly stejné číslo. Tímto se zhoršují podmínky pro padělání bankovek ofsetovým tiskem. [10]

Obrázek 7 – Číslování a sériování bankovek

- Giloš – Složitý obrazec, který se skládá ze spojitých jemných linek a uspořádání se opakuje v pravidelných intervalech. Dříve se tiskly gilošérce. Dnes se tvoří pomocí softwaru. Při kopírování na domácích kopírkách dochází k rozrušení na jednotlivé segmenty, kde jsou vidět mezery mezi jednotlivými úseky. [10]



Obrázek 8 – Giloš

- Hologram – Ochranná kovová fólie, na níž můžeme vidět vypálen laserem určitý motiv. Často obsahují mikro prvky ve formě mikro písma, nebo grafické obrazce. Jde o moderní způsob ochrany, který je nenapodobitelný v domácích možnostech. Můžou být nalepeny nebo vyraženy, buď po celé jejich délce nebo kusově. [10]

Obrázek 9 - Hologram

- Soutisková značka – Průhledná značka, která se skládá z obrazce, který je rozložen na obě strany. Z jedné strany je vidět jedna část značky a na druhé straně je viditelná zbylá část. Při pohledu proti světlu vidíme tento obrazec jako kompletní obrazec. Při padělání soutiskové značky dochází k nekompletnímu obrazci, který se rozchází a není tak jasně čitelný. [10]

Obrázek 10 – Soutisková značka

k) **Neoprávněné nakládání s osobními údaji**

V současné době má každý z nás svůj vlastní e-mail a ne jeden, inzerát na různých seznamkách, programy pro internetovou komunikaci (MSN messenger, AIM, ICQ, Skype, Jabber, Qip, Trillian, Miranda), profily na sociálních sítích (Lide, Facebook, Badoo nebo Libimseti), píší si vlastní blogy o sobě nebo se také účastní různých internetových diskuzí. Lidé si při vytváření a používání těchto programů a stránek neuvědomují, že po vyplnění na těchto stránkách a programech jsou jejich osobní údaje snadno zneužitelné a jsou k dispozici celé široké veřejnosti. Jde teda o nechráněné a nezabezpečené údaje, které jsou pro pachatele snadnou kořistí pro páchání trestního činu. Každý uživatel internetu by si měl uvědomit, co všechno na internetu poskytuje za osobní údaje, co všechno sdílí dalším

uživatelům, které vůbec nezná a jestli nejsou tyto údaje dosti citlivé, že by mohli v budoucnu jakkoliv poškodit jeho nebo osobu jemu blízkou.

1.3.2 Trestná činnost související s obsahem

Rozvoj informačních technologií a internetu umožnil nejen rozhled lidem v různých oblastech, ale také značnou mírou se zapsal i v trestné činnosti. Zmínit určitě musím šíření závadného obsahu ať už jde o šíření pornografie nebo extremismu.

a) Závadná pornografie

Označení této problematiky se zaměřuje na šíření závadné pornografie, ve které se projevuje násilí nebo neúcta k člověku. Může také popisovat, zobrazovat nebo jinak dokazovat pohlavní styk se zvířetem a v poslední řadě taky nejzávažnější problém posledních let, kterou se stala dětská pornografie. V dřívější době byl tento problém hodně omezený až do doby, než vznikl internet, který dopomohl k velkému rozšíření mezi veřejností. Šíření pornografie dřív probíhalo převážně pomocí časopisů a videokazet. Znovu tady hraje velkou roli internetová anonymita, která napomáhá tomuto trestnímu činu. Velkou sledovatelnost má v posledních 10 letech, kdy se objevuje tato problematika čím dál častěji. Hlavně díky velkému vývoji výpočetní techniky a hodně častému používání internetu mezi uživateli. [20]

Nejen u nás ale také ve světě se stala dětská pornografie nejvíce diskutovatelným tématem, které je označeno za nejzávažnější problematiku. V článku 9 Úmluvy o počítačové kriminalitě musí byt trestně postihováno nabízení, zpřístupňování, šíření, posílaní dětské pornografie prostřednictvím počítačového systému a výrobu dětské pornografie za tímto účelem a konečně taky obstarávání a držení. V úmluvě je také vytvořena vyjimka, kdy nejsou trestáni lidé, kteří drží nebo získávají dětskou pornografii pro vlastní potřebu nebo pokud v ní není zobrazena osoba, která vypadá pouze jako dítě nebo zobrazuje neexistující dítě. Právní úprava v České Republice jde nad rámec Úmluvy, kdy i samotné držení je nezákonné. [21]

b) Extremismus

Komunikačním prostředkem a ideálním místem pro extremistické skupiny se stal internet. Naleznout zde můžeme velké množství extremistických hnutí (pravicové, levicové, náboženské skupiny a jiné). Právě internet je místem kde tyto skupiny dostali možnost veřejně se prezentovat a ukazovat své názory, publikovat, účastnit se internetových diskuzí

a celkově ukazovat svoje myšlení a ideologii. Pomocí internetu tyto skupiny mezi sebou komunikují a navazují kontakty s jinými skupinami ať už u nás nebo v zahraničí.

Rozvoj informačních technologií, resp. internetu, tedy určitě znamenal i rozvoj extremismu. Čím dál víc se názory těchto skupin stávají dostupnější pro každého s přístupem k internetu a mají možnost se zapojit nejen ke konverzaci ale taky k nejbližší skupině v blízkosti jeho bydliště. Stejnou možnost mají i extremistické skupiny, které mají vyhledávání nových členů daleko jednoduší pro případné přijetí. Propagace a šíření těchto informací na internetu není vůbec nákladné, což je pro autory nebo vedoucí skupin velkou výhodou. Největší výhodou a hlavním důvodem, proč se spousta lidí zapojuje do diskuzí a vyjadřování svých extremistických myšlenek pomocí internetu je anonymita, kterou všem uživatelům internet poskytuje. Člověk po napsání svých myšlenek a názorů je těžko dohledatelný. [14]

Všichni tito extrémisté nepatří do běžné společnosti. Z důvodu, že se jedná o velkou řadu uživatelů, mělo by se toto chování sledovat a rázně trestat.

1.3.3 Trestné činy se vztahem k počítači

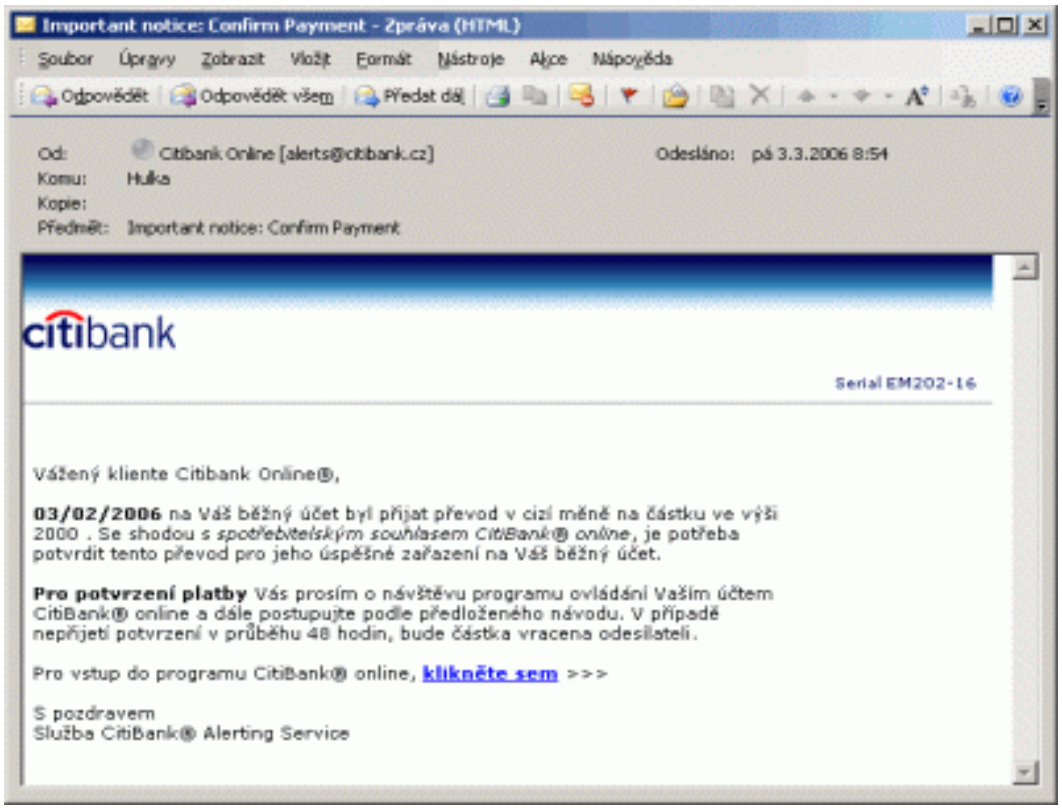
a) Podvod a zpronevěra

Prostřednictvím internetu se stal podvod a zpronevěra velmi dobrým nelegálním zaměstnáním, na které člověk narazí na každém kroku. Setkat se můžeme s celou řadou nabízení neexistujících služeb, ať už jde o práci nebo falešné obchody. Jednu velkou věc mají všechny tyto věci společné a to, že pachatelé od obětí vylákají peníze za účelem dalšího výdělku nebo nějaké služby ale oběť tohoto podvodu už u většiny případů peníze nikdy nedostane zpátky.

b) Phising

Podstatou metody, usilující o zcizení digitální identity uživatele, jeho přihlašovacích údajů, čísel bankovních karet, účtů apod. za účelem jejich následného zneužití, je vytvoření podvodné zprávy, šířené obvykle elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy jsou převážně maskovány tak, aby co nejvíce limitovaly důvěryhodné odesílatele. Může jít např. o padělaný dotaz banky, jejichž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PINu pro kontrolu (použití dialogového okna, předstírajícího, že jde o okno banky – tvz. Spoofing). [3]

Žádná banka nemá důvod kontaktovat své zákazníky pomocí e-mailu s odkazy na formulář s vašimi důvěrnými informacemi, i když logově, vzhledově případně graficky odpovídá e-mail důvěryhodně k vaší bance. Nemusí jít vždycky jen o e-mail z vaší banky, můžete narazit i na jiné organizace pracující s penězy jako je například PayPal, eBay, Skype atd.



Obrázek 11 – Případ Citibank [37]

c) Pharming

Mladšího bratříčka od Phishingu nazýváme Pharming, který je sofistikovanější metodou. Pachatel napřed hackuje DNS server, tj. server obsahující přiřazení doménových jmen jednotlivým IP adresám, a pozmění přiřazení tak, aby doménové jméno banky ukazovalo na jeho IP adresu, na níž se nachází podvržené stránky. Alternativně změní hosts file přímo v počítači oběti. Oběť tak nemůže pojmout podezdření z podvrženého odkazu jako při obyčejném phishingu. Pharming se tedy od phishingu příliš neliší, snad jen tím, že při něm navíc dochází k hacku (cracku) DNS serveru nebo počítače oběti. Můžeme tedy konstatovat, že se jedná o především nebezpečnější metodu. [3]

1.3.4 Další formy trestné činnosti

Mezi další formy počítačové trestné činnosti jsou i počítačové viry, které mají za úkol dostat od uživatele k pachateli veškeré důležité informace, jako jsou přihlašovací jména, hesla, čísla kreditních karet apod.

a) Backdoors

Po nainstalování programu na cílový počítač umožňuje jeho vzdálené řízení a to mnohdy pro opakované zneužití. Pomocí „zadních vrátek" jak se metoda často překládá je nebezpečná hlavně z důvodu, že umožňuje několikanásobné propojení tzv. řetězení počítačů. Backdoors na sebe neupozorňují a čekají na povel od pachatele. Pomocí řetězení je dopadení pachatele hodně náročné, protože se připojuje přes několik již už dřív napadených počítačů a tak se jeho odhalení znatelně komplikuje.

Základní požadavky na backdoor:

- Neviditelnost – uživatel se nesmí dozvědět o tom, že je program spuštěn
- Všestrannost – program se musí přizpůsobit podmínkám, jaké na daném počítači jsou (šifry, hesla, certifikáty apod.)

Zadní vrátka můžou být v programu zanechána úmyslně nebo se může jednat o pomůcku pro ladění programu, která jsou omylem zanechána i pro ostrou verzi, kterou používají uživatelé, kteří nemají žádné tušení, že by je někdo mohl napadnout. [4] [5]

Tato forma kriminality není žádnou novinkou a často můžeme na internetu narazit také na články, kdy např. vývojáři operačního systému Windows informují svět, že objevily zadní vrátka ve verzi, kterou dali k dispozici uživatelům, ale pomocí aktualizace tento problém opravili pro vlastníky legálních operačních systémů.

b) Souborové viry

Virus se aktivuje pouze po spuštění napadeného souboru. Tyto viry připojují nebo přepisují spustitelné soubory nebo také soubory obsahující spustitelný kód.

c) Boot viry

Jsou umístěné v boot sektoru diskety nebo na pevném disku počítače. Spouští se po zavedení systému z napadení disku. Jestli je virus spuštěn, může napadnout každou nechráněnou disketu proti zápisu, se kterou pracujeme na nakaženém počítači. Z diskety se

virus může dostat na pevný disk jen v případě zavedení systému z napadené diskety a to nemusí byt disketa pouze systémová.

d) Keylogger

Keylogger neohrožuje přímo počítač, jde o software, který snímá stisky jednotlivých kláves a zaznamenává je do souboru nebo je přímo odesílá pomocí internetu k pachateli, který daný software nainstaloval do počítače, aby získal potřebné údaje popřípadě data k páchání trestního činu. Tento software u antivirů bývá označován jako virus. USB keylogger je jeden z nejpoužívanějších a v době každodenního využívání USB flash disku se tato hrozba stává postrachem všech uživatelů, kteří používají počítač. Narazit na tento software může každý prakticky kdekoliv a kdykoliv. [6]

e) Spyware

Program, který pomocí internetu odesílá data z počítače k pachateli bez vědomí jeho uživatele případně majitele dat. Existuje ale i spyware odesílající k pachateli hesla a čísla platebních karet nebo spyware fungující stejně jako backdoor (zadní vrátka).

Jde o programy, které běží na počítači bez vědomí uživatele a různým způsobem jej poškozují nebo zhoršují jeho funkčnost. Většina antivirových programů spyware nenaleznou, proto je nutné použít antispyware a ne pouze jeden z důvodu, že každý spyware má různou databázi těchto škodlivých programů, takže by nemusel zrovna ten váš být ten pravý pro odhalení konkurenčního programu. [7]

Spyware rozdělujeme do 3 skupin podle toho, jak nám škodí:

- Adware – Uživateli vnucuje reklamu, ve většině případů jde o vyskakování nových oken s reklamou nebo reklamní proužky v prohlížečích. Pro uživatele je to velice nepříjemné a hlavně se zvyšují nároky na rychlost připojení. [16]
- Hijacker – Pomocí změn v registrech bez vědomí uživatele změní domovskou stránku nebo se přidá nežádoucí stránka mezi oblíbené stránky uživatele. Často se také stává, že domovská stránka nelze vrátit na naši původně oblíbenou. [16]
- Dialer – Dokáže změnit nastavení přípojení pomocí modemu, který přesměruje na zahraniční číslo s vysokou sazbou. Následně dochází k obdržení velkého účtu za telefon. Tyto programy se zejména vyskytují na porno stránkách a probíhá to pomocí stažení souboru, který místo videa obsahuje koncovku exe a po jeho

nainstalování dochází k okamžitému přesměrování. V dnešní době jde spíše o zastaralou metodu, která již nepatří mezi aktuální problematiku. [16]

f) Spam-server

Pomocí tohoto viru se mění napadený počítač na server, který slouží k rozesílání nevyžádané pošty nebo spamu na jiné počítače, aniž by o tom majitel počítače nebo jeho provozovatel měl nějaké tušení.

g) URL trojan

Jde o metodu, která infikovaný počítač přesměrovává na daleko dražší tarify internetu připojeného pomocí vytáčeného připojení.

S tímto virem se v moderní době nemůžeme setkat. Největší pohromu tento vir zaznamenal v době, kdy se na internet počítače připojovalo pomocí vytáčejícího připojení přes pevnou telefonní linku. Tento vir dokázal přesměrovat vytáčení připojení na dražší linku a tak člověk platil za internet daleko více než za normálních okolností.

h) Počítačový červ

Červi se můžou na rozdíl od virů šířit sami. Počítačový červ je zvláštním typem počítačového viru, který se šíří pomocí infikovaných souborů nebo paketů počítačové sítě. Tímto způsobem se červi množí a hlavně zahlcují internet. U většiny červů není nutné aby uživatel tento virus spustil, jelikož využívají bezpečnostní chyby existujících programů a tyto následně využijí k nabourání se do dalšího počítače. Počítačový červ funguje jako samostatná jednotka a samostatný proces, který nevyužívá hostitelský program ke svému zamaskování. Červi využívají nedokonalosti operačního systému a mají na svědomí zahlcení a neprůchodnost sítě. [11]

i) Trojský kůň

Skrytá část programu nebo aplikace s funkcí, se kterou uživatel nesouhlasí. Na uživatele se trojský kůň tváří užitečně (spořič obrazovky, hra nebo jednoduchý nástroj). Nejčastěji jde o erotické spořiče obrazovek nebo pornografii. Trojský kůň se může také vydávat za program odstraňující počítačovou nečistotu (viry, trojské koně), který je sice funkční ale odstraňuje pouze konkurenční nečistotu, kterou je počítač zasažen. Tato funkčnost slouží pouze jako maskování záškodnické činnosti, kterou v sobě trojský kůň ukrývá.

„V Microsoft Windows může trojský kůň využít toho, že řada programů včetně systémového správce souborů (exploreru) skrývá přípony souborů. Vypadá následně jako

soubor s obrázkem, zvukem, archivem nebo čímkoliv jiným, přestože se ve skutečnosti jedná o spustitelný kód. Chce-li uživatel obrázek kliknutím zobrazit, je ve skutečnosti spuštěn program (trojský kůň) o kterém majitel počítače nemá ani tušení, že ho on sám spustil, protože se problémy neobjeví ihned.“[13]

j) Útoky DoS a DDoS

Zkratka DoS (Denial of Service) v překladu znamená odmítnutí služby. Touto zkratkou jsou označovány všechny útoky, které mají za svůj cíl znemožnit přístup k síti, počítači nebo také službě. Pomocí tohoto neoprávněného útoku na počítač dochází ke snížení výkonu, vyřazení z činnosti a následnému zahlcení spojovací cesty dat díky nesmyslným požadavkům. Problematika DoS útoků je stále aktuální, i když si hodně uživatelů myslí, že je to právě naopak. Dříve se tyto útoky využívaly proti jakémukoliv počítači, nyní se využívají DoS útoky na slabé místa v jednotlivých programech. [22]

DoS útoky dělíme na:

- Lokální – nezbytnou nutností pro lokální útok je přímý přístup k počítači, na který chceme zaútočit
- Vzdálený – není potřebné mít přímý přístup k počítači, na který chceme zaútočit a lze tento útok provést i vzdáleně pomocí internetu nebo sítě.

Mezi DoS útoky patří například:

- Mass mailing list – Tento útok zaplaví vaši e-mailovou schránku. Hlavním úkolem tohoto útoku je zahlcení vaší schránky do stádia, kdy se stává nepoužitelnou. Po tomto útoku nepřichází do schránky žádné další e-maily, protože kapacita schránky je plná. V dřívější době to nebyl problém jelikož schránky měli velikost v řádech MB ale v dnešní době jsou schránky často mnohonásobně větší a někdy i neomezené. Jedinou možností je každodenní poslání tisíce e-mailů, aby bylo dosaženo stejného efektu. Útok je velice jednoduchý a nebezpečný. Dopadení pachatele je téměř bez šance. [22]
- E-mail bombs – Tento útok se dost podobná mass mailingu, který jsem rozebíral v předešlém bodě. Rozdíl u tohoto útoku je vytvoření e-mailu pomocí programu, které si generuje útočník sám a jejich množství záleží na něm samotném, kolik jich zrovna chce poslat. Při tomto útoku nemusí byt cílem pouze vyřazení nějakého e-mailu, ale může se stát, že cílem se stává přímo poštovní server, který chce pachatel

vyřadit z provozu. Pachateli v této době nejvíce pomáhá při tomto útoku fakt, že e-mailový server obstarává poštu, často taky kontroluje, jestli se nejedná o spam nebo zda nejde o nějaký virus. Tato funkce napomáhá pachatelům, protože pro odbavení jedné e-mailové zprávy je potřeba více procesorového času. Tento útok je velice snadný a nejvíce se používá jako osobní pomsta. [22]

- Fork bomb – Jméno tohoto útoku vzniklo pomocí funkce „fork()“, která spouští běžící program znova. Díky tomuto nekonečnému spouštění dochází k pádu systému nebo jeho zahlcení. Když vezmeme Fork bomb jako útok, lze konstatovat, že se jedná pouze o lokální útok. K provedení tohoto útoku dochází pomocí programů, které se sami pořád dokola pouštějí až do nekonečna. Jeho útok není nebezpečný díky omezenému použití na lokálním počítači, za to ale účinnost je stoprocentní. [23]

Stejně jako jiné viry, programy nebo aplikace se zdokonalují, dochází také ke zdokonalení DoS útoku a vydání nové verze, která je pojmenovaná skoro stejně jako předchůdce. Jde o DDoS (Distributed Denial of Service) útok který v překladu znamená distribuované odmítnutí služby. Tento útok může provádět jednotlivec pouze v případě, že má na to pachatel kapacity. Častěji se však stává, že útok provádí více lidí současně tzv. skupinově protože skupina dokáže vytvořit zátěž na serveru daleko snadněji, aniž by potřebovali takové kapacity k úspěšnému provedení útoku jako jednotlivec. DDoS útoky mají pouze jeden velký cíl a to zahltit server. Tento útok je možné využít nejen na server ale taky na e-mailovou schránku tím, že skupina lidí posílá do této schránky zprávy. DDoS útoky nejsou označovány za trestní čin ani za nelegální akt. Jde pouze o demonstrující vyjádření nesouhlasu pomocí tohoto útoku. [24]

1.3.5 Jednání porušující autorská práva

a) Warez

Označení pro obsah, při kterém dochází k šíření a odstraňují ochranné prvky autorských děl, včetně jejich používání, šíření a jiné nakládání v rozporu s autorských právem. Lépe řečeno, jde o používání, šíření a upravování softwaru, aniž by jsme za všechny jeho funkce zaplatily částku, kterou firma požaduje. [25]

Přímo s touto problematikou se můžeme nejvíce setkat na warez fórech, které jsou založena za účelem šíření warezu. Tyto fóra jsou určeny pouze pro diskuzi, ale obsahují taky sekce, ve kterých nalezneme textové odkazy, které nejsou klikatěné, aby si jej musel

každý uživatel zkopírovat do adresního řádku sám. Tímto se provozovatelé těchto serverů brání, jelikož neodkazují na servery, kde se sdílí různá data.

Jak to přibližně funguje, můžeme sledovat na obrázku níže, který tuto problematiku vystihuje a byl přepracován z původní verze.

Obrázek 12 – Jak funguje nelegální stahování dat [25]

b) Cracking

Cracking je odvozen od anglického slova „crack“ které v překladu znamená lámat. Můžeme tedy říct, že jde o metodu, která odstraňuje ochranné prvky softwaru, který je chráněn proti kopírování. K využití všech možností je nutné zadat sériový klíč, který získáme bez nutnosti zakoupení. U originálních her pomocí cracku mnohdy odstraníme kontrolu, zda je CD v mechanice. Lidé, kteří se vydají touto nelegální cestou, jsou nazýváni crackerama. Mnozí lidé si je pletou s hackery, přitom jde o zcela jinou a hlavně složitější problematiku. Ve většině zemí je problematika překonávání softwarových ochran nezákonná, protože software je chráněn autorským právem tzv. copyrightem. Takto upravený software se nazývá warez a většinou se šíří po internetu přes datové uložiště popřípadě P2P sítě. Vývojáři a programátoři se snaží crackování svého softwaru maximálně zamezit nejrůznějšíma technikami ale většinou i crackeři si najdou svoji cestu

jak i nepřekonatelné bezpečnostní prvky překonat, aniž by zaplatit za legální verzi. Při zakoupení legální verze nejen že platíme vývojářům za jejich práci, kterou museli vykonat, ale také přispíváme firmě pro její další rozvoj nebo vylepšení stávajícího programu. [27]

c) Cybersquatting

Cybersquatting znamená neoprávněné užívání nebo zaregistrování domény, která zní totožně s názvem známého projektu nebo firmy. Každý vlastník domény si zakládá na originalitě, nezaměnitelnosti jeho doménové prezentace a zaregistrování pouze pro něho jako jediného vlastníka. Převážně v podnikání je pro zákazníky důležité, aby doménové jméno bylo známé s konkrétní společností. Možná záměna domén s jinýma firmami, které se zabývají stejnou nebo podobnou činností, se může stát pro firmu velkým problémem při prodeji a prezentaci.

V podstatě se jedná o ukradení názvu domény, která se může stát atraktivní a pro mnoho společností představuje velký problém. Vykupují se oblíbená slova a registrují se jako domény a jejich hlavní cíl je prodej společnostem a vlastníkům ochranných známek za účelem vysokého zisku oproti původní nákupní cenně. Existují uz i aukční servery, kde je možné prodat název domény nejvyšší nabídce. Cybersquatting brání jiným osobám v plnohodnotném způsobu prezentace jejich firmy pomocí internetu, protože název firmy je již doménově registrován.

V této kriminality se můžeme v praxi setkat s několika podobami: [26]

- Držení domény či podobné s obchodním názvem firmy či ochrannou známkou jiné osoby a parazitování na její návštěvnost.
- Držení zaměnitelné domény s překlepem a parazitování na její návštěvnost
- Držení shodných či zaměnitelných domén s cílem blokovat jejich využití
- Předvídat určité skutečnosti s cílem z ní v budoucnu těžit. Jde typicky o registraci domén k budoucím událostem, jména kandidátů v různých soutěžích apod.

Všechny podoby, které má cybersquatting na internetu jsou činy, které by neměly zůstat bez povšimnutí. Převládá zde lidská vypočítavost, zlá víra, snaha vydělat si na úkor cizích nápadů nebo projektů. [26] [28] [29] [30]

1.4 Role počítače v počítačové kriminalitě

Počítač může figurovat v počítačové kriminalitě ve dvou funkcích. V první řadě může být počítač jako předmět, kdy pachatel pomocí počítače získá veškeré data z daného počítače nebo jen určitou část, kterou potřebuje k dalšímu použití a tím pádem k poškození vlastníka těchto dat nebo majitele počítače. Jde o nejčastější cíl pachatelů. Pokud je počítač využit jako nástroj, jde o velkou řadu různých metod jak pomocí počítače získat důležité informací z jiných počítačů nebo páchání různých trestních činů.

1.5 Nosič informací

Nosič informací je označováno zařízení nebo médium, na které dokážeme uložit data nebo informace a následně je z něho využít nebo přenést do jiného zařízení. Mezi nosiče informací patří následující zařízení nebo média:

- Diskety
- CD
- DVD
- Flash disky
- Pevné a přenosné disky
- Paměťové karty
- Čipy

Obrázek 13 - Média

1.6 Digitální stopa

Každý člověk, který používá internet ať už doma, v práci nebo kdekoliv jinde za sebou zanechává stopy, jak když jde po mokré půdě. Jsou to stopy, které zůstanou viditelné a tak je možné nás snadně sledovat. Na každém záporu najdeme i pozitiva a jinak tomu nebude ani u digitální stopy. V digitálním světě se pohybuje každý z nás a určitě si najde i svoje záliby v diskuzích, různých portálech ať už herních nebo novinkových, kde si vytvoří potřebný přístup aby měl daleko lehčí vyjadřovat svůj názor nebo si vybrat rubriky, které chce sledovat. Otázkou ale zůstává, jestli nám to stojí za to, aby naše digitální identita byla přístupná lidem z virtuálního světa a tak se mohli o nás dozvědět daleko více informací, než častěji chceme. [32] [33]

1.7 Digitální identita

Pojem identita má mezi lidmi různý význam. Pokud se díváme ale na virtuální svět, označujeme tuto identitu za digitální a mnohdy nepravdivou. Každý z nás má ve svém reálném životě nějakou identitu, kterou čím dál častě přenášíme i na svou digitální identitu. Mezi oběma světy se ale hodně věcí liší. V digitálním světě narazíme daleko více na

virtuální jedince, kterým při vyplnění své digitální identity podle reálné dáváme velkou možnost získat více informací, než by jsme chtěli prozradit. Prokázat totožnost v digitálním světě je daleko obtížnější při porovnání s reálným světem, kde je možnost si totožnost ověřovat pomocí osobních dokladů do kterých patří občanské průkazy, občanky a jiné doklady obsahující fotku s vaším příjmením. Lidé si při vyplňování profilů na různých seznamkách, sociálních sítích nebo fórech neuvědomují, že jejich digitální identita je snadným cílem pro pachatele, kteří odcizí vaši identitu a můžou ji zneužít na jiných stránkách, kde si zaregistrují vaší přezdívku daleko dřív než vaše maličkost a tím dochází k odcizení vaší digitální identity. Nutné při vyplňování vašich profilů a internetových účtů je nesmírně důležité se pořádně zamyslet, co opravdu chcete všem zveřejnit a jestli je to opravdu nutné zveřejnit veškeré vaše data a osobní informace. Mnohdy stačí tyto údaje vyplnit fiktivně aby jste se chránily před zneužitím, pokud internetovou identitu nevyužíváte pro práci a při nevyplnění správných údajů byste se mohli dostat do problémů. .[33] [34]

1.8 Copyright

Autorské právo, které chrání autorská díla a nároky jejich tvůrců po jistou zákonem stanovenou dobu. Při této ochraně, má právo rozhodovat jak bude s jeho dílem naloženo pouze jeho autor nebo osoba, kterou k tomu pověřil. Autor má hlavní slovo při rozhodování jestli bude dílo možné prodávat, půjčovat, pronajímat, sdílet na internetu, vystavovat, promítat nebo jinou metodou dávat k dispozici ostatním uživatelům. Copyright chrání konkrétní díla nikoliv myšlenky nebo ideje. To jestli je nějaké vámi sledované dílo chráněno autorským právem poznáte podle symbolu, kterým bývají tyto díla označovány. Mezi nejčastější tvůrce patří hudebníci, filmaři, spisovatelé, programátoři apod.

Obrázek 14 – Ochranná značka autorských děl

2 ZPŮSOBY PÁCHÁNÍ POČÍTAČOVÉ KRIMINALITY

2.1 Útok proti počítači

Tento útok není vedený proti počítači nijak fyzicky. Nejde o rozbití počítače pachatelem přímo na místě, kde se počítač nachází ba naopak. Počítač, který byl označený za cíl je napadený pachatelem na dálku a to za pomocí různých virů, softwarů nebo jiných podobných metod. Útok je směřován na cenné programové vybavení nebo uloženým důležitým datům. Můžeme tedy říct, že jde o kriminalitu, která se zaměřuje na sběr, přenos, uchování, zpracování a distribuci dat nebo informací, které se provádí za pomoci výpočetní techniky. Pachatel provádí útok za obohacení svojí nebo třetí osoby.

2.2 Útok proti programovému vybavení a datům

Pachatel si určil za cíl jen programové vybavení počítače a data, která jsou v tomto počítači uložené. Tento útok může být proveden několika způsoby. Jako nejjednodušší způsob tohoto útoku je smazání dat přímo z určeného počítače až po nakažení počítače virem do programového vybavení, které způsobí poškození nebo vymazaní programů a dat.

Informace nebo data, které jsou poškozené nebo i nenávratně smazány nelze finančně ohodnotit, proto vyčíslení vzniklé škody je prakticky nemožné. Určitou hodnotu mají tyto informace a data u vlastníka, který ví, jak obtížné bylo tyto data vytvořit nebo získat. Vzniklá škoda se může také skládat z nemožnění uzavření smlouvy na nějaký kontrakt, znemožnění realizace smluvně ujednané zakázky nebo plnění závazků vůči druhé stranně, kdy vše má na svědomí pachatel, který se dopustil trestního činu.

Protože každý útok na programové vybavení nebo útok proti datům je v každé situaci jiný, tím pádem není možné mít vypracovanou metodiku v této oblasti a tak se stává každý případ experimentem a zároveň i základem této problematiky. Po určení hodnoty dat pro vlastníka se soudní znalci překlápí do pozice badatelů, kteří probádávají nezmapované části této problematiky a mapují je. [35]

2.3 Počítačové pirátství

Je označováno taky jako softwarové pirátství, kdy pachatel bez řádného oprávnění od autora páchá trestní čin buď to kopírování programového vybavení, nebo pracuje na nelegálně získaném programu pro sebe nebo jinou osobu za viditelností finančního ohodnocení. Autorské práva se označují pomocí ochranné značky „©“. [42]

Činy, které provádí kdokoliv kdo: [35]

- Užívá programy zaměstnavatele pro své soukromé účely (většinou v domácnosti ale může se stát, že se tak děje i na pracovišti)
- Užívá nelegálně získaný program, který získal z pracoviště nebo datových hostingů
- Programy jsou používány na více počítačích, než je smluvně sjednáno
- Provádí změny, úpravy nebo zasahuje různě do programu
- Prodá nebo poskytne program třetí osobě
- Brání zaměstnavateli užívat program vytvořený zaměstnancem ke splnění povinností vyplývajících z pracovního poměru

2.4 Destrukční činnost prostřednictvím virů

Počítačové viry jsou malé programy, kdy běžný uživatel ani nepostřehne, že jeho počítač je jimi nakažen. Jejich schopností je samovolné rozmnožování při každém jejich spuštění a můžou napadat: [35]

- Určité programy, zpravidla soubory s koncovkou COM, EXE, (ale není to pravidlem), je nazýváme souborové viry
- Určité oblasti disku (např. BOOT sektor), pak je nazýváme boot viry
- Po spuštění je rezidentně uložen v paměti počítače po celou dobu jeho chodu, tyto viry označujeme jako rezidentní viry

Při každém spuštění nakaženého programu dochází k nakažení dalšího programu, který je v jeho blízkosti, pokud již tento program už nebyl nakažen. Nakažený program po nakažení virusem funguje jinak než byl měl, i když pro uživatele se tento program navenek chová stále stejně. Virus zasáhne v programu nejen obsah ale i sled informací, které změní a program provádí něco jiného, než dělal před jeho nakažením. [36]

Viry můžeme dělit:

- Neškodné – Nejčastěji neškodné viry provádí žertíky, které ale díky svojí nekontrolovatelnosti můžou přerůst, až velkému nakažení počítače kdy se stává tento vir škodným. Z neškodného viru se může stát i zákeřný vir ale naopak to nikdy nelze.

- Zákeřné – Tento typ virů má za cíl pouze jednu věc a to je uškodit za každou cenu. Je úplně jedno jestli dojde ke smazání dat nebo jestli dokáže poškodit hardware, že se stává nepoužitelný.

Oba tyto druhy virů jsou z pohledu uživatelů škodlivé a nevyzpytatelné. V žádném případě ale nejde o žádné fyzické násilí proti počítači nebo jeho vybavení.

Nejnebezpečnější viry pro společnost se stali logické útoky, nejen díky své razantnosti, ale taky kvůli slabinám počítačového systému, které pachatel zneužívá. Logické útoky můžeme také označit jako logické bomby, kdy dochází k jejich aktivaci až po splnění určitých podmínek. Může jít o určitou dobu kdy je tento virus spuštěn nebo také po spuštění určitého souboru dochází k jejich aktivaci a následně vykonávají činnost, kterou mají naprogramovanou. [44]

Důležitým bodem při zjištění pachatele který tento čin provedl se stává, jestli byl vykonán za určitým úmyslem či nikoliv. V případě že pachatel donesl do zaměstnání nějakou hru, která dokázala zavirovat počítač, aniž by o tom daný člověk věděl, můžeme bezpochyby označit toto jednání za neúmyslné. Paradoxně podle zákonného ustanovení jde o nepostižitelný čin, který má stejné následky jako při úmyslném zavirování počítače.

2.5 Zneužití výpočetní techniky pro osobní účely

Trestní čin, zneužívání výpočetní techniky pro osobní účely může byt páchán v práci na počítači, používání programu nebo komunikačního zařízení, které vlastní zaměstnavatel, který nedal pracovníkovi souhlas k soukromým účelům během pracovní doby. Tato trestní činnost spočívá v prodávání programů, které byly vytvořeny během pracovního poměru, aniž by o tom zaměstnavatel věděl.

Pachatelé tento čin páchají nejčastěji na úkor svých pracovních povinností nebo při splnění všech požadavků od zaměstnavatele. Počítač, na kterém pachatel pracuje během dne, je jim přístupný i po pracovní době, a to nevýdělečně i výdělečně. Nezbytnou nutností je tedy rozlišovat, jestli pachatel porušuje pracovní povinnosti, což vede ke zdokonalování zaměstnance, což je pro zaměstnavatele jediné pozitivum a označujeme to tedy za nevýdělečné neoprávněné užívání počítače. Druhá možnost je označována za trestnou činnost, kdy zaměstnanec porušuje vlastnická práva a výdělečně využívá počítač na pracovišti.

Mezi nejčastější pachatele tohoto trestního činu bývají označování specialisté na zpracování dat, systémoví programátoři apod. Pachatelé zneužívají cizí věci k zakázaným činům, ať už jde o používání mimo pracovní dobu nebo je věc vytvořena pro nevýdělečnou činnost během pracovní doby.

Každý zaměstnavatel, který má ve svojí firmě počítače by si měl se zaměstnanci stanovit, do jaké míry můžou využívat svěřený počítač. Jedině tato možnost může následně posloužit k rozeznání, zda se jednalo o oprávněnou nebo neoprávněnou manipulaci s počítačem. Mezi další faktory spadá určitě i možnost vyčíslení škody nebo možnostem užívání z čeho lze následně určit i míru páchání trestního činu. [43] [35]

Je nutné rozlišovat jednotlivé případy:

- Porušování pracovních povinností
- Porušování vlastnických práv
- Páchání trestního činu

Když jde o porušování ať už pracovních povinností nebo vlastnických práv může kdykoliv zasáhnout právě zaměstnavatel a udělat tak určité opatření aby měli možnost jeho zaměstnanci prostor pro soukromé realizace a tak si mohli zvyšovat kvalifikaci a dovednost při obsluze počítače. V případě že jde o trestní čin, měl by bez ohledu na vlastníka zasáhnout statní orgán, pokud se nejedná o dodatečně nezlegalizovanou činnost vlastníkem. V případech kdy jde o výdělečnou činnost, by měl být pachatel pokaždé stíhán za čin, který páchá.

2.6 Pronikání do počítačových systémů

Jak již je zvykem označovat lidi, kteří páchají trestní čin v této problematice pachateli, tak se při pronikání do počítačových systémů můžeme setkat i s tím, že pachatelé jsou označováni za hackery. Hackeři se snaží obejít bezpečnostní prvky informačních systémů a neoprávněně do něj proniknout. V zárodku tohoto činu je touha dokázat, že hacker je lepší než bezpečnostní systém, který jeho cíl používá.

Postih za proniknutí do zabezpečeného systému nepovolanou osobou je velice složité označovat za trestní čin, protože dokázat hackerovi, že měl v úmyslu dál využít data nebo informace ke kterým se dostal, je nemožné. Nutné je zjistit, jestli nebyly tyto data použité nebo se chystali k použití, což by vedlo k trestně právnímu postihu. Velká část těchto

hackerů tuto činnost berou jako zábavu pro svůj volný čas, kdy je jejich jediný cíl výzva překonat bezpečností prvky systému bez dalších úmyslů.

Úplně jiná situace vzniká, kdy hacker který vnikne do databáze pro něj zajímavé, vede jeho mysl k získání informací, které následně využije jako protihodnotu. Jedna věc je neoprávněný přístup k datům a druhá věc je, získání utajovaných informací, kdy pachatel spadá úplně do jiné kategorie hackerů. Každá napadená firma nebo instituce se snaží nezveřejňovat tyto problémy a to se jim daří velice úspěšně. Po zjištění napadení jejich systému je nejvíce prioritní bez vyhlášení jakéhokoliv poplachu vylepšit svůj ochranný systém proti těmto útokům. Při zveřejnění průniku do jejích databázového systému by mohli firmy nebo instituce ztrácet prestiž a důvěru nejen na trhu ale i mezi lidstvem.

V literatuře se můžeme často setkat se záměnou termínů hacker a cracker. Mezi tím co crackeři se zabývají vymyšlením a realizací narušení ochrany programů, ať už jde například o neoprávněné kopírování, tak hackeři se zabývají pronikáním do cizí databáze. Každá z těchto skupin se zaměřuje na úplně jiný cíl. Činnost, kterou obě skupiny vykonávají, porušují platná zákonná ustanovení a jsou pro společnost nepřípustná.

2.7 Změny v programech, datech a technickém zařízení

Změny provádí pachatelé za pomoci různých programů, virů nebo pomocí přímého zásahu programátora. Tato metoda se taky nazývá počítačová defraudace, která se kvalifikuje jako trestní čin poškozování cizí věci. V ojedinělých případech se pachatelé dopouští úprav v zapojení nebo v jiném technickém vybavení počítače případně komunikačního prostředku. [35]

2.8 Neoprávněný přístup k datům, získávání utajovaných informací

Jde o data nebo informace, které jsou přístupné jen určitým lidem a pokud se k nim dostane někdo neoprávněný, můžeme říct, že jde o hrozbu. Tuto problematiku často nazýváme taky jako počítačovou špionáž, kdy se jedná o následující činy: [35]

- Ohrožení státního tajemství – Při získávání podkladů potřebných pro zahájení vyšetřování musí vyšetřovatel myslet na to, že se musí jednat o data, které pachatel chtěl získat pro vyzrazení státního tajemství nepovolené osobě. Tyto data jsou předmětem státního tajemství a jsou přístupné pouze vyvoleným lidem. Vyzradit je možné i informace v elektronické podobě.

- Ohrožení hospodářského tajemství – Mezi hospodářské tajemství spadají utajované technologie, technologické postupy, veřejné zakázky ale také počítačové programy apod. K získání těchto informací může dojít za pomocí počítačové techniky.
- Zkreslování údajů hospodářské a obchodní evidence – Tuto trestní činnost nemusí páchat pouze zaměstnanec, ale může se jí dopouštět také zaměstnavatel. Pachatel může provádět útok nejen do programového vybavení, ale může mít přístup přímo ke změně vstupních údajů vkládaných do počítače nebo taky pro změnu podkladů.
- Porušování předpisů o ochraně osobních údajů v informačních systémech

2.9 Zneužívání počítačových prostředků k páchání jiné trestné činnosti

Mezi nejsnadnější a nejúčinnější metodu, jak získat finanční ohodnocení pomocí počítače je manipulace s daty. Tato metoda může byt zaměřena na různé činnosti, kdy dochází k vymazání nebo přepsání správných údajů na pevném disku počítače kterému obsluha, která se o něj stará plně důvěřuje. Zjistit správnost těchto údajů je prakticky nemožné jelikož se tato metoda využívá například ve velkých skladech kde je nespočet různých výrobků a sekcí. Přemazání nebo vymazání je nemožné dohledat kvůli nezanechávání prakticky žádných stop, což vede k velké úspěšnosti páchání tohoto trestního činu za pomoci výpočetní techniky pachatelem.

Pachatelé, kteří páchají tuto trestní činnost, mění data na podkladech, ze kterých jsou data pořizována nebo pomocí změny přímo na médiu na kterých jsou uložena. Manipulovat s těmito daty je možné jak při výpočtech v počítači tak při výstupní sestavě. Mezi nejčastější změny patří změna vstupních dat nebo také zavedení zcela nesprávných dat do počítače. Pachatel využívá situace, kdy zaměstnanec, starající se o zpracované data může data změnit před zpracováním, v průběhu zpracování nebo až po něm. Nezbytně nutné při této činnosti je upravit i ostatní informační soustavy, které jsou propojeny logickými vazbami.

Trestní činy kvalifikované jako podvod jsou páchány pomocí počítačových prostředků a jsou spjaty především k vnitřní kontrole systému organizace, kterými jsou například:

- Správné finanční účetnictví
- Fungování vnitropodnikové kontroly
- Včasná reakce na zjištěné nedostatky o možnostech zneužití apod.

Tento druh kriminality se nejvíce vyskytuje ve finančních institucích, do kterých řadíme banky, pojišťovny, spořitelny apod. Nejčastěji jde o podvody, kdy jsou převedeny finanční prostředky na účet k této činnosti speciálně založené pomocí neoprávněných převodů pachatelem.

Mezi pachatele této trestní činnosti řadíme nejčastěji zaměstnance finančních institucí, kteří napadají počítačové systémy, které jsou chráněny identifikací a autorizací. Pachatelé si vybírají za cíl automatizované i neautomatizované systémy, které jsou nedostatečně vybaveny pro rychlé zjištění trestné činnosti a jeho dostatečnému zadokumentování. V této trestné činnosti není možné spoléhat pouze na bezpečnostní ochranu počítačových systému, ale je třeba mít zodpovědné a kvalitní zaměstnance podniku, vnitřní systém kontrol a celkovou bezpečnost managementu. [35] [42]

2.10 Užití počítače k páchání další trestní činnosti

Kriminální jevy, kde je počítač nástrojem pachatele k páchání další trestné činnosti, která není součástí nebo není spojována s výpočetní technikou, programy nebo daty. V této oblasti je hlavní problematikou výpočetní technika k modelování různých situací, které můžou nastat při páchání trestního činu. Tato činnost patří k hodně náročným, které zvládá pouze opravdový odborník zabývající se problematikou modelových situací. Vytvořit při modelování dokonalé situace je nemožné ale napomáhá tento čin pachatelům jak různým situacím při páchání trestních činů předejít nebo se jim vyhnout a tak dost ulehčují práci pachatelům. [35]

II. PRAKTICKÁ ČÁST

3 PACHATELÉ

Nejčastěji osoby, které jsou obviněné, obžalované, odsouzené nebo propuštěné jsou označovány jednotným názvem a to pachateli. Pachatelem není pouze osoba vykonávající trestní čin ale také osoba, která se podílí jak na přípravě, tak i na pokusu o tento trestní čin. Vlastnosti trestně odpovědného pachatele je osoba, která je starší 15 let a jde o osobu příčetnou. Osoba příčetná je taková osoba, která dokáže ovládat své duševní schopnosti.

Pachatele můžeme dělit do dvou skupin a to jako profesionály a amatéry které budu ve své práci nazývat laiky. Rozdíl mezi tímto dělením je hned na první pohled, že se jedná hlavně o dělení podle zkušeností a možností pachatelů.

3.1 Laici

Obecně za laiky označujeme lidi, kteří v dané problematice nemají příslušné vzdělání nebo nejsou s tímto problémem dostatečně seznámeni. Můžeme tedy konstatovat, že je to osoba, která se konkrétní problematikou sice zabývá, ale její zkušenosti nejsou dostačující, aby obohatily téma nějakým smysluplným a ideálním řešením. Nejsou za svoji práci ohodnoceni žádnou finanční částkou.

Laici pronikají do informačních systémů pomocí zranitelných míst. Většinou jde o pachatele, kteří se dostanou do systémů náhodně nebo cílevědomě aniž by věděli, k jakým datům se dostali. Tito pachatelé si většinou ani neuvědomí, že páchají trestní čin, i když informace ke kterým se dostanou, většinou nerozšíří dál.

Pachatelé, které označujeme za laiky, mají většinou vyšší inteligenci než obyčejní lidé. Ti, kteří jsou takto označování, dokáží na rozdíl od jiných lidí naučit se pracovat s počítačem daleko rychleji. Nad většinou věci oproti jiným nepřemýšlí a dělají ji automaticky, aniž by si to uvědomovali. Jsou daleko schopnější se naučit novějším věcem, všechny nové informace daleko rychleji vnímat a používat. Při změněném plánu reagují hbitě na rozdíl od běžných lidí. Můžeme je tedy označit za talentované lidi, kteří to s výpočetní technikou umí. Laiky můžeme dělit do následujících podkapitol.

3.1.1 Hackery

Za hackera je označován člověk, který disponuje s vynikajícími znalostmi počítačů, operačních systémů, přenosových protokolů a programování. Zná jak silné tak slabé stránky programů ale největší jeho silnou stránkou je vynalézavost při hledání bezpečnostních děr v systémech. Hacker na rozdíl od virů, které dělají pouze to, co jim programátor naprogramoval, se přizpůsobuje situaci a dělá, co zrovna uzná za vhodné, aby se do systému jakkoliv dostal.

Aniž by chtěli získat informace nebo se pokusit o narušení systému, je pro ně nezbytně nutné prokázat jejich schopnosti kvality díky pronikání do chráněných systémů. Jejich činy považují za zábavu, dobrodružství a nepotřebují ani žádnou pochvalu od jiných. Jediná věc, která je zajímá, zda se o tomto činu mluví.

3.1.2 Neúspěšní kritikové

Tímto pojmem jsou označováni lidé, jak jednotlivci, tak skupiny, kteří poukazují na nedostatky v ochraně informačních systémů. Neúspěšní kritikové v počítačové kriminalitě upozorňují na kritické situace, které je potřeba nejlépe okamžitě řešit, dřív než dojde pomocí tohoto nedostatku k napadení počítače. Mezi své hlavní priority berou vyprovokování odpovědných lidí k nápravě nedostatků a tak ke zvýšení bezpečnosti.

3.1.3 Mstitelé

Mstitelé jsou lidé, kteří vykonávají pomstu za věci, které se jim nelíbí nebo pozměnily jejich životy. Jako ideální příklad bych dal vztah zaměstnance, který od svého zaměstnavatele dostal výpověď z práce za něco, co nemohl ovlivnit nebo možná ani neudělal. Zaměstnanec se chce kvůli nespravedlnosti pomstít svému zaměstnavateli a daný čin se označuje jako pomsta. Pomstu vykonávají mstitelé, kteří si neuvědomují, že se dopouští trestného činu.

3.1.4 Crackeři

Cracker je v internetovém světě označován člověk, který zneužívá získané informace o slabých místech zabezpečení nebo bezpečnostních mezerách k trestním činům nebo pro své vlastní přilepšení.

Potěšení tito lidé nemají z toho, jak se dostanou do informačních systémů nebo jak se dostanou k datům, které následně nemají zájem využít pro svoje vlastní obohacení.

Největší potěšení těmto pachatelům dělá zničení systému, do kterého se nabourali a odkud získali i nějaké data.

3.2 Profesionálové

Osoby, které jsou při činnosti v oboru dostatečně vzdělaní nebo mají bohatou praxi s činností, kterou vykonávají, jsou označovány za profesionály. Tito lidé jsou za práci finančně ohodnoceni, nikoliv však dostatečně, i když disponují dostatečnou praxí nebo znalostmi v oboru.

Profesionálové se dělí do následujících kategorií:

- Zaměstnanec s pravidelným příjmem
- Nezávislý profesionálové na volné noze
- Zaměstnavatel, častěji spíš podnikatel

Mezi hlavní dělení profesionálních pachatelů řadíme rozdělení na jednotlivce a skupiny, kdy podle počtu pachatelů je možné zařadit do správné skupiny. Máme tedy profesionály jednotlivce a nebo skupiny.

3.2.1 Jednotlivci

Jednotlivci, jsou lidé, kteří při plnění své práce nebo úkolech nepotřebují dalšího člověka pro jeho dokončení nebo úspěšné splnění. Můžeme tedy jednotlivce označit za takovou samostatnou jednotku, která svoji činnost zvládá díky svým schopnostem a znalostem.

Při popisování této problematiky jsem uznal za vhodné zmínit i konkrétní jména, dle zahraničních serverů „fresherwolrd“ a „science“ a to tří nejnebezpečnějších pachatelů s cílem vytvoření vyšší představy o závažnosti dané problematiky.

Za pomocí zahraničních serverů „fresherwolrd“ a „science“, na které je nejvíce odkazováno. Jsou označovány za nejnavštěvovanější zahraniční servery zabývající se žebříčkem, které informují o deseti nejhorších hackerech na světě. Tyto servery informují v angličtině širokou veřejnost o 10 nejnebezpečnějších hackerech na světě, o bližších informacím, co nejnebezpečnější pachatelé jednotlivci spáchali za trestní čin a tak upoutali na sebe nemalou pozornost všude na světě. Podle studií a závažnosti trestního činu se umístily mezi 3 nejnebezpečnějšími následovně: [39] [40]

a) **Jonathan James** - James získal publicitu, když se stal prvním člověkem, kterého poslali do vězení za hacking. Odsouzen byl v šestnácti letech. V jeho anonymním rozhovoru pro PBS prohlásil: "Pouze jsem se rozhlížel, pohrával si. Byla to pro mě výzva, zjistit co všechno se mi může podařit."

Hlavním cílem Jamesových průniků byly vysoce postavené organizace. Podařilo se mu nainstaloval backdoor do serveru Defense Threat Reduction Agency (DTRA), což je oddělení Ministerstva obrany Spojených států zodpovědné za snižování nebezpečí útoku nukleárními, biologickými, chemickými, konvenčními a speciálními zbraněmi proti U.S.A. a jejich spojencům. Tento backdoor mu umožnil prohlížet si citlivé emaily a zachytit uživatelské jména a hesla zaměstanců.

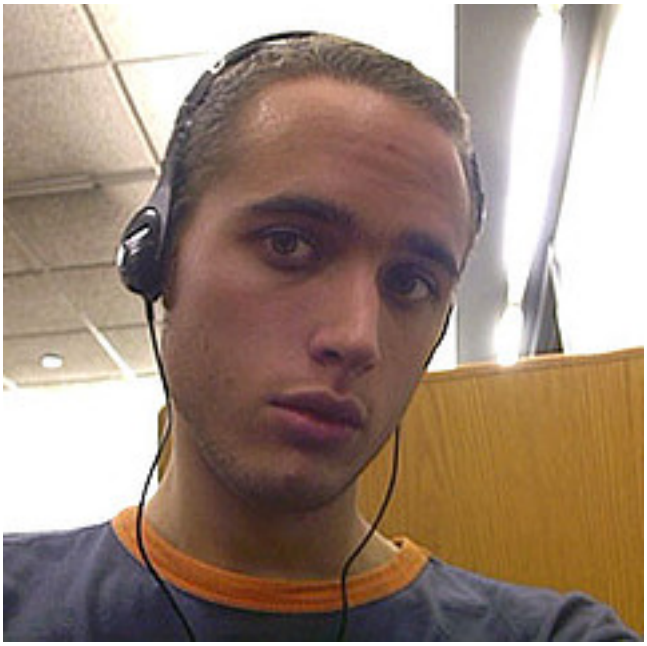
Jamesovi se rovněž podařilo nabourat se do počítačů NASA a ukrást software za přibližně 1,7 milionu dolarů. "Software měl za úkol kontrolovat prostředí na Mezinárodní vesmírné stanici, včetně regulace teploty a vlhosti v obytných prostorech", znělo vyjádření ministerstva spravedlnosti. NASA byla donucena vypnout své systémy což vedlo ke škode 41 tisíc dolarů. James prohlásil, že si kód stáhnul aby prohloubil své znalosti programování v C. "Ten kód samotný byl velice špatný, určitě neměl cenu 1,7 milionu dolarů jak tvrdili".

Obrázek 15 – Jonathan James [39]

b) **Adrian Lamo** - Lamova sláva tkví v jeho průnicích do významných organizací jako The New York Times a Microsoft. Lamo, přezdívaný jako "hacker bezdomovec", používal pro své útoky internetové připojení v různých kavárnách a knihovmách a přespával v opuštěných budovách.

Lamovy průniky spočívali zejména v testování systémů proti průnikům a posléze o těchto nedostatcích v zabezpečení informoval příslušné firmy. Jeho cíle zahrnovaly Yahoo!, Bank of America, Citigroup a Cingular. Pokud jsou hackeři najmuti aby takto testovali systémy, je to legální. Počínání Lama ovšem nebylo.

Když se naboural do intranetu The New York Times, přidal se do seznamu expertů a mohl tak prohlížet osobní informace přispěvatelů včetně jejich rodných čísel. Lamo se rovněž naboural do účtu LexisNexis a mohl tak zkoumat vysokoprofilové témata.



Obrázek 16 – Adrian Lamo [39]

c) **Kevin Mitnick** - Za jeho průniky do The New York Times mu bylo nařízeno zaplatit odškodnění zhruba 65 tisíc dolarů. Rovněž byl odsouzen na šest měsíců domácího vězení s dvouletou podmínkou, která vypršela 16. ledna 2007. Lamo nyní pracuje jako oceněný novinář a řečník.

Mitnick si prošel veřejným pronásledováním úřady. Jeho prohřešky byly medializovány, ale jeho skutečné činy jsou méně vyznámné než může jeho sláva napovídat. Ministerstvo spravedlnosti ho popisuje jako nejhledanějšího

počítačového kriminálníka v historii Spojených států. Na motivy jeho prohřešků byly natočeny dva filmy: Freedom Downtime a Takedown.

Mitnick již měl nějaké zkušenosti předtím, než spáchal činy, které ho proslavily. Začal zneužíváním jízdenkového systému autobusové dopravy v Los Angeles a poté se začal zabývat, podobně jako spoluzakladatel firmy Apple Steve Wozniak, phreakingem (napojování se na cizí telefonní linky). I když měl několik prohřešků (včetně prohřešků vůči telefoním gigantům Nokia a Motorola), byl nakonec odsouzen za průnik do počítače firmy Digital Equipment Corporation, z kterého zcizil software.

Dnes ze z Mitnicka stal produktivní člen společnosti. Poté co si odseděl pět let, začal pracovat jako poradce pro počítačovou bezpečnost a je rovněž autorem a řečníkem.

Obrázek 17 – Kevin Mitnick [39]

3.2.2 Skupiny

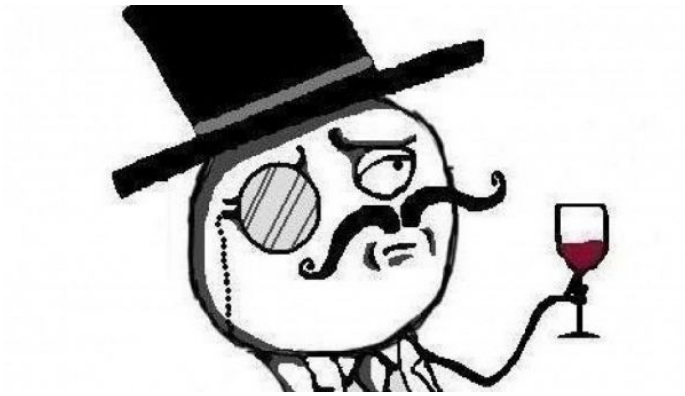
Skupinu tvoří minimálně dva členové a maximálním počtem není nijak omezena. Každý člen ze skupiny má přidělenou svoji vlastní roli, kterou ve skupině vykonává a umí jí dobře ovládat. Za jednotlivce ve skupině zodpovídá vedoucí skupiny, který rozděluje jednotlivé úkoly mezi tyto lidi a za výsledek nese odpovědnost.

Ve světě jsou proti počítačové kriminalitě zřízeny speciální skupiny, které se zaměřují pouze tímto fenoménem. U nás v CŘ se zatím počítačové kriminalitě nevěnuje až taková pozornost, která by vedla ke snížení počtu trestních činů spojené s počítačovou kriminalitou.

Mezi skupiny pachatelů, které označujeme za profesionály, patří převážně zahraniční skupiny hackerů. Jde o skupiny, o kterých jsme už nejednou zaslechli nebo jsme se mohli o jejich činnech dočíst. Mezi skupiny pachatelů patří například Lulz Security, P1R@T3Z'SEC , Anonymous, TrollSec, apod. Ze stejných důvodů uvedených v kap. 3.2.1 si zde dovolím opět nastínit i některé konkrétní skupiny.

a) **Lulz Security** - Za nebezpečnou skupinu byla označená právě skupina Lulz Security, která se přezdívala jako LulzSec. Skupina se podle dostupných informací skládala ze 6 členů. Své útoky směřovala na CIA a pornografické servery. Na svědomí měla celou řadu útoků. Tato skupina si předem určila dobu její existence, která byla pouze 50 denní. Podle různých názorů měla spíše tato skupina obavy, že budou dopadeni a proto ukončila své působení. Jejich vyjádření, které zveřejnila skupina LulzSec na svých internetových stránkách znělo následovně: [41]

   „Za posledních 50 dnů jsme ničili a obnažovali společnosti, vlády, často i veřejnosti samostatnou a dost možná i všechny ostatní, a to jen proto, že jsme mohli."



Obrázek 18 – Logo skupiny Lulz Security [41]

b) Anonymous – Velké znepokojení a obavy má na svědomí skupina, která se nazývá Anonymous. Jde o skupinu, se kterou se teď setkáváme na každém kroku, jelikož se můžeme dočíst nejen na internetu ale také v novinách, o jejich úspěšných útocích mezi které patří útoky na velké finanční společnosti včetně takových jako jsou Visa a MasterCard.

Válku tato skupina vyhlásila pedofilům, kterým shodila nejrozsáhlejší síť s tímto materiálem a to Lolita City. Tuto síť vyřadila úplně z provozu a zveřejnila kompletní seznam návštěvníků, kteří tuto stránku navštěvují.

Deník Guardian přinesl informaci že skupina Anonymous zveřejnila na internetu osobní data všech klientů firmy Stratfor, což poškodilo okolo 850 tisíc lidí, mezi které patřili zaměstnanci NATO, britské vlády či Scotland Yardu. Následně tato skupina oznámila, že firmě odcizila 200 GB e-mailů a údajů o kreditních kartách, které patří klientům firmy Stratfor. Po zveřejnění někteří odborníci objevili jako největší problém, že některé e-mailové kontakty nejsou obecně známé a že hackeři ze skupiny Anonymous zveřejnily taktéž jejich zakódované hesla, které jsou pro nadané uživatele snadno dekódovatelné.

Obrázek 19 – Logo Anonymous [42]

3.3 Teroristé

Speciální skupina lidí, která slouží k dosažení předem určených cílů. Trestní čin, který páchají teroristé, nazýváme terorismus. Nezbytnou součástí terorismu je plánování, promyšlení a politicky motivované násilí. Jsou zaměřené na ohrožení chodu státu nebo mezinárodní organizace, které si určí.

Terorismus patří mezi nezákonné užití síly a násilí použité proti osobám nebo majetku s určitým záměrem vůči státu, obyvatelstvu nebo jinou skupinu. Fungují převážně jako skupina lidí, protože spáchat terorismus jako jedinec je nereálné.

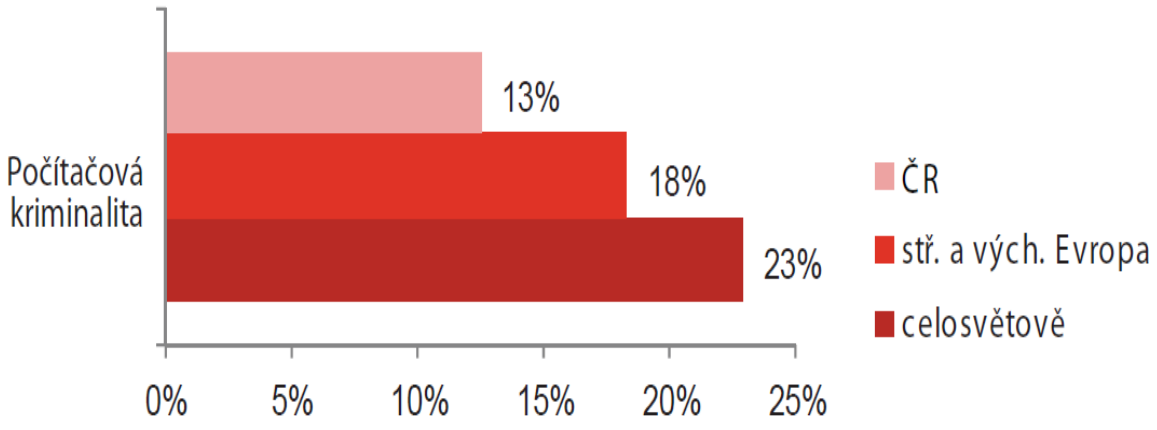
Jsou označovány za vysoce kvalifikované skupiny, které vlastní zpravodajské sítě pro získávání potřebných informací nebo pro ochranu vlastních gangů. Do těchto skupin většinou spadají pracovníci zpravodajských služeb, kteří využívají jiných způsobů a prostředků pro úspěšné splnění úkolu než obyčejní zpravodajští pracovníci.

3.4 Statistiky útoků

Společnost PwC, která se v současné době zabývá nejrozsáhlejším průzkumem svého druhu na světě v roce 2011 zveřejnila výsledky celosvětového průzkumu hospodářské kriminality. V tomto průzkumu nalezneme zkušenosti a názory 3877 odborníku ze 78 zemí kde i své zastoupení mají přední společnosti z České republiky.

3.4.1 Spáchané podvody v počítačové kriminalitě

Počítačová kriminalita patří mezi nejčastěji páchané hospodářské zločiny. Tato trestní činnost ročně roste z důvodu malé prevence ať už u firem nebo organizací. Dle statistiky, která ukazuje, že počítačová kriminalita je na 4.místě v průzkumu se 13% a s velkou pravděpodobností a sledovatelností je každoročně pozoruhodný nárust tohoto činu. K tomuto růstu přispívá i fakt, že 2 z 5 českých respondentů by v uplynulém roce neprošli žádným školením se zaměřením na počítačovou bezpečnost.



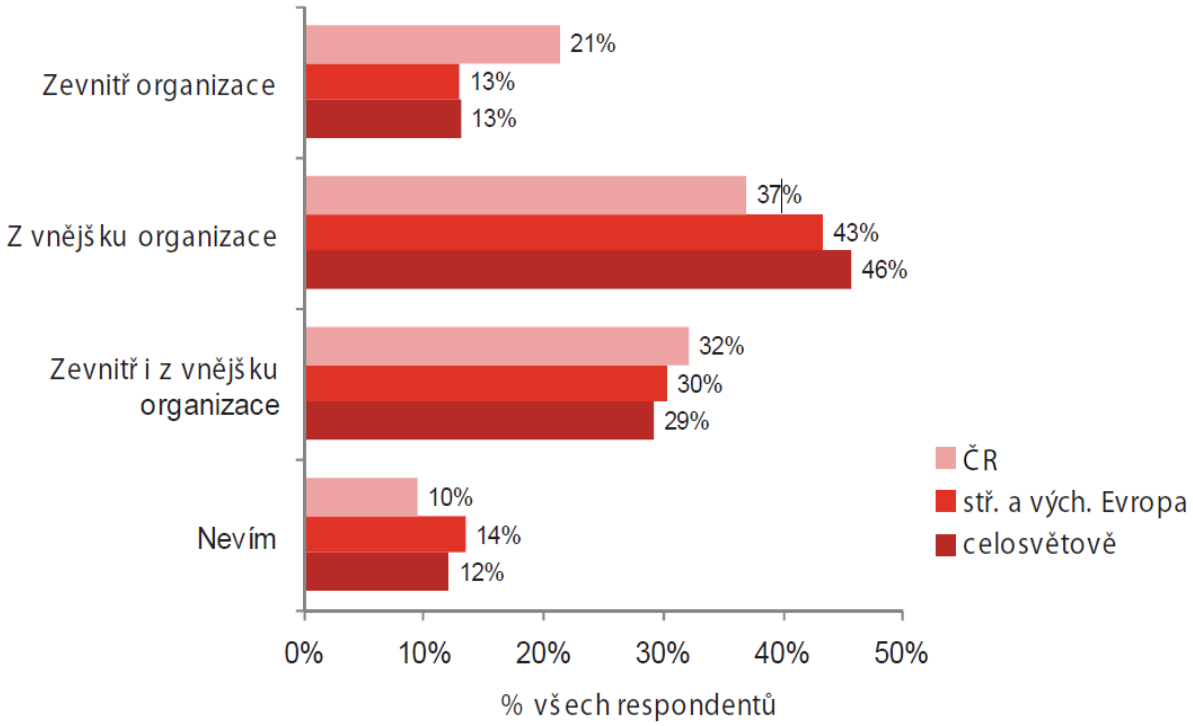
Obrázek 20 – Podíl ze spáchaných podvodů v počítačové kriminalitě [38]

V dnešním světě čím dál více společností využívá internetu, sociálních síťí nebo mobilních aplikacích k svému zviditelnění a zlepšení komunikace se zákazníky. Využití těchto forem

má svoje jak klady, tak i zápory. Mezi klady této stránky patří informovanost zákazníků jak eventuálních tak nových. Zápory jsou označovány většinou hrozby, které se rozšiřují závratnou rychlostí stejně jako technologie.

3.4.2 Největší rizika pro organizace

Počítačová kriminalita je nejvíce vnímána jako hrozba zvenčí. Průzkum, který se tímto zabýval, nás díky svým výsledkům nijak extra nepřekvapil. Potvrdil nám pouze fakt, že nejvíce se rizik musíme obávat z vnějšku organizace ale je potřeba se mít určitě na pozoru i zevnitř organizace.

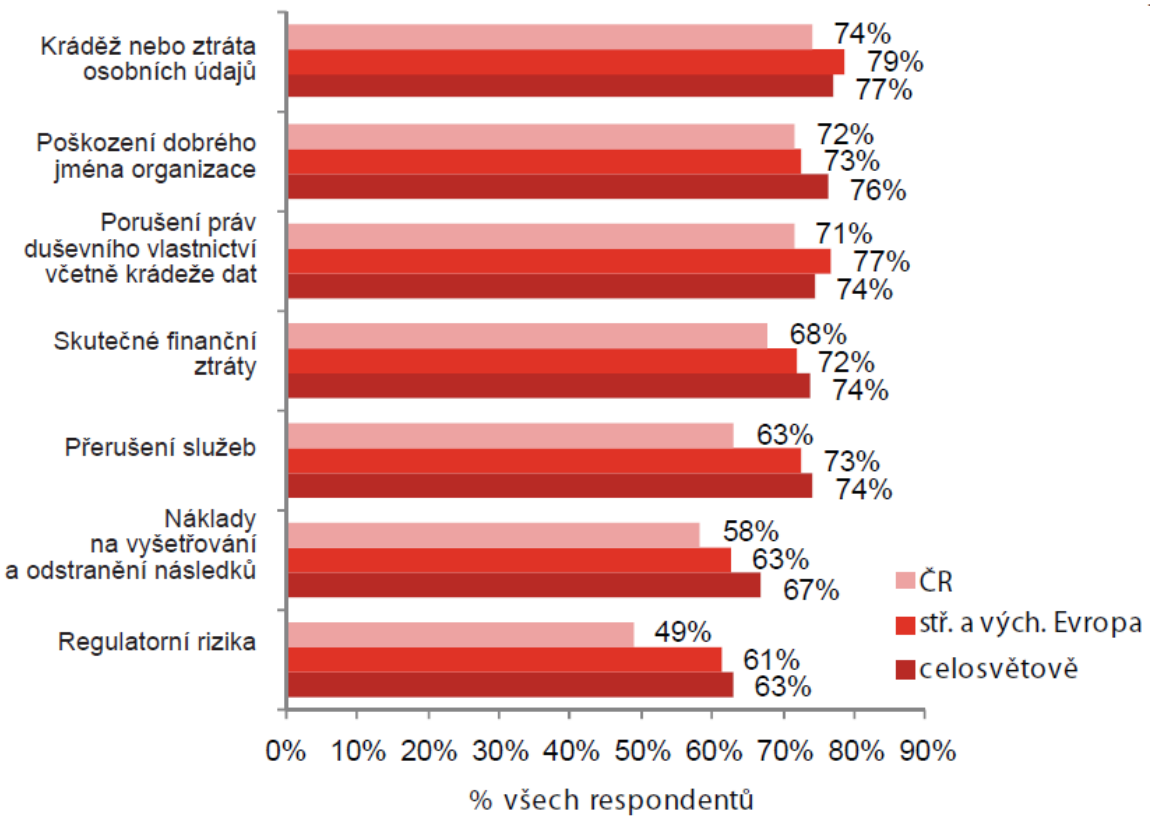


Obrázek 21 – Odkud hrozí největší rizika pro organizace [38]

Neexistuje dosud žádný návod jak přimět organizace ke sledování počítačové kriminality. Když už dojde ke sledování této problematiky, donutí to organizace k zamyšlení, co by se stalo s jejich dobrým jménem v případě, že by byly z jejich firmy odcizeny důležité data jejich klientů.

3.4.3 Největší obavy společností v počítačové kriminalitě

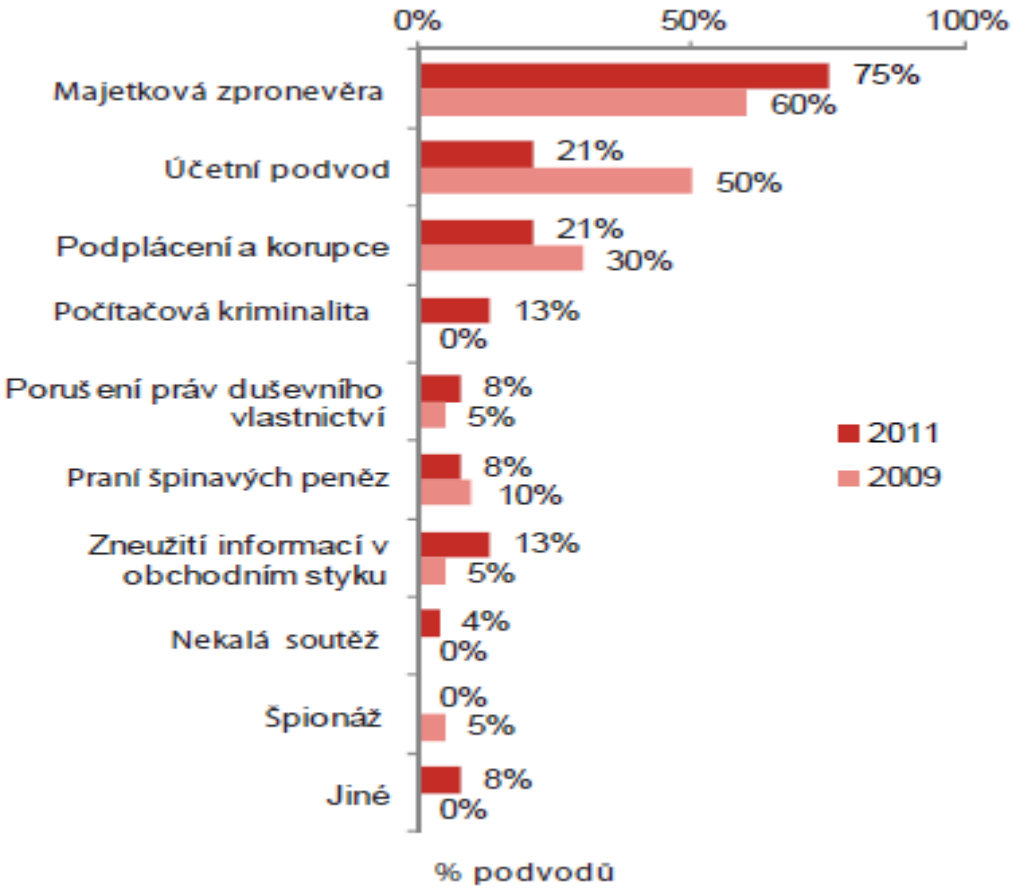
Jak již z grafu vyplívá, mají největší obavy organizace z krádeží nebo ztráty osobních údajů. Hned v závěsu stojí poškození dobrého jména organizace a nejmenší obavy mají z regulatorních rizik. Z důvodu, že organizace mají obavy z těchto činů, je nezbytně nutné, aby zákazníkovi nabídly nejbezpečnější místo a připravily co nejvíce konkurenci schopnou nabídku pro svoje klienty vůči konkurencím.



Obrázek 22 – Největší obavy v počítačové kriminalitě [38]

3.4.4 Typy hospodářské kriminality v ČR

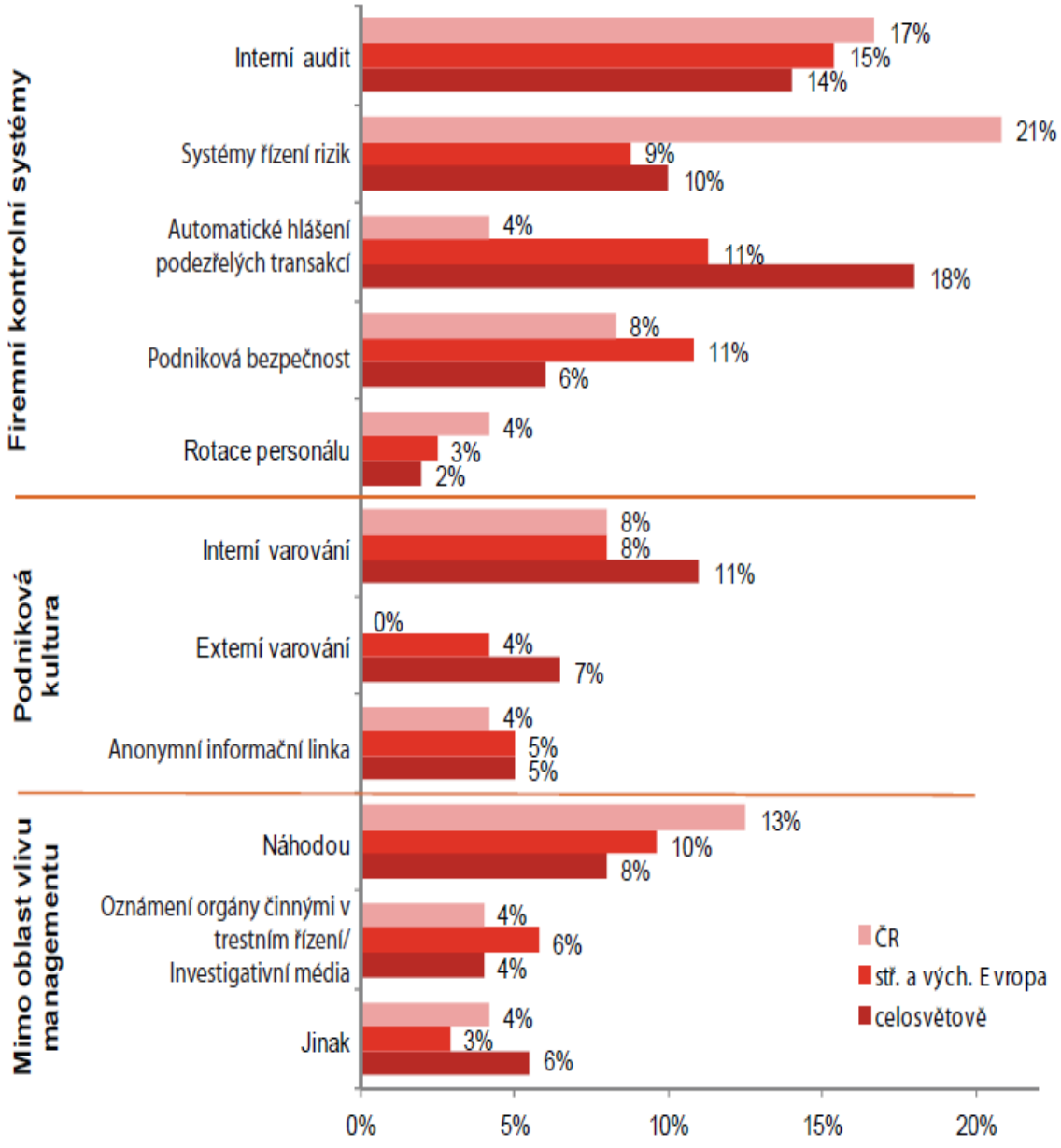
Nejčastějším typem hospodářské kriminality zůstává tradičně majetková zpronevěra, která zažívá i velký vzestup od roku 2009 a to až o 15%. Počítačová za poslední 2 roky zažívá velké rozšíření a to z 0 na 13%. Z této studie vyplývá, že největší nárůst získala majetková zpronevěra, ale počítačová kriminalita začíná byt mezi pachateli čím dal populárnější a nebude tomu v blízké budoucnosti jinak, pokud kompetentní osoby nezasáhnou.



Obrázek 23 - Jednotlivé typy hospodářské kriminality v ČR [38]

3.4.5 Způsoby odhalení podvodů ve společnostech

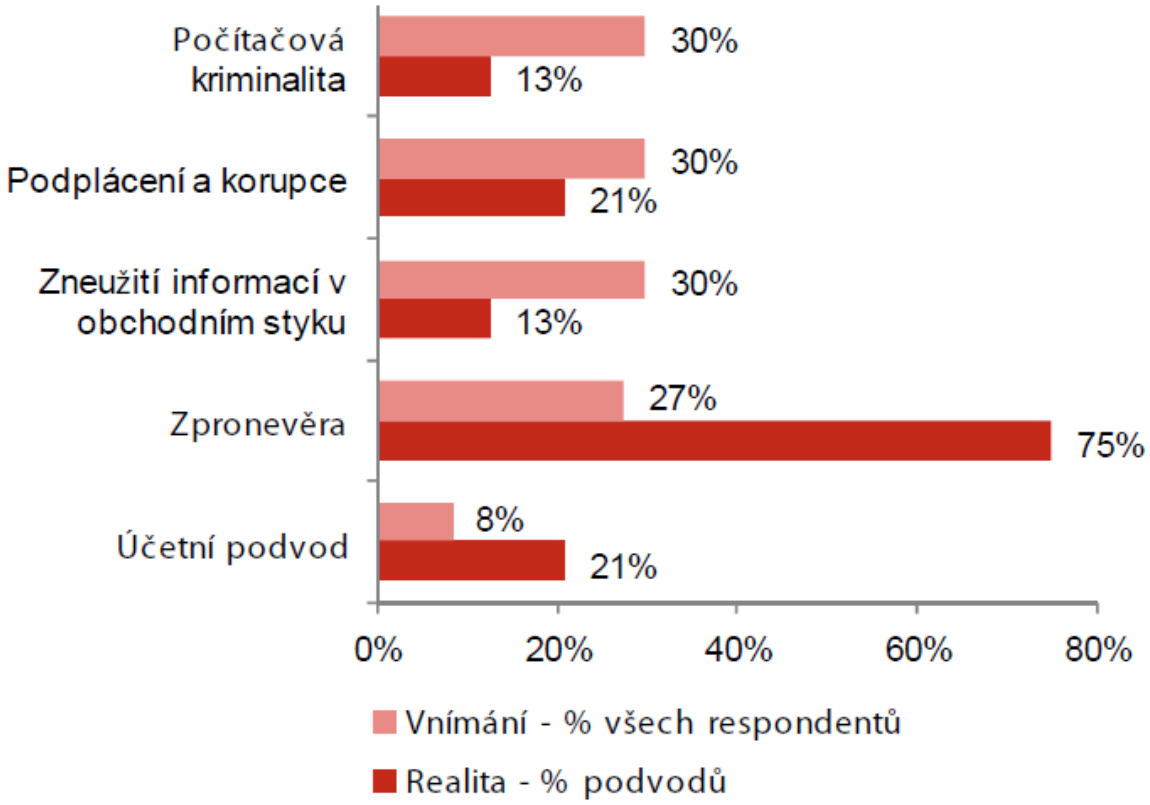
Z níže uvedeného grafu vyplývá, že nejvíce odhalených podvodů ve společnosti je za pomocí firemních kontrolních systémů, které využívají detekční mechanismy. Ve srovnání s rokem 2009 je velice pozitivní pokles podvodných případů z 30% na 21% a to za pomoci náhodného odhalování nebo jiných faktorů.



Obrázek 24 – Způsoby odhalení podvodů ve společnostech [38]

3.4.6 Hospodářská kriminalita v budoucnu

Podle studií, které firma PwC prováděla, lidé vnímají počítačovou kriminalitu za daleko problémový subjekt, než je realisticky zaznamenáno. Velkou roli v tomto hraje obzvlášťě fakt, že velké množství případů v počítačové kriminalitě není nikde zaznamenáno, protože poškození lidé nemají mnohdy ani tušení , že byli napadeni pachatelem a tak i poškozeni.



Obrázek 25 – Vnímání a skutečnost vývoje kriminality v ČR [38]

4 PREVENCE PŘED POČÍTAČOVOU KRIMINALITOU

Prevence je řada opatření, které ochraňují počítač a zároveň pomocí prevence předcházíme různým druhům napadení. Pomocí prevence můžeme předejít nedostatečnému základnímu zabezpečení, vyvarovat se nedostatečným ochranám v různém softwaru. Je důležitou částí ochrany před nežádoucími nástrahami, se kterými se můžeme setkat jak na internetu, tak v síti. Pomocí prevence, na kterou mnoho lidí nedbá, se může podařit snížit počet těchto trestních činů, které každoročně rostou, jak již jsme se mohli dozvědět v předešlé kapitole, kde jsme se zabývali i statickými údaji páchání této kriminality.

Nezbytně nutné než sepíšeme postupné body prevence je důležité zjistit, jak počítač budeme využívat. Počítač je možné využívat pomocí dvou způsobů. Jedním ze způsobu je, že počítač je určen pro běžné používání nebo je počítač určen jako server. Ne ve všech krocích se prevence liší, ale je velice důležité vědět, jak bude počítač používán, aby bylo prevence před počítačovou kriminalitou účinná a odvracela tak případné útoky ať už na server nebo na běžný počítač.

Dle mého názoru je nezbytně nutné rozdělit v systémech bezpečnostních služeb prevenci před počítačovou kriminalitou na běžné počítače připojené k internetu a počítače nepřipojené k internetu.

4.1 Počítače nepřipojené k internetu

Základem každého počítače je operační systém a to hlavně legální. Rozdílů mezi nelegálním systémem a legálním je hned celá řada. Velkou výhodou u legálních operačních systémů se stala velká podpora ze strany vývojářů, kteří i po vydání daný systém dolaďují během jeho chodu chyby v něm vytvořené nebo mezery, které nejsou úplně dodělané. Nezbytně nutnou prevencí před počítačovou kriminalitou je používání pouze nezávadného softwaru a hlavně pouze potřebných programů pro činnost, pro kterou je tento počítač určen. Instalování jiných aplikací či softwaru pro vlastní účely, který není dostatečně zabezpečen, nahráváme pachatelům k páchání trestné činnosti. Základem pro bezpečnost je využívání jiných účtů než s plnými právy administrátora, aby při napadení neměl pachatel tak velké možnosti k páchání trestního činu. Každý účet by měl být opatřen silným heslem, aby se předešlo k jeho zneužití. V případě že je počítač součástí střeženého objektu nebo areálu je nezbytně nutné mít nainstalován antivirový program, aby bylo možné detekovat hrozby ať už při zálohování záznamů nebo dalším úkonům ohrožující

tento počítač. Obsluhovat počítač nebo přístup k němu by měli mít pouze osoby k tomu určené. Tento počítač je často označován jako server, který se musí nacházet v zabezpečené místnosti, do které je možné vstoupit jen za pomoci čipové karty, která vás pustí nebo za pomocí klíčků od dané místnost.

4.2 Počítače připojené k internetu

Základ prevence ať už u počítače připojeného k internetu nebo nepřipojeného je totožný. Základem je instalovat jedině legální operační systém a pouze nezávadný potřebný software, který neohrozí jak chod počítače samotného, tak důležité data v něm uložené. Opomenout bychom neměli taky změnu hesla pro administrátora případně i uživatelského jména pro přístup na tento server s plnými právy, ze kterého je možné cokoliv instalovat, měnit nastavení apod. Přihlašovací jména často bývají nastavené na admin nebo administrátor a k nim přidělené hesla totožné s přihlašovacím jménem nebo řadou jdoucích čísel po sobě aby byly snadno zapamatovatelné, přitom jde o velice slabou až možná nulovou zabezpečenost přihlašovaní. Takové hesla nejsou dostatečně bezpečná, proto pro zkvalitnění zabezpečení se doporučuje používat silná hesla, které obsahují jak velké tak malé písmena ale i čísla a různé znaky. Takové hesla odhalit je i pro pachatelé zapeklitý oříšek.

Totožné zabezpečení jako u uživatelských účtů, bychom měli provést na routeru nebo modemu, pomocí kterého se připojujeme k internetu. Počítače připojené k internetu se nejčastěji v systémech bezpečnostních služeb používají k hlídání objektů nebo areálů. Jde o tzv. monitorování objektu před nežádoucími vlivy. Tento počítače je nejčastěji využíván jako server. Zabezpečení serveru se moc od zabezpečení počítače neliší. V případě, že server má být připojen k internetu, musíme patřičně po nainstalování všeho potřebného nastavit bránu firewall, což je software, který odděluje provoz mezi dvěma síťěmi a zajišťuje, aby se neoprávněné osoby nedostali do tohoto serveru a nezískaly přístup k informacím, které jsou na serveru uložené.

Server slouží k sledování objektu jak přímo v místě objektu, tak pomocí internetu hlídání na dálku. Za pomocí počítače dokážeme sledovat široký okruh zabezpečených míst a nejen přímo z jednoho serveru ale i z více zároveň. Z důvodu, že se počítač stává důležitým předmětem v ochraně, stává se také častým cílem pachatelů, proto je samozřejmostí, aby byl tento server umístěn v uzamčené místnost tak, aby k nim měli přístup pouze oprávněné osoby za pomocí klíče nebo čipové karty se speciálním kódem. Data, které počítač denně

zaznamenává a ukládá na disk, který je součástí počítače, by měli být pravidelně zálohována na externí disk, který se využívá pouze za tímto účelem. Tento disk při běžném provozu počítače nesmí byt napadnutelný a zálohování se nesmí provádět v pravidelných intervalech, aby se pachatelé na tuto činnost nemohli nijak připravit.

Tuto činnost nejčastěji využívají bezpečnostní složky, které se zabývají hlídáním objektů, areálů a míst, které potřebují v časovém rozmezí nebo nepřetržitý přehled co se na sledovaných místech odehrává.

ZÁVĚR

Cílem této práce nebylo pouze vytvořit učební pomůcku do předmětu Kriminalistické technologie a systémy, ale snaha informovat o počítačové kriminalitě a poukázat na závažnost této celosvětové problematiky. Předložená práce je rozdělena na teoretickou a praktickou část.

Teoretická část práce se zabývá nejen pojmem kybernetická a počítačová kriminalita, ale také popisem jednotlivých typických útoků spadající do počítačové kriminality. Tato část práce se také soustředí na samou roli počítače v počítačové kriminalitě a v návaznosti na nosič informací, digitální stopu, identitu nebo copyright. Nemalá část je také věnována možným způsobům páchání počítačové kriminality s cílem vytvoření lepší představy o dané problematice.

Praktická část je především zaměřena na možné pachatele, statistické údaje páchání počítačové kriminality a preventivní opatření proti tomuto fenoménu. Pachatele jsem dle zkušeností získaných během vypracování této práce rozdělil do dvou hlavních kategorií a to dle schopností a zručností při páchání trestního činu, konk. tedy počítačové kriminality. Statistické údaje poukazují na fakt, že se jedná o rozsáhlou oblast kriminality a to nejen u nás v ČR, ale také na celém světě. Práce také poukazuje na skutečnost, že se ve světě danou problematikou zabývají daleko více a to prostřednictvím vytvořených skupin zaměřených pouze na počítačovou kriminalitu. Ze statistik také vyplívá, že největší obavy mají společnosti z útoků z vnějšku, které pachatelé směřují nejčastěji na krádež nebo odcizení osobních údajů. V nemalé míře je také věnována pozornost konkrétním příkladům činů této trestné činnosti jednotlivých pachatelů a skupin s cílem vytvoření lepší představy a zdůraznění závažnosti problematiky zvané počítačová kriminalita.

Problematika počítačové kriminality je stále aktuálním tématem. Z vlastního pohledu běžného uživatele připojeného k internetu, bych prevenci neponechával náhodě. Investice do softwarového zabezpečení patří ve společnostech k zanedbatelným položkám, pokud si vypočteme škody, které po napadení můžou nastat. Preventivní opatření vede ke zmenšení pravděpodobnosti výskytu rizikové události nebo taky ke zmírnění jejich dopadů. Po napadení je už pozdě plánovat preventivní opatření, protože dochází k odcizení informací u kterých vyčíslit hodnotu je nereálné. Každé opatření, které provedeme, nás stojí nejen čas ale taky finanční zátěž. V budoucnu se ale může toto opatření projevit pouze kladným dojmem.

CONCLUSION

The goal of this work wasn't only making of learning task into criminal technology subject and systems, but also to inform about computer criminality and to show difficulty of this world's problem. This work is divided into theoretical part as well as practical part.

The theoretical part of this work deals with cybernetic and computer criminality as well as with description of attacks that are part of the computer criminality. This part also focuses on the role of a computer as a part of a computer criminality in relationship with information media, digital trace, identity or copyright.The large part is dedicated to possible ways of committing computer crime with purpose of making better ideas about mentioned problems.

The practical part is mostly focused on possible offenders, statistic data of committing computer crime and prevention against this phenomenon.According to experience I got during writing this work I divided offenders into two main categories as per skills and abilities during committing computer crime.Statistic data show the fact that computer criminality is spread not only in our country but all over the world.The work also shows the fact that they deal more with this problem abroad than in our country especially by groups focused only on computer criminality. From statistics we also know that companies are afraid of attacks from outside which steal personal data.This work also makes attention on concrete examples of crimes of individual offenders and groups with purpose to make better ideas and emphasis relevancy of problems in computer criminality. The computer criminality is always actual issue.In my opinion as an ordinary user of the internet connection I wouldn't leave the prevention on the luck.

Investment in software security belongs to inappreciable items in companies if we calculate losses which can happen after attack. Prevention leads to decreasing of probability of high-risk events or also to minimize their impacts. It can be very late to plan prevention after attack because the information is stolen and it's impossible to evaluate its value. Every proceeding we make cost us time as well as money.But this proceeding can prove in positive way in the future.

Seznam použité literatury

[1] Zákon č. 140/1961 Sb.; trestní zákon, ve znění pozdějších předpisů

[2] MATĚJKA, Michal. *Počítačová kriminalita*. 1. Vydání. Praha : Computer Press, 2002. s. 72

[3] JIROVSKÝ, Václav, KRULÍK, Oldřich. Základní definice vztahující se k tématu kybernetických hrozeb [online]. 2005 [cit. 2012-04-18]. Dostupný z WWW: <http://www.micr.cz/bezpecnost/informacni/zakladni_info.pdf>.

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

[5] ZAPLETAL, Josef. ZA KOLEKTIV. *Aktuální problémy kriminologie*. 2009. vyd. Praha: Policejní akademie České Republiky v Praze, 2009. ISBN 978-80-7251-316-1.

[6] SPY SHOP. *SPY SHOP*: *Keylogger - "odposlouchávací zařízení" ve vašem počítači* [online]. 2012 [cit. 2012-04-20]. Dostupné z: http://www.spyshop.sk/index.php?option=com_content&task=view&id=105&Itemid=29

[7] Trojan help. *Trojan help* [online]. 2004 [cit. 2012-04-20]. Dostupné z: http://trojanhelp.wz.cz/co/spywa/spywa.htm

[8] MATĚJKA, Michal. *Počítačová kriminalita*. 1. vydání. Praha : Computer Press, 2002.

[9] JELÍNEK, Jiří a kol. *Trestní právo hmotné.* 1. vydání. Praha : Leges, 2009.

[10] *Papírové platidla, bankovky* [online]. 2012 [cit. 2012-04-20]. Dostupné z: http://www.papirovaplatidla.cz/informace/ochranne-prvky

[11] Počítačový červ. *Jak na náš počítač* [online]. 2009 [cit. 2012-04-20]. Dostupné z: http://mujcomp.mypage.cz/menu/menu/pojmy/slovnik-pojmu-viry-havet-spyware/pocitacovy-cerv-cervi-a-jejich

[12] Cyberstalking - praktické ukázky. *Cyberstalking - praktické ukázky*. 2008, č. 1. Dostupné z: http://cms.e-bezpeci.cz/content/view/44/63/lang,czech/

[13] Trojský kůň. *Trojský kůň*. 2011, č. 1. Dostupné z: http://tema.novinky.cz/trojsky-kun

[14] GŘIVNA, Tomáš a kol. *Kyberkriminalita a právo.* 1. Vydání Praha : Auditorium, 2008.

[15] Nebuď oběť. *Nebuď oběť* [online]. 2010 [cit. 2012-04-20]. Dostupné z: http://www.nebudobet.cz/?page=hoax

[16] SPYWARE - info. *SPYWARE - info* [online]. 2005 [cit. 2012-04-20]. Dostupné z: http://www.spyware.kvalitne.cz/Co-je-spyware.htm

[17] Phreaking v kostce: jedno místo, jeden článek. *Phreaking v kostce*. 2008, č. 1. Dostupné z: http://www.phreaking.eu/hlavni/phreaking-v-kostce-jedno-misto-jeden-clanek/

[18] Co je to Sniffing?. *Co je to Sniffing?*. 2011, č. 1. Dostupné z: http://www.ikarus.jecool.net/?p=76

[19] Mozek tě vidí: Počítačová a internetová bezpečnost. *Mozek tě vidí* [online]. 2010 [cit. 2012-04-20]. Dostupné z: http://mozektevidi.cz/hacking-hacker/

[20] Matějka, M.: Počítačová kriminalita. Praha : Vydavatelství a nakladatelství Computer Press,2002

[21] Gřivna, T., Polčák, R.,(eds.) Kyberkriminalita a právo, nakladatelství Auditorium, Praha 2008, první vydání – ÚMLUVA O POČÍTAČOVÉ KRIMINALITĚ Budapešť 23. listopadu 2001 česká verze

[22] Denial of Service (DoS) útoky: úvod. *Denial of Service (DoS) útoky*. 2006, č. 1. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/

[23] Denial of Service (DoS) útoky: typy využívající chyb a vyčerpání systémových prostředků. *Denial of Service (DoS) útoky*. 2006, č. 2. Dostupné z: http://www.lupa.cz/clanky/typy-vyuzivajici-chyb-a-vycerpani-systemovych-prostredku-2/

[24] Útok Anonymous na web České protipirátské unie a co je to vlastně DDoS?. *Útok Anonymous na web České protipirátské unie a co je to vlastně DDoS?*. 2012, č. 2. Dostupné z: http://diit.cz/clanek/co-to-je-ddos-utok-a-jak-se-dela

[25] Internetová kriminalita: Ve šlépějích warezu za porušováním autorských práv.*Objevit*. 2012, č. 1. Dostupné z: http://objevit.cz/internetova-kriminalita-ve-slepejich-warezu-za-porusovanim-autorskych-prav-t8938

[26] Co je cybersquatting. *Co je cybersquatting*. 2010, č. 1. Dostupné z: http://svet-hostingu.cz/2010/10/13/co-je-cybersquatting/

[27] Kdo je to cracker a co znamena cracking?. *Kdo je to cracker a co znamena cracking?* 2011, č. 1. Dostupné z: http://www.ikarus.jecool.net/?p=69

[28] Cybersquatting a jeho podoby. *Cybersquatting a jeho podoby*. 2008, č. 1. Dostupné z: http://www.pravoit.cz/article/cybersquatting-a-jeho-podoby

[29] Cybersquatting ? červená spekulantům!. *Cybersquatting ? červená spekulantům!*. 2007, č. 1. Dostupné z: http://www.pravoit.cz/article/cybersquatting-cervena-spekulantum-1-dil

[30] Cybersquatting: Co to vlastně znamená?. *Cybersquatting*. 2006, č. 1. Dostupné z: http://www.dsl.cz/clanek/455-cybersquatting-co-to-vlastne-znamena

[31] Matějka, M.: Počítačová kriminalita. Praha : Vydavatelství a nakladatelství Computer Press, 2002

[32] ČERNÝ, Michal. Znáte své digitální stopy?. *Znáte své digitální stopy?*. 2007, č. 1. Dostupné z: http://www.lupa.cz/clanky/znate-sve-digitalni-stopy/

[33] ČERNÝ, Michal. Digitální stopy a digitální identita. *Digitální stopy a digitální identita*. 2011, č. 1. Dostupné z: http://clanky.rvp.cz/clanek/o/g/12943/DIGITALNI-STOPY-A-DIGITALNI-IDENTITA.html/

[34] BALAŽÍK, Milan. Principy ochrany proti zcizení digitální identity. *Principy ochrany proti zcizení digitální identity*. 2012, č. 1. Dostupné z: http://www.systemonline.cz/it-security/principy-ochrany-proti-zcizeni-digitalni-identity.htm

[35] LÁTAL, Ivo. Počítačová (informační) kriminalita a úloha policisty při jejím řesení. *Počítačová (informační) kriminalita a úloha policisty při jejím řesení* [online]. 1998, č. 3 [cit. 2012-04-20]. Dostupné z: http://www.scritube.com/limba/ceha-slovaca/Potaov-informan-kriminalita-a-1513463.php

[36] ŠKOLNÍK, Jiří. *Počítačové viry*. 2005, 8 s. Dostupné z: http://www.gymnazium.milevsko.cz/dokumenty/mat_ivt/viry.pdf

[37] První phishing v Česku, terčem byla CitiBank. *První phishing v Česku, terčem byla CitiBank*. 2006, č. 1. Dostupné z: http://www.finance.cz/zpravy/finance/63677-prvni-phishing-v-cesku-tercem-byla-citibank/

[38] *Počítačová kriminalita pod lupou*: *Celosvětový průzkum hospodářské kriminality*. 2011. Dostupné z: http://www.pwc.com/cz/en/hospodarska-kriminalita/assets/Crime_survey_CR_czech_ele.pdf

[39] Freshersworld. *Freshersworld* [online]. 2010 [cit. 2012-05-20]. Dostupné z: http://freshersworld.com/blogs/post/10/11/21/10-Most-Dangerous-HACKERS-In-The-World

[40] Science. *Science* [online]. 2010 [cit. 2012-05-20]. Dostupné z: http://science.discovery.com/top-ten/2009/hackers/hackers.html

[41] Hackeři z Lulz Security ohlásili konec činnosti: Bojí se prý odhalení identity. *Http://zpravy.ihned.cz/c1-52175630-hackeri-z-lulz-security-ohlasili-konec-cinnosti-boji-se-pry-odhaleni-identity* [online]. 2011, č. 1 [cit. 2012-05-20]. Dostupné z: http://zpravy.ihned.cz/c1-52175630-hackeri-z-lulz-security-ohlasili-konec-cinnosti-boji-se-pry-odhaleni-identity

[42] Dolphin: Policie. *Dolphi*: *Počítačová kriminalita* [online]. 1998 [cit. 2012-04-20]. Dostupné z: http://www.dolphin.cz/policie/pocitacova_kriminalita.html

[43] 70 % pracovníků využívá PC v práci pro osobní účely. *Podnikatel* [online]. Brno: Profil, 2011, č. 1, 15.11.2011 [cit. 2012-04-20]. Dostupné z: http://www.podnikatel.cz/clanky/pracovnici-vyuzivaji-pc-v-praci-pro-osobni-ucely/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Kč Koruna Česká (měnová jednotka České Republiky)

PC Počítač

PČR Policie České Republiky

MB Megabajt

GB Gigabyte

ČR Česká republika

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: