

Právnická fakulta Masarykovy univerzity v Brně

Katedra trestního práva

Bakalářská práce

POČÍTAČOVÁ KRIMINALITA

Hana Hellebrandová

2006

„Prohlašuji, že jsem bakalářskou práci na téma: Počítačová kriminalita zpracovala sama a uvedla jsem všechny použité prameny“.

.....

Poděkování

Ráda bych chtěla tímto poděkovat vedoucímu mé bakalářské práce prof. JUDr. Vladimíru Kratochvílovi, CSc. za cenné připomínky, rady a odborné vedení při vypracování bakalářské práce.

OBSAH

1	ÚVOD	5
1.1	CHARAKTERISTIKA POČÍTAČOVÉ KRIMINALITY	6
1.2	HISTORICKÁ DOBA POČÍTAČOVÉ KRIMINALITY	7
1.3	DŮVODY VZNIKU POČÍTAČOVÉ KRIMINALITY	9
2	DRUHY POČÍTAČOVÉ KRIMINALITY	10
2.1	DĚLENÍ DLE RADY EVROPY	10
2.2	DĚLENÍ DLE TRESTNĚ PRÁVNÍCH HLEDISEK	11
3	PROTIPRÁVNÍ JEDNÁNÍ PROTI POČÍTAČŮM	12
3.1	ÚVOD K PROBLEMATICE	12
3.2	POŠKOZENÍ A ZNEUŽITÍ ZÁZNAMU NA NOSIČI INFORMACÍ	12
3.2.1	ÚTOK Z VNĚJŠKU SUBJEKTU	12
3.2.1.1	Neoprávněné získání informací	15
3.2.1.2	Zničení, poškození nebo učinění informací neupotřebitelnými	16
3.2.1.3	Zásah do technického nebo programového vybavení počítače	17
3.2.2	ÚTOK ZE VNITŘ SUBJEKTU	17
3.2.3	KOMBINOVANÝ ÚTOK	18
3.2.3.1	Úmyslné jednání umožňující útok	18
3.2.3.2	Neúmyslné jednání umožňující útok	18
4	PROTIPRÁVNÍ JEDNÁNÍ S VYUŽITÍM POČÍTAČŮ	19
4.1	ÚVOD K PROBLEMATICE	19
4.2	PORUŠOVÁNÍ AUTORSKÉHO PRÁVA – SOFTWAREOVÉ PIRÁTSTVÍ	19
4.2.1	NEOPRÁVNĚNÉ UŽÍVÁNÍ SOFTWARE	20
4.2.1.1	Neoprávněné užívání softwaru domácím uživatelem	20
4.2.1.2	Užívání nelegálního softwaru pro komerční účely	21
4.2.2	VÝROBA NELEGÁLNÍHO SOFTWARE	21
4.2.3	ŠÍŘENÍ NELEGÁLNÍHO SOFTWARE	22
4.2.4	NEOPRÁVNĚNÁ INSTALACE POČÍTAČOVÝCH PROGRAMŮ DO NOVÉ VÝPOČETNÍ TECHNIKY	23
4.2.5	FREE SOFTWARE A VOLNĚ DOSTUPNÉ OPERAČNÍ SYSTÉMY	23
4.2.5.1	Free software	23
4.2.5.2	Volně dostupné operační systémy	24
5	INTERNETOVÁ KRIMINALITA	25
5.1	ZÁKLADNÍ ROZDĚLENÍ	25
5.2	ZAKÁZANÁ PORNOGRAFIE	25
5.3	EXTRÉMISTICKÉ PROJEVY	26
5.4	ZNEUŽÍVÁNÍ PLATEBNÍCH KARET A SYSTÉMŮ	27
5.5	PODVODNÉ E-MAILY, SPAMY, HOAXY	27

5.5.1	SPAM	27
5.5.2	HOAX	28
5.6	PHISHING	28
5.7	DIALER	29
5.8	SNIFFING - NEOPRÁVNĚNÉ MONITOROVÁNÍ ELEKTRONICKÉ KOMUNIKACE	30
5.9	DOMÉNOVÉ PIRÁTSTVÍ	30
6__ VYŠETŘOVÁNÍ POČÍTAČOVÉ KRIMINALITY		31
6.1	PACHATELÉ POČÍTAČOVÉ KRIMINALITY	31
6.1.1	AMATÉŘI	31
6.1.2	PROFESIONÁLOVÉ	32
6.2	PODNĚTY K VYŠETŘOVÁNÍ	32
6.2.1	OZNÁMENÍ KONTROLNÍCH , INSPEKČNÍCH A REVIZNÍCH ORGÁNŮ	32
6.2.2	OZNÁMENÍ OBČANŮ	33
6.3	DOKAZOVÁNÍ	33
6.4	TYPICKÉ STOPY	34
6.5	POČÁTEČNÍ ÚKONY	34
6.6	NÁSLEDNÉ ÚKONY	35
6.6.1	VÝSLECH OBVINĚNÉHO	35
6.6.2	VÝSLECH SVĚDKŮ	36
7__ PREVENCE		37
8__ ZÁVĚR		38
9__ RESUMÉ		40
10__ SEZNAM POUŽITÉ LITERATURY		41

1 ÚVOD

Cílem mé bakalářské práce je upozornit na nebezpečnost počítačové kriminality, její masivní rozvoj a aktuální problémy související s touto oblastí. Zároveň bych chtěla poukázat na možná opatření, která je třeba učinit, aby bylo možno tento druh trestné činnosti co nejefektivněji potírat.

Informační a počítačová kriminalita je relativně novým oborem. Elektronické technologie jejich vznik a bleskový vývoj se během posledních desetiletí staly jedním z nejvýznamnějších fenoménů moderní doby. V současné společnosti jsou počítače využívány jako nedělitelná součást každodenního života ve všech oblastech společenských vztahů od obchodu a služeb, přes umění či erotiku a tedy i v oblasti páčání trestných činů a organizovaného zločinu. Tzv. počítačová (informační multimediální) kriminalita patří v současné době mezi nejzávažnější formy trestné činnosti a je také formou nejrychleji se rozvíjející.

Rozsah problematiky počítačové kriminality, dle mého názoru, velmi dobře dokumentuje preambule manuálu pro prevenci a kontrolu počítačového zločinu OSN.

Počítačové systémy nabízejí nové a vysoce sofistikované možnosti porušování práva a především potenciálu pro páčání tradičních typu zločinů netradiční cestou. K ekonomickým škodám, které počítačová kriminalita přináší, je třeba připočíst závislost celého lidstva na počítačových systémech doslova ve všech oblastech denního života.¹

Člověk je stále závislejší na fungování informačních technologií a tudíž roste společenský požadavek na ochranu těchto technologií před zločinci.

Při pojednání o čemkoli z problematiky moderních informačních technologií je třeba mít neustále na paměti jeden základní problém. Dynamika vývoje v této oblasti je natolik závratná, že jakýkoli pokus o teoretické nebo vědecké zkoumání se stane zastaralým již v momentě svého prvního uveřejnění. tzv. permanentní revoluce².

Počítačová kriminalita může postihnout značnou šíři osobního i společenského života. Výpočetní technika je nasazena do řízení a správy státu, v armádě, policii, ekonomice, průmyslu i zemědělství, ve zdravotnictví a jinde. V počítačových systémech jednotlivých institucí se soustřeďují informace ze všech oblastí života společnosti i jednotlivce. Proto poškození funkce počítačových systémů, nejen celostátně budovaných, ale i lokálních může vést k dezorganizaci v mnoha sférách lidské činnosti.

¹ Manuál OSN pro prevenci a kontrolu počítačového zločinu, OSN 1994

² Matějka, M., Počítačová kriminalita, Praha: Computer Press, 2002, str. 4

1.1 Charakteristika počítačové kriminality

Jednoznačně definovat tento pojem je velmi obtížné. "Počítačová kriminalita" je jakýsi "terminus technicus", jímž se označuje skupina trestných činů mající stejný charakter. Stejně tak jako je tomu u pojmů např. hospodářská kriminalita, násilná kriminalita, apod. Obecně lze říci, že počítačová kriminalita je mnohdy i přes své nesporné prvky moderních technologií jen jinou tváří různých standardních trestných činů.

Aby bylo možno hovořit o počítačové kriminalitě, musí pachatel ke svému jednání užít nejen výpočetní techniku, ale jeho jednání musí také naplňovat znaky skutkové podstaty některého trestného činu uvedeného v trestním zákoně³ a nebezpečnost takového jednání musí dosahovat požadovaného stupně nebezpečnosti činu pro společnost⁴.

Má však řadu výrazných znaků, které ji odlišují od kriminality klasické. Zvláštnosti tohoto druhu kriminality vyplývají již ze samé podstaty moderních informačních technologií.

Významným znakem je skutečnost, že zatímco bez výpočetní techniky se musí zločinec, který se např. rozhodne vyloupit banku objevit na daném místě a svůj čin tam fyzicky provést, většinou za použití nebo alespoň pod pohrůžkou násilí, tento jev se u použití moderních technologií výpočetní techniky často vytrácí a pachatel může sedět před obrazovkou počítače tisíce kilometrů daleko a svůj lup si převést na konto do banky během několika sekund. Z policejní praxe vyplývá, že případy počítačové kriminality také obvykle provází nedostatek klasických důkazních materiálů.

Existuje více různorodých pojetí podle toho, z jakého hlediska se jejich autoři na problém dívají.

Rada Evropy definovala „*Computer Related Crime*“ jako nelegální, nemorální a neoprávněné jednání, zahrnující užití nebo změnu dat získaných prostřednictvím VT.

Diskuse, která proběhla u nás v devadesátých letech především, se přiklonila k názoru poprvé publikovaném kolektivem Smejkal, Sokol, Vlček⁵, že pod pojmem „počítačová kriminalita“ je třeba chápat páčání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď:

³ Zákon č. 140/1961 Sb., Trestní zákon, ve znění pozdějších předpisů.

⁴ Čin, jehož stupeň nebezpečnosti pro společnost je nepatrný, není trestným činem, i když jinak vykazuje znaky trestného činu. Stupeň nebezpečnosti činu pro společnost je určován zejména významem chráněného zájmu, který byl činem dotčen, způsobem provedení činu a jeho následky, okolnostmi, za kterých byl čin spáchán, osobou pachatele, mírou jeho zavinění a jeho pohnutkou.

⁵ Smejkal, V., Sokol, T., Vlček, M. Počítačové právo. Praha: C.H.Beck, 1995, 220 str.

- jako *předmět* této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité;
- nebo jako *nástroj* trestné činnosti.

Termín informační kriminalita se užívá při zdůraznění skutečnosti, že trestný čin má vztah k softwaru, k datům, resp. uloženým informacím, nebo obecněji k informačním technologiím.

V poslední době lze však sledujeme odklon od širokého pojmu počítačové kriminality jako celku k jednotlivým dílčím problémovým okruhům s důrazem na podstatu problému, méně již na formu, tedy na to že trestná činnost je páchána počítačem. Počítačové podvody, falzifikace, poškozování dat a programů, neoprávněná užívání hardware, porušování autorských práv jsou již samostatnými specializacemi a překrývají se s jinými fenomény kriminality (hospodářskou majetkovou, organizovanou kriminalitou atd.).

Pojem počítačové kriminalita lze v tomto smyslu chápat tedy jako otevřený systém.

1.2 Historická doba počítačové kriminality

Tak, jak se vyvíjely počítačové a informační technologie, vznikla a dále se vyvíjela počítačová a informační kriminalita. Stav techniky a jejího využívání limitoval i možnosti zločinců, což uvidíme z charakteristiky počátečního období počítačů a počítačových zločinů .

Je mnoho zdrojů, které se zabývají historií fenoménu počítačového zločinu. Pro potřeby této práce jsem vybrala členění, které uvádí ve své knize Michal Matějka⁶:

1. pravěk – období od vynálezu telefonu do uvedení prvního PC na trh v roce 1981
2. středověk – období od roku 1981 do případu Citibank⁷ v roce 1994.
3. novověk – od případu Citibank do doby současné.

Historie počítačové kriminality u nás.

Až do konce 80 let nebylo vůbec možné o počítačové kriminalitě v ČSSR mluvit, neboť informační technologie patřily k embargovanému zboží pro dovoz do zemí socialistického tábora. Situace se změnila koncem 80let, kdy k nám byly, vesměs nelegálně, dovezeny první osmibitové počítače.

Pravděpodobně první čistě počítačový zločin se u nás odehrál v sedmdesátých letech, kdy nespokojený pracovník Úřadu důchodového zabezpečení poškozoval magnetem záznamy

⁶ Matějka, M., Počítačová kriminalita, Praha: Computer Press, 2002, str. 17

⁷ Wilson, C.H., Computer Crime, Případ Citibank, 1999

na magnetických páskách, ale jeho skutečná existence je neověřená (případ měl být kvalifikován jako sabotáž)⁸.

Dalším příkladem je zpronevěra za použití počítače spáchaná v zásilkové službě MAGNET⁹, kdy pracovnice odebírala zboží a v počítači měnila status objednávek učiněných svou matkou z nezaplaceno na zaplaceno.

Jiné způsoby těchto deliktů spočívaly v zasílání faktur na jiné velkoodběratele, manipulace s výplatami apod. Jednalo se o nejčastější odhalený počítačový zločin, jehož podstatou byly manipulace v mzdových účtárnách, odbytech a na jiných pracovištích, kde pracovník měl možnost manipulovat s penězi, jen v osmdesátých letech to bylo 14 případů trestního stíhání¹⁰.

Právní kvalifikace v době předrevoluční se obvykle klonila k § 132 tehdejšího TrZ „Rozkrádání majetku v socialistickém vlastnictví“, zatímco dnes jsou skutky tohoto typu obvykle kvalifikovány jako podvod (§ 250 TrZ) nebo zpronevěra (§ 248 TrZ).

O jiné počítačové nebo podobné trestné činnosti v době sálových počítačů prakticky nelze hovořit, protože komunikace byly v nepřetržitém kolapsu a ty, které fungovaly, byly přísně střeženy. Co nebylo povoleno, to bylo zakázáno nebo přinejmenším netolerováno a netrpěno. Distanční trestná činnost prostřednictvím telekomunikací byla zcela nerealizovatelná snad s výjimkou zasílání výhružných či pomlouvajících dopisů.

Významnou událostí během středověku na území tehdejší už České a Slovenské Federativní Republiky bylo oficiální připojení k internetu 13.2.1992.

Pro období novověku je charakteristické především masivní rozšíření PC s operačním systémem Microsoft Windows a s ním i výrazný nárůst počítačové kriminality ve všech oblastech.

V oblasti průniku do systému došlo k několika zajímavým a počítačovou veřejností široce diskutovaným případům. Prvním z nich byl podvod z roku 1995 v souvislosti s tehdy mohutně sledovanou televizní hrou BINGO¹¹. Počítačový program byl modifikován tak, aby výhru obdržely nastrčené osoby. Pachatel byl souzen pro § 257a TrZ (poškození a zneužití záznamu na nosiči informací) a odsouzen k pěti letům odnětí svobody.

⁸ Smejkal, Vl., Informační a počítačová kriminalita v České republice, MV ČR, 1999

⁹ Matějka, M., Počítačová kriminalita, Praha: Computer Press, 2002, str. 42

¹⁰ Smejkal, Vl., Informační a počítačová kriminalita v České republice, MV ČR, 1999

¹¹ Zelenáková, I., Do České republiky byl vydán jeden z deseti osob obžalovaných v kauze televizní hry BINGO. Dostupný z <http://www.mvcr.cz/aktualit/sdeleni/2001/bingo.html>

Kromě klasického pirátství a hackingu zaznamenala Česká republika za dobu své porevoluční existence několik dalších případů např. hry typu letadlo, trestné podle § 250c TrZ (podvod), padělání platebních karet, šíření dětské pornografie apod.

Pod vlivem rozvoje informačních technologií byly do TrZ zařazeny nové trestné činy v roce 1991 § 257a TrZ (poškození a zneužití záznamu na nosiči informací) nebo roku 1993 § 178 TrZ (neoprávněné nakládání s osobními údaji)¹².

1.3 Důvody vzniku počítačové kriminality

Obecně se v různém pořadí uvádí několik faktorů, které jsou příčinnou informační kriminality, nebo ji připravují živnou půdu. Ve své knize je zmiňuje také Michal Matějka¹³.

„Anonymní“ a pohodlné prostředí, jež nám nabízí židle naproti monitoru. Jinak řečeno, krádež v elektronické bance je v případě znalostí „pohodlnější“, než krádež v kamenné bance s punčochou na hlavě.

Důvěra uživatelů, představuje značný problém, pokud si ji informační technologie (počítač), „dovede“ získat. Jinými slovy, ne každá obchodní transakce může proběhnout bez nežádoucí asistence, ne každý odkaz na webové stránce vede na nezávadný obsah.

Neznalost práva ve společnosti, má za následek bezstarostné jednání, které může být v rozporu se zákonem (kopírování softwaru). „Anonymní“ prostředí nás například na internetu svádí ke skutkům (kopírování původního materiálu, extremistické diskuse, nelegální pornografie) jichž bychom se na veřejnosti nedopustili.

Objem dat a jejich tok je na internetu tak velký a rychlý, že není technicky možné je zaznamenávat a kontrolovat.

Nedokonalost legislativy, je posledním důvodem. Vzhledem k rychlému vývoji informačních technologií a kriminality nemohou zákonné normy pružně reagovat.

¹² Zákon č. 140/1961 Sb., Trestní zákon, ve znění pozdějších předpisů.

¹³ Matějka, M., Počítačová kriminalita, Praha: Computer Press, 2002, str. 17

2 DRUHY POČÍTAČOVÉ KRIMINALITY

2.1 Dělení dle Rady Evropy

Úmluva rady Evropy o počítačové kriminalitě¹⁴ byla publikována dne 23.11. 2001, vstoupila v platnost 1.7.2004 a Česká republika ji podepsala 9.2.2005. Jejím smyslem je mj. sjednotit legislativu evropských zemí, nejen proto, že se jedná o problematiku počítačové kriminality, ale také z toho důvodu, že tato trestná činnost má mezinárodní charakter. Členění podle Rady Evropy je následující:

Do minimálního seznamu trestných činů jsou zahrnovány:

- počítačové podvody,
- počítačové falzifikace,
- poškozování počítačových dat a programů,
- počítačová sabotáž,
- neoprávněný přístup,
- neoprávněný průnik,
- neoprávněné kopírování autorsky chráněného programu,
- neoprávněné kopírování fotografie.

Do volitelného seznamu trestných činů je zahrnuto:

- změna v datech nebo počítačových programech,
- počítačová špionáž,
- neoprávněné užívání počítače,
- neoprávněné užívání autorsky chráněného programu.

Minimální seznam obsahuje taková jednání, která by měla být jako skutkové podstaty trestných činů zapracována do právních řádů jednotlivých zemí, aby bylo možné vést účinný boj proti počítačové kriminalitě. Ve volitelném seznamu jsou uvedena jednání, která by bylo vhodné kvalifikovat jako trestné činy, avšak není to nezbytné.

Pro příklad uvádím tabulku: Srovnání legislativy u nás a v Evropě.

Rada Evropy	Česká republika
počítačové podvody	podvod - § 250, 250a
počítačové falzifikace	?
poškození počítačových dat a programů	poškození a zneužití a programů záznamu na nosiči informací (§ 257a tr.z.)
počítačová sabotáž	sabotáž - § 97, obecné ohrožení - § 179-180, poškozování cizí věci - § 257

¹⁴ Úmluva Rady Evropy o počítačové kriminalitě, Budapešť, 23. listopadu 2001, Convention on Cybercrime - ETS no. 185. Dostupný z <http://conventions.coe.int/>

neoprávněný přístup	neoprávněné užívání cizí věci-§ 249
neoprávněný průnik	neoprávněné užívání cizí věci-§ 249 (?)
neoprávněné kopírování autorsky chráněného programu	porušování autorského práva - § 152
neoprávněné kopírování topografie	porušování autorského práva - § 152, porušování práv k vynálezu a prům. vzoru - § 151, (dále také podle zák. č.529/191 Sb. o ochraně topografií počítačových výrobků)
změna v datech nebo počítačových programech	poškození a zneužití záznamu na nosiči informací (§ 257a tr. z.), zkreslování údajů hospodářské a obchodní evidence - § 125 (?)
počítačová špionáž	vyzvědačství- § 105, ohrožení stát. tajemství - § 106, ohrožení hosp. tajemství - § 122, ohrožení služeb.tajemství - § 173
neoprávněné užívání počítače	neoprávněné užívání cizí věci-§ 249
neoprávněné užívání autorsky chráněného programu	porušování autorského práva - § 152

Tab. 1.: Srovnání legislativy u nás a v Evropě

2.2 Dělení dle trestně právních hledisek

Většinou rozlišujeme dvě hlavní kategorie počítačové kriminality. První je ta, kdy je trestná činnost páchána s využitím počítačů. Druhá kategorie vymezuje nezákonné jednání proti počítačům. Jako samostatnou oblast bych vyčlenila internetovou kriminalitu, tzn. trestnou činnost prováděnou pomocí internetu.

3 PROTIPRÁVNÍ JEDNÁNÍ PROTI POČÍTAČŮM

3.1 Úvod k problematice

V tomto případě pachatel vede útok pouze proti programovému vybavení počítače a uloženým datům. Ten útok může nabýt několika forem. Od nejjednoduššího smazání programového vybavení až po zavedení viru do programového vybavení a následné ztráty programů a dat. Skutková podstata tohoto jednání je vyjádřena v § 257a trestního zákona¹⁵.

3.2 Poškození a zneužití záznamu na nosiči informací

Jako nosič informací je chápáno jakékoliv záznamové médium určené pro informační techniku. § 257a trestního zákona je jediným ustanovením, které je určeno pro informační technologie jako takové a postihuje vysoce kvalifikovanou trestnou činnost.

Objektem trestného činu je nejen nosič informací nebo počítač, ale i nehmotný obsah informací. Tím se zprostředkovaně chrání další zájmy a vztahy, např. projevy osobní povahy, obchodní tajemství, soukromí osob, autorská díla, státní tajemství apod. Trestnou činnost tohoto typu je možno rozdělit na dvě mezní formy. Útok z vnějšku a zevnitř subjektu, který je cílem útoku.

Skutečný útok samozřejmě může být i kombinovaný vedený současně z vnějšku i zevnitř subjektu.

3.2.1 Útok z vnějšku subjektu

S rostoucím počtem uživatelů počítačů a zvyšujícím se objemem přenosu informací prostřednictvím Internetu a e-mailu roste také nebezpečí nákazy počítače a poškození nebo odcizení dat nebezpečnými počítačovými programy.

Touto formou útoku je myšlen tzv. „hacking“¹⁶ čímž se rozumí násilné tj. neoprávněné získání přístupu k datům. Podmínkou je, že výpočetní technika umožňuje připojení z jiného počítače. Trestná činnost je obvykle prováděna tak, že pachatel nebo pachatelé se nepřipojují k počítači přímo, ale přes jeden i více internetových serverů v různých částech světa.

Pachatele tvoří tzv. skupina „hackerů“ - průnikářů, kteří se snaží obejít zabezpečení. Mnoho hackerů tuto činnost provozují jen pro zábavu a proniknutí do systému berou jen jako

¹⁵ Zákon č. 140/1961 Sb., Trestní zákon, ve znění pozdějších předpisů

¹⁶ Michelle Slatalla, Hackers Hall Of Fame, Discovery Online, 1997

určité intelektuální vítězství. Odlišná situace nastává v okamžiku kdy cílem jednání hackera je zisk.

Nástroje používané hackery k získání přístupu k počítači uživatele spočívají v softwaru, který zahrnuje různé nelegální programy pro zjišťování zranitelných míst, programy pro zjišťování hesel a další typy softwaru používaného k prolamování síťových zdrojů nebo k získání neoprávněného přístupu k napadenému systému.

Všeobecně lze nebezpečné programy rozdělit do následujících tří kategorií¹⁷:

- Červi využívají ke svému šíření slabá místa v zabezpečení sítě. Označení „červ“ je používáno kvůli schopnosti těchto programů šířit se mezi počítači pomocí sítě, e-mailu a dalších kanálů. Díky této schopnosti se červi mohou šířit velice rychle. Červ pronikne do počítače, zjistí adresy dalších počítačů a rozešle do nich své kopie. Červi rovněž využívají údaje obsažené v adresářích e-mailových klientů nainstalovaných v infikovaném počítači. Mohou na discích vytvářet pracovní soubory, ale mohou fungovat bez použití prostředků infikovaného počítače s výjimkou paměti. Průnik viru je předběžnou fází, za kterou často následuje průnik dalších nebezpečných programů do napadeného počítače. Červ může například vytvořit zranitelná místa, která později použijí k průniku do počítače trojské koně.

- Viry jsou programy, které napadají jiné počítačové programy přidáním vlastního kódu, takže po spuštění napadeného souboru může virus provést neoprávněnou akci. Tato jednoduchá definice pomáhá určit, že hlavní akce, kterou virus provádí, je *infikování počítačových programů*. Viry se šíří o něco pomaleji než červi.

- *Trojské koně* provádějí neoprávněný přístup k infikovaným počítačům; mohou například vymazat informace na pevném disku, zablokovat systém nebo odcizit důvěrné informace. Přísně vzato trojské koně nejsou viry, protože neinfikují programy ani data a nejsou schopny samostatného šíření do počítačů, ale jsou šířeny uživateli se zlými úmysly jako „užitečný“ software. Přesto však škoda způsobená trojským koněm může být mnohem větší než škoda způsobená útokem klasického viru. Nejrozšířenějším typem nebezpečných programů se v nedávné době stali červi, následovaní viry a trojskými koňmi. Některé nebezpečné počítačové programy splňují vlastnosti dvou nebo dokonce všech tří uvedených kategorií.

Mezi speciální případy infiltrace můžeme zařadit¹⁸:

Adware – kód, který je bez vědomí uživatele vložen do kódu programu a zobrazuje reklamní zprávy. Adwarové programy jsou často používány ke shromažďování osobních

¹⁷ Hák, I.: Moderní počítačové viry, 2005, str. 9. Dostupný z <http://www.viry.cz>

¹⁸ Hák, I.: Moderní počítačové viry, 2005, str. 14. Dostupný z <http://www.viry.cz>

informací o uživateli a jejich odesílání tvůrci programu, změně nastavení prohlížeče (domovská stránka, stránka vyhledávání, úroveň zabezpečení atd.) a přenosu dat, který uživatel nemůže ovlivnit. To vše může vést k narušení zásad zabezpečení a dále k přímým finančním ztrátám.

Riskware – programy, které nemají provádět žádné nebezpečné funkce, ale obsahují bezpečnostní trhliny a chyby a proto je mohou útočníci použít jako pomocnou součást nebezpečného programu. Tento typ softwaru zahrnuje například programy pro vzdálenou správu, klientské programy IRC, programy FTP a různé nástroje pro ukončování nebo skrývání spuštěných procesů.

Spyware – software používaný k získání neoprávněného přístupu k datům uživatele, ke sledování akcí prováděných v počítači a získávání informací o obsahu pevného disku. Tyto programy pomáhají útočnickovi nejen shromažďovat informace, ale také získat kontrolu nad počítačem uživatele. K tomuto typu softwaru patří programy pro sledování klávesových úhozů, programy pro zjišťování hesel a software pro shromažďování důvěrných informací např. čísel kreditních karet.

Programy pro automatické telefonní připojení – programy, které navazují modemové připojení k různým internetovým zdrojům, obvykle pornografickým serverům, zpoplatňovaným za každou návštěvu.

Pouhý fakt, že nepovolaná osoba vnikla do systému, není sám o sobě kvalifikovaný jako trestný čin.

Jednání pachatele trestného činu podle § 257a TrZ spočívá v získání přístupu k nosiči informací a zároveň:

- v neoprávněné užití informací, (§ 257a odst. 1a);
- ve zničení, poškození nebo učinění informací neupotřebitelnými, (§ 257a odst. 1b);
- v zásahu do technického nebo programového vybavení počítače, (§ 257a odst. 1c).

Pokud se však nezjistí a neprokáže, že informace byla použita anebo se její použití chystalo, je trestně právní postih průnikáře omezený. Nebezpečnost takového jednání je zřejmě úměrná úmyslu a kvalitě získané informace.

3.2.1.1 Neoprávněné získání informací

Neoprávněné získání informací a jejich *následné užití* lze považovat za jeden z nejnebezpečnějších útoků na jakákoliv data. Samotné nebezpečí je v tom, že se kvalifikovanému pachateli podaří spáchat tento čin beze stop a bez odhalení správcem dat, což přináší zásadní bezpečnostní riziko pro rozsáhlé databáze různých subjektů.

U této skupiny počítačových deliktů se jedná především o to, že pachatel získá průnikem do systému přístup k datům, která se poté snaží využít ke svému prospěchu. Pokud se například takto dostane k firemnímu know-how¹⁹, případně obchodnímu tajemství, spadá tato činnost pod pojem průmyslové špionáže. Pokud se naopak dostane k informacím o zaměstnancích či klientech oběti, může se jednat o zneužití osobních údajů. V tomto případě se jedná o trestný čin s velkým společenským rizikem, neboť neoprávněné získání údajů například z databází bank či zdravotnických zařízení může vést k velmi nepříjemným důsledkům pro subjekty údajů (vydírání, obtěžování, šíření pomluv aj.). V krajní případě může taková činnost znamenat bezprostřední ohrožení bezpečnosti státu nebo způsobení újmy státu.

Tuto formu trestné činnosti mohou využívat i cizí zpravodajské služby, protože přináší nejmenší riziko odhalení jejich činnosti. Takto spáchaný trestný čin se samozřejmě nemusí vyznačovat pouze kopírováním dostupných dat jako celku, ale i konkrétních fragmentů. V současnosti dochází k zvyšování počtu útoků tohoto druhu.

Pachatel této trestné činnosti může činit nejen zásahy do programového vybavení, ale i přímo změnit podklady nebo vstupní údaje vkládané do počítače. Vždy se jedná o velmi snadnou trestnou činnost, které se může dopustit nejen zaměstnavatel, ale i zaměstnanec.

Celá tato problematika zároveň naráží na nový zákon č.412/2005 Sb.²⁰, o ochraně utajovaných informací a o bezpečnostní způsobilosti. Na tento zákon navazuje nařízení vlády č.522/2005 Sb.²¹ a vyhlášky č.523 až 529/2005 Sb.²² Zde je řešen způsob, jakým je fyzická i právnická osoba povinna chránit utajované informace.

¹⁹ Znalost, informovanost, souhrn poznatků, receptů, výrobních a obchodních znalostí a postupů získaných dlouholetou zkušeností, hospodářský nehmotný statek. viz. <http://slovník-cizich-slov.abz.cz>

²⁰ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nahradil zákon č. 148/1998 Sb., o ochraně utajovaných skutečností.

²¹ Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.

²² Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. Vyhláška č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací. Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. Vyhláška č. 526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti). Vyhláška č. 527/2005 Sb., o stanovení vzorů v oblasti personální bezpečnosti a

Mezi jednotlivé druhy zabezpečení ochrany informací patří i personální bezpečnost. Zde je nastíněna problematika udělení bezpečnostních prověrek, které velmi často organizace podceňují a bez posouzení způsobilosti zaměstnají neprověřený personál, který má přístup k databázím či důležitým programům podniku. Je však nutno podotknout, že další druhy ochrany na sebe navazují a jsou postaveny prakticky vedle sebe a zajištění ochrany informací určuje pochopitelně nejslabší článek, což nezvykle často bývá právě zmiňovaná personální bezpečnost²³.

Tyto postupy využívají státní organizace jako jsou například Policie ČR, Armáda ČR, NBÚ a další subjekty, u kterých je potřebná bezpečnostní spolehlivost.

Poskytnutí dat z informačních systémů bez ohledu na to, zda se tak stalo za úplatu či nikoliv, je v rozporu s ustanovením zákona č.101/2000 Sb.²⁴, o ochraně osobních údajů a taková jednání lze kvalifikovat jako trestný čin neoprávněného nakládání s osobními údaji podle §178 TrZ²⁵.

3.2.1.2 Zničení, poškození nebo učinění informací neupotřebitelnými

Zničení, poškození, změnění a učinění informací neupotřebitelnými podle §257a odst. 1 písm. b) představuje takový zásah do nosiče informací, že se snižuje nebo zcela zaniká hodnota jeho informačního obsahu.

Zničení je charakteristický zásah na nosič informací při němž dojde k fyzickému zničení informace samé.

Při poškození informace nejde o zničení informace v pravém slova smyslu, ale k odstranění části záznamu informací z nosiče nebo k snížení jeho informační hodnoty v důsledku snížení jeho kvality, použitelnosti či rozsahu.

Rovněž může dojít k doplnění informací nových a nežádoucích při zachování stávajících dat.

Poškození může pachatel realizovat fyzicky přímo na nosiči informací nebo softwarově, např. zablokováním dat kódem, narušení souboru virem atp.

bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti). Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací

²³ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

²⁴ Zákon č. 101/2000 Sb., o ochraně osobních údajů a o působnosti Úřadu pro ochranu osobních údajů a o změně některých dalších zákonů., ve znění pozdějších předpisů, který nabyl účinnosti dnem 1.6.2000.

²⁵ Zákon č. 140/1961 Sb., Trestní zákon, ve znění pozdějších předpisů

Některou trestnou činnost lze snadno zjistit. Příkladem nám mohou být vizuální změny webových stránek. Někdy má tato činnost podtext poukázání schopností pachatele anebo v horším případě se jedná o záměrné poškození dat firmy či osoby. Útok závisí na etickém smýšlení pachatele. Někteří hackeři takto poukazují na některá slabá místa v zabezpečení systému a nechávají prostor k nápravě správci sítě. I při dobré vůli jednotlivců se jedná o trestné činy, které sebou nesou mnohdy finanční následky. Ochranou před takovou činností je pravidelné zálohování dat. V případě, že je to možné provádí se záloha na nosič, který je následně uložen na zabezpečeném místě mimo systém. V případě totálního selhání máme tak jedinou funkční zálohu pro obnovu informací²⁶.

3.2.1.3 Zásah do technického nebo programového vybavení počítače

Tento zásah může znamenat dočasné nebo trvalé ochromení činnosti počítače nebo telekomunikačního zařízení zablokováním funkce příslušných programů, přístupu k datům uloženým v paměti počítače tak, že bude porušena kontinuita komunikace mezi jednotlivými zařízeními, jejichž funkčnost bude značně omezena.

Všeobecně závisí na zabezpečení technického a programového vybavení. Pokud se tato problematika podcení může dojít k jejímu narušení vlivem soustředěných útoků nebo virů (např. trojské koně, backdoory apod.). Z toho vyplývá, že ve stejné rovině jsou posazeny jak technické a programové vybavení, tak i lidský faktor. Tento element je nejslabším článkem, proto si zasluhuje při konfiguraci zařízení či systému nejprísnejší důslednost.

3.2.2 Útok zevnitř subjektu

Pozice pachatele stojícího uvnitř subjektu je podstatně jednodušší. Pachatel vychází ze znalosti vnitřního systému, což ho podstatně odlišuje od mimo stojícího útočníka, který disponuje jen těmi informacemi, které sám při testování systému nebo při samotném útoku zjistí

Tato osoba obvykle navíc disponuje dle své pozice i určitou úrovní oprávnění přístupu k výpočetní technice nebo k informačnímu systému a těchto výhod pak zneužívá k samotnému trestnému činu. Pachateli uvnitř subjektu mnohdy nahrává i úroveň vnitřní informační bezpečnosti. Zaměstnanci těchto subjektů jsou vystaveni značnému pokušení, jak poměrně jednoduchým způsobem získat značný finanční prospěch. Relativní jednoduchost takového činu spočívá ve znalosti systému a vlastnění přístupových práv. K tomu se přidávají

²⁶ Bitto, O., Časopis Computer č.3, Brno: Computer Press, 2006, str. 82

další faktory, kdy zaměstnanci zodpovědní za bezpečnost a výpočetní techniku nesplnili své povinnosti nebo podcenili hrozící nebezpečí. Jestliže přístup k terminálu vnitřního systému není kontrolován, pohyb zaměstnanců je naprosto volný včetně příchodů a odchodů ze zaměstnání a přístupové oprávnění zná více osob je odhalení pachatele takového útoku velmi problematické. Ale i přes výše zmíněné nedostatky je problém útoků zevnitř systému řešitelný lépe než útok z vnějšku, neboť vždy je zde omezený okruh pachatelů.

3.2.3 Kombinovaný útok

Je útok vedený současně z vnějšku i zevnitř subjektu. Tyto útoky pak můžeme dále rozdělit na úmyslné a neúmyslné.

3.2.3.1 Úmyslné jednání umožňující útok

Zde dochází k selhání osoby, která má přístup k internímu zabezpečení systému.

V tomto případě dochází k předání informací a poznatků o systému a jeho slabých místech osobou, která „pouze“ poskytne tyto údaje pachateli z venku pro snadnější průnik do systému, ale sama tuto činnost neprovádí.

3.2.3.2 Neúmyslné jednání umožňující útok

Neúmyslné jednání spočívá v nevědomém nainstalování programu většinou již zmíněných „backdoors“²⁷.

Po nainstalování tento program umožní osobě mimo firmu mít kontrolu nad počítačem uvnitř celého systému, z kterého se lze mnohem snadněji dostat k žádaným datům. Hlavní příčinou je neznalost uživatelů, kteří bez sebemenších pochybností a kontroly takové soubory otevírají. Vzhledem k tomu, že z hlediska trestnosti se musí jednat o úmyslný útok, není toto jednání trestně postižitelné, ačkoli škody způsobené nevědomým nainstalováním tohoto typu programu mohou mít stejné destruktivní následky jako stejný typ jednání s prokázaným úmyslem.

²⁷ Hák, I.: Moderní počítačové viry, 2005, str. 10. Dostupný z <http://www.viry.cz>

4 PROTIPRÁVNÍ JEDNÁNÍ S VYUŽITÍM POČÍTAČŮ

4.1 Úvod k problematice

V tomto případě chápeme informační technologii jako nástroj k usnadnění nezákonné činnosti. Většinou se jedná o porušování Autorského zákona²⁸ (nedovolené kopírování a zneužívání softwarových produktů, hudebních nosičů aj.)

4.2 Porušování autorského práva – softwarové pirátství

Z právního pohledu je software považován za nemotný statek - autorské dílo. Nositeli práv k software jsou jeho autoři, případně firma v níž byl utvořen. Autorský zákon stanoví, že ke každému užití autorského díla je nutný souhlas nositele autorských práv. Jedinými výjimkami je pořízení archivní a záložní kopie nebo pořízení kopie programu nezbytné pro provoz programu na počítači, pro nějž byl program určen. Veškeré kopie software, které nejsou povoleny autorským zákonem a licenčním ujednáním, je nutno považovat za nelegální kopie, znamenající porušení zákona i smlouvy.

Jako softwarové pirátství se označuje takové jednání uživatelů software, které je v rozporu s licenční smlouvou, a také neautorizované používání nebo reprodukce materiálů, na které se vztahuje copyright, osobou nebo subjektem, která k této činnosti nebyla autorizována.

Za porušování autorského práva v organizaci je odpovědný každý, kdo úmyslně autorské právo porušil vlastním jednáním, tj. např. věděl, že jde o nelegální kopii softwaru a přesto ji používal. Účastníkem na tomto trestném činu, kterému hrozí tentýž trest jako hlavnímu pachateli, je ten, kdo nelegální používání softwaru organizoval, naváděl k němu a poskytoval k němu pomoc²⁹.

Za hlavní druhy tohoto pirátství lze považovat nelegální provozování počítačových programů, plagiátorství, neoprávněnou tvorbu a šíření národních verzí počítačových programů a jejich doprovodné dokumentace, šíření pirátských rozmnožení počítačových programů a jiných autorských děl.

Trestní odpovědnost softwarového pirátství je založena především na základě ust. §152 TrZ (porušování autorského práva), ale i §150 TrZ (porušování práv k ochranné známce,

²⁸ Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)

²⁹ Jelínek J. Trestní právo hmotné, Obecná část, Praha: Linde, 2004, str.277

obchodnímu jménu a chráněnému označení původu), §151 TrZ (porušování průmyslových práv) a § 149 TrZ (nekalá soutěž)³⁰.

4.2.1 Neoprávněné užívání softwaru

Typickým příkladem toho druhu trestné činnosti je používání software na větším počtu počítačů, než pro jaký byla zakoupena licence, případně provozování software zcela bez zakoupení licencí. V těchto případech se bere v potaz, zda se užíváním software dosahuje dalšího zisku, či jde o finanční úsporu. Každé neoprávněné užívání softwaru de facto přináší svému uživateli zisk, totiž částku, kterou by za daný software zaplatil, kdyby si ho řádně koupil. Trestní zákon v §152 TrZ nerozlišuje „běžného pachatele“ a „domácího uživatele“.

K posouzení společenské nebezpečnosti je však vhodné rozlišovat případ, kdy nějaký jedinec užívá software doma pro svou osobní potřebu, od případů ostatních, kdy program neoprávněné užívá právnická osoba nebo fyzická osoba v rámci své komerční činnosti.

Tyto případy je ještě možné rozdělit na případy, kdy se užíváním daného programu dosahuje dalšího zisku a případy, kdy je jediným ziskem úspora kupní ceny.

4.2.1.1 Neoprávněné užívání softwaru domácím uživatelem

Neoprávněné užívání počítačových programů pro soukromou potřebu je nejrozšířenějším činem, který lze zařadit mezi čistě počítačovou kriminalitu. Neoprávněné užívat počítačové programy se v ČR stalo po roce 1989 běžným zvykem. Podle statistik³¹ dosahovala míra používání nelegálního softwaru až 80%. Dnes sice patří Česká republika se zhruba 40% mezi 20 států s nejnižším softwarovým pirátstvím ovšem jako alarmující bych označila fakt, že softwarové pirátství se stále častěji objevuje, i přes zvýšenou osvětu již na základních školách, kde dochází k masivnímu porušování zákona žáky, kteří si mezi sebou počítačové programy běžně půjčují, vyměňují a prodávají. Tato situace zakládá negativní důsledky do blízké budoucnosti, protože „vychovává“ nejmladší generaci k porušování autorských práv, které se tak stává normální. Starší generace na druhou stranu takové jednání často nepovažuje za nemorální, proti svým potomkům nezasahuje, nýbrž je v jejich činnosti ještě podporuje.

³⁰ Zákon č. 140/1961 Sb., Trestní zákon, ve znění pozdějších předpisů

³¹ Business Software Alliance. Dostupný z <http://www.bsa.org/czechrepublic/antipiracy/statistiky.cfm>

4.2.1.2 Užívání nelegálního softwaru pro komerční účely

V komerční oblasti dochází k podobným problémům jako v oblasti domácích uživatelů. Základním rozdílem je především množství informačních technologií používaných jednotlivci pro komerční účely a specifika v jejich využití.

Obvyklým případem je jednání, kdy podnikatel buď získá nelegálně software a užívá ho, nebo, a to je nejčastější případ, zakoupí menší množství licencí, než pak ve skutečnosti užívá. Přitom se nejedná o žádné náhodné instalace nelegálního softwaru, jde kolikrát o desítky kopií v mnoho pobočkách. Kromě vysokých peněžitých trestů, propadnutí věci či dokonce trestů odnětí svobody do výše až pěti let hrozí takovým firmám platby vysokých finančních částek poškozeným softwarovým firmám. Ty mohou požadovat až dvojnásobek licenčních poplatků. Navíc si musí viník samozřejmě legální software řádně zakoupit, pokud jej chce dále užívat. Uhrazením vzniklé škody totiž nedojde k legalizaci již užívaného nelegálního softwaru. Negativním faktorem je vztah k řešení problému ze strany subjektů, které přímo prodávají licence k užívání počítačových programů, případně i zajišťují servis. Tyto společnosti a jednotlivci stojí na prodejním žebříčku mezi autorem nebo vykonavatelem autorských práv na území ČR a konečným uživatelem. Stává se, že zákazník, užívající více licencí než zakoupil, požaduje na nelegální instalace servisní zásahy a je mu vyhověno. Prodejci a jejich servisní složky tak disponují s informacemi o nelegálním užívání počítačových programů, a přitom nejsou zásadním způsobem motivováni k odstranění tohoto problému³².

4.2.2 Výroba nelegálního software

Výrobu nelegálního softwaru můžeme rozdělit na výrobu průmyslovou, kdy pachatel potřebuje zvláštní vybavení, odlišné od vybavení běžného uživatele, případně musí zadávat tovární výrobu, kde deklaruje svou osobu jako nositele nebo vykonavatele autorských práv, a výrobu domácí, k níž pachatel nepotřebuje žádné výrazně odlišné vybavení v porovnání s běžným počítačem, ale stačí mu tzv. vypalovací mechanika. Na začátku 90.let převažovala hlavně výroba průmyslová, což znamenalo masový růst kopírovacích společností, jejichž činnost byla mnohdy na hranici a ještě častěji za hranici zákona. Zákon byl často ignorován nebo vědomě porušován.. Kopírovací služby stojí však v současnosti již mimo masivní zájem zákazníků. Důvod je zřejmý. Vývojem nových technologií a jejich cenovou dostupností má

³² Trestný čin porušování autorského práva podle § 152 tr. zákona není zařazen mezi trestné činy, jejichž neoznámení nebo nepřekážení by bylo samo o sobě trestným činem.

většina uživatelů možnost i v domácím prostředí vyrábět kopie originálů na první pohled totožné s předlohou. Je samozřejmě dnes již běžnou záležitostí, kdy sama mechanika podporuje „vypálení“ potisku na samotné medium.

Nelegální software se také vyrábí tzv. *klonováním disků*³³, kdy se pomocí odpovídajících programů vyrábí přesná kopie obsahu disku i se všemi nainstalovanými programy na disk jiného počítače. Lze čekat problémy s registrací produktů nebo značek klonovaných disků. Díky různým programům v síti internet lze však lehce problém s registrací obejít. Samozřejmostí je, že takové obcházení je porušování autorských práv.

Dnes se v masovém měřítku klonují filmové a zvukové nosiče. Zejména pak filmy na DVD způsobují velké ztráty filmovým společnostem. Někteří obchodníci tuto činnost provádějí a distribuují ji za podstatně nižší cenu než je za originální nosič. Někteří domácí uživatelé rovněž provozují tuto činnost, protože je cenově příznivější půjčit si film od známého a provést jeho věrnou kopii než si zakoupit originál. Porušení zákona je zřejmé a porušení etického kodexu raději nebudeme vůbec rozebírat.

4.2.3 Šíření nelegálního softwaru

U prodeje a šíření nelegálního software jde o úmyslné porušování zákona ze strany osob provádějících tuto činnost. Internet je dominantním prostorem výměny informací o programech i vlastních programů. V komunikaci internetových uživatelů je častým tématem „vzájemná pomoc“ při řešení problémů s nelegálním softwarem jeho umístěním na konkrétní internetové adrese nebo získáním tzv. cracku³⁴.

Pokud uživatel zatouží po nelegálním softwaru, má na výběr hned z několika cest směřujících k jeho cíli. Za klasiku již můžeme považovat vystavení dat na veřejných FTP³⁵ serverech, odkud si kdokoliv může zdarma a bez okolků stáhnout vše potřebné. Bohužel i bohudík, záleží na úhlu pohledu, rychlost takovéhoho připojení nedosahuje závratných výšin, takže stažení jednoho CD nebo dokonce DVD zabere delší dobu. Řada FTP serverů dokonce funguje čistě pro tento účel, kdy se provozovatelé snaží zřít svému dílu odpovědnosti „pouhým“ poskytnutím nahrávání a stahování dat neomezenému okruhu uživatelů. Jiná situace nastává v oblasti velice oblíbených P2P (peer to peer)³⁶ sítí, kde lze s trochou štěstí a

³³ Ke klonování se používají často dostupné programy Clone DVD/CD, DVD Shrink, NERO apod.

³⁴ Crack – program, který po svém spuštění odstraní ze systému ochranu z chráněné aplikace

³⁵ FTP – File Transfer Protokol. Služba umožňující kopírovat soubory ze vzdáleného systému na Internetu na jejich systém.

³⁶ P2P výměnné sítě jsou postaveny na tzv. „rovnosti“ uživatelů, kdy spolu komunikují přímo jednotliví klienti (uživatelé).

umu stahovat data rychlostí v řádu megabajtů za vteřinu. Decentralizované výměnné sítě navíc mají větší šanci na přežití, než tomu bylo například v případě průkopnického Napsteru³⁷. V současnosti je řád věcí takový, že díky výměnným systémům DC++, BitTorrent, iMesh³⁸ a jim podobným má každý uživatel nelegální software na dosah ruky. Ponecháme-li na chvíli stranou etické hledisko rozkrádání softwaru, můžeme prozkoumat i stránku technických rozdílů mezi pirátskou a originální podobou aplikace. Při stahování ilegálního softwaru z pochybných a zakázaných vod internetu si uživatel nemůže být jist, zda ve stažené verzi aplikace nejsou implementovány nějaké další funkce, jako jsou například „zpečná vrátka“, viry apod.³⁹ Další markantní rozdíl spočívá v technické podpoře, která je charakteristická právě pro legální software.

4.2.4 Neoprávněná instalace počítačových programů do nové výpočetní techniky

Klasičtí vypalovači nelegálního softwaru, kteří šířili seznamy s pirátskými kopiemi, jsou na ústupu a nahrazují je sofistikované formy pirátství právě prostřednictvím internetu. To, že se jedná o nelegální počítačové programy, je někdy zřejmé, někdy však například e-mailem lidé obdrží profesionálně vypadající nabídku značkového softwaru, který lze stáhnout za podezřele nízké ceny. Tito šejdiři si dávají velmi záležet na tom, aby vytvořili iluzi, že lidé stahují originální, zcela legální verze softwaru. Běžnou fintou je prodej softwaru jako tzv. OEM verze softwaru. Jedná se o software, který je levněji prodáván jako součást zakoupeného hardware. Pokud podnikatelé využítí nabídky takových nekorektních prodejců, před možnými postihy je to neuchrání.

4.2.5 Free software a volně dostupné operační systémy

4.2.5.1 Free software

Svobodný software se překládá do angličtiny jako *Free Software* (*free speech, not free beer*). Samotné *free software* má v angličtině však také druhý význam, který znamená software zadarmo, tedy něco zcela odlišného. Tomu se však obvykle říká *freeware*.

Za získání kopií svobodného software můžete platit, nebo je obdržet zdarma, ovšem bez ohledu na způsob, jak jste je získali, máte vždy svobodu kopírovat a měnit software, dokonce prodávat nebo darovat jeho kopie nebo pozměněné verze.

³⁷ Matějka, M., Počítačová kriminalita, Praha: Computer Press, 2002, str.37

³⁸ Bitto, O., Časopis Computer č.3, Brno: Computer Press, 2006, str. 82

³⁹ Červeň, P., Cracking a jak se proti němu bránit, Brno: Computer Press, 2003

4.2.5.2 Volně dostupné operační systémy

V roce 1984 založil Richard Stallman projekt GNU⁴⁰, aby tak vytvořil kompletní unixový operační systém založený na svobodném software. Na platformě UNIXu byl vystavěn operační systém LINUX. Název je složeninou slov Linus (křestní jméno autora Linuse Torvaldse) a Unix. Jádro Linuxu je volně šiřitelné (public domain) podle pravidel GNU General Public License. Původně byl vytvořen pro počítače typu IBM PC s procesorem i386 a vyšším, v současnosti ale existují i verze pro jiné architektury (např. MIPS, Sun Sparc, DEC Alpha/AXP aj.). Hlavní výhodou Linuxu oproti komerčním operačním systémům (MS Windows apod.) je jeho nulová cena (platí se pouze jeho distribuce), snadno dostupný základní software (většinou rovněž volně šiřitelný) a kvalitní dokumentace. Je používán převážně jako operační systém provozující internetové servery, kde se svými nízkými pořizovacími náklady představuje alternativu systémů firmy Microsoft⁴¹. Stále častěji je Linux používán také na běžných domácích počítačích.

⁴⁰ Nadace pro svobodný software v copyleft en:GNU General Public License a en:GNU Lesser General Public License

⁴¹ Microsoft je americká společnost, která sídlí v městě Redmond. Vznikla v roce 1975, kdy ji založili Bill Gates a Paul Allen.

5 INTERNETOVÁ KRIMINALITA

Současná praxe internetové kriminality v ČR je poměrně rozvinutá, ať už se týká kriminálních činů, v nichž hraje internet hlavní a jedinou roli, nebo rozsáhlejších deliktů, ve kterých je internet součástí komplexnější trestné činnosti. V největší míře se jedná o mravnostní trestné činy, projevy extremismu, útoky na data, finanční podvody, atd.

5.1 Základní rozdělení

1. Zakázaná pornografie
2. Extrémistické projevy
3. Zneužití platebních a obchodních systémů v síti Internet
4. Podvodné e-maily, spamy, hoaxy
5. Phishing
6. Dialer
7. Sniffing – monitorování elektronické komunikace
8. Doménové pirátství

5.2 Zakázaná pornografie

Témata s erotickou, pornografickou a sexuální tematikou patří na Internetu k tomu nejvyhledávanějšímu a nejžádanějšímu. Ne všechny kategorie se však vejdu do zákonného rámce. Sice se nezvýšil počet osob, kteří takovou činnost páchají, ale razantně se zvýšil počet útoků, kdy uživatel rychle zaplaví nějakým materiálem celý svět. Z hlediska české právní úpravy je otázka šíření pornografie řešena v § 205 TrZ (ohrožování mravnosti). Podle této úpravy je trestná výroba a distribuce pornografických materiálů, ve kterých jsou znázorněny násilné a lidskost ponižující činnosti ,styky s dětmi a zvířaty, případně jiné patologické sexuální praktiky, dále je trestné zpřístupňování jakýchkoli pornografických materiálů nezletilým⁴².

Za nejzávažnější problém bych zde označila šíření dětské pornografie. Rozvoj nových technologií, snazší dostupnost internetu ale také určité zdání anonymity a nepostižitelnosti přispívá i k rychlému šíření dětské pornografie.

⁴² Matějka, M., Počítačová kriminalita, Praha: Computer Press, 2002, str.66

Distribuce materiálů s dětskou pornografií či navazování kontaktů mezi pedofily a dětmi je nyní v snazší než kdykoli dříve. Odkazy se objevují přímo ve vyhledávačích.

Situace je velmi usnadněná i laxním postojem rodičů dětí, kteří bagatelizují nebezpečí, kterým je jejich dítě ohroženo. Přitom právě podněty ze strany veřejnosti by vysokou měrou mohli ovlivnit odhalování této trestné činnosti.

Vyšetřování podobných případů je přitom velmi náročné a policisté jsou odkázáni na to, jak budou ochotni provozovatelé free-webů spolupracovat. Servery totiž nic nenutí podobné případy hlásit a nechtějí se zbytečně zatěžovat administrativou a komunikací s úřady.

Držení podobných materiálů totiž není trestné. Policie musí prokázat další šíření těchto souborů. To by měl změnit nový trestní zákoník. Postižen tak bude i ten, kdo bude mít dětské porno v počítači. Podle nové právní úpravy budou trestně stíháni všichni pedofilové, kteří mají dětské porno pouze u sebe v počítači⁴³.

5.3 Extrémistické projevy

Institut pro kriminologii a sociální prevenci ministerstva spravedlnosti chápe extremismus jako: *Souhrn určitých sociálně patologických jevů vytvářených více či méně organizovanými skupinami osob.*

Internet, jako ideální prostředek rychlé, pohodlné a efektivní komunikace, nahrává také různým extrémistickým skupinám, jako jsou například neonacisté, komunisté, anarchisté či militantní náboženské sekty.

Internet slouží extremistům především jako:

- nástroj pro propagandu a pro komunikaci s případnými zájemci o hláсанou propagandu;
- nástroj pro spojení a konspiraci, které může následně vyústit v nezákonnou činnost, jde tedy o formu přípravy k trestnému činu. Typickým případem může být např. mailová či chatová domluva o provedení útoku na romskou či přistěhovaleckou komunitu v určitém městě apod.

Internet je takový, jaká je společnost. Podstatné ale je, aby díky propracovanosti a organizovanosti určité aktivity nebyly za využití technologií vydávány masivně, respektive s nějakým masivním účinkem, který je založen na porušování práv jiných osob či skupin obyvatelstva.⁴⁴

⁴³Kopta, M., Dětská pornografie - problém Internetu, Lupa, 2004. Dostupný <http://www.lupa.cz/clanky/>

⁴⁴ Ambrož, J., Jak silná je naše softwarová policie, Lupa, 2005. Dostupný z <http://www.lupa.cz/clanky/>

5.4 Zneužívání platebních karet a systémů

Zneužívání platebních karet a obchodních systémů souvisí především s rozvojem internetové komerce. Platba kartou je i v české republice velmi rozšířeným způsobem, ale i přes neustálou snahu mnoha firem o vývoj nových bezpečnostních prvků nelze její zabezpečení zcela zajistit.

Vzhledem k tomu, že pomocí platební karty lze nezdědka získat i přístup k celému bankovnímu účtu a způsobit tak majiteli nemalé škody, velmi rychle vznikají nové a nové postupy a metody i ze strany pachatelů od klasické krádeže, nelegálně vyrobených padělků, změnu některých údajů na platební kartě, přes nejčastěji používanou techniku s relativně minimálním rizikem prozrazení. Pachatelé většinou vyberou bankomat se samoobslužnou zónou, kde na čtecí zónu, která slouží pro vstup do zóny, namontují zařízení, které může kopírovat magnetické proužky. Poté využijí jakoukoliv plastickou kartu s magnetickým proužkem, a nahrají na ně okopírovaný záznam. PIN nutný k neoprávněným výběrům této karty z bankomatů pachatelé zjistí pomocí mikrokamery, kterou pomocí magnetu uchytí na bankomatu.

Výše popsané jednání se dá kvalifikovat a trestně stíhat jako trestné činy podle:

§ 140 TrZ padělání a pozměňování peněz s odkazem na § 143 TrZ neboť platební karta požívá ochrany též jako bezhotovostní platební prostředek.

§142 TrZ výroba a držení padělatelského náčiní

§249bTrZ neoprávněné držení platební karty

§250 TrZ podvod

5.5 Podvodné e-maily, spamy, hoaxy

5.5.1 Spam

Spamy, nebo-li nevyžádaná pošta (obvykle jde o reklamní nabídky) zaplavují schránku a omezují uživatelské soukromí. Policie se spamy v podstatě nezabývá, jelikož samotné rozesílání této nevyžádané pošty není kvalifikováno jako trestný čin. Odpovědnost spadá na Úřad pro ochranu osobních údajů⁴⁵, na který se mohou lidé obracet.

⁴⁵ Úřad pro ochranu osobních údajů (ÚOOÚ) je nezávislým orgánem, který:
Provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů;
vede registr povolených zpracování osobních údajů;
přijímá podněty a stížnosti občanů na porušení zákona;
poskytuje konzultace v oblasti ochrany osobních údajů.

5.5.2 Hoax

Hoaxy, nebo-li poplašné e-maily, jsou rovněž na Internetu běžně přítomny. Obvykle obsahují nepravdivý, šokující či citlivý obsah, který obvykle varuje před neexistujícím nebezpečným virem. Využívá neznalosti a nezkušenosti uživatelů, kteří je rozšiřují dále. Nejen, že šíří poplašné zprávy, omezují soukromí, ale také zatěžují servery. Ve většině případů se jedná o nemorální chování, ale existují také hoaxy ryze nezákonné – výzvy k finančnímu plnění apod. Těmto se dostalo označení „nigerijské dopisy“.

Tématicky se může jednat o různé druhy zpráv od méně nebezpečných, jako jsou varování o počítačových virech (virus hoaxes), kde se ve většině případů pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů „IBM a FBI varují“ nebo „Microsoft upozorňuje“ atd. a poté informuje uživatele, co vše jim tento virus může provést, po varování mnohem nebezpečnější, které využívají strach uživatelů. Jsou to e-maily které hovoří například o nastrčených stříkačkách infikovaných virem HIV v kinech či divadlech nebo varování o rakovinových látkách obsažených v šamponech apod.

Trestnost takového protiprávního jednání naplňuje skutková podstata §199 TrZ (šíření poplašné zprávy), ale jen v případě pokud je pachateli prokázán úmysl takového jednání.

5.6 Phishing

V zahraničí se velmi rozmohly podvody prostřednictvím e-mailové pošty, tzv. phishing. V České republice se phishing někdy překládá jako „rhybaření“. Zjednodušeně řečeno, phishing většinou (není podmínka) začíná e-mailem, který se do posledního detailu tváří jako by pocházel z nějaké instituce (častokrát nějaké banky apod.). V e-mailu je odklik na stránku s podvrženým obsahem. Tam se od „obětí“ žádá vyplnění hesla, čísla kreditní karty, čísla účtů apod. údajů. Ty pak samozřejmě nejsou odeslány do banky ani do jiné instituce, ale přímo do rukou útočníků za jediným účelem – zneužití. Pravděpodobně poprvé se do České republiky dostal masivní případ phishingu v březnu tohoto roku, v podobě falešného mailu od Citibank. Jednalo se o krátké oznámení o příjmu 2000 (v neurčené zahraniční měně) na váš účet. Abyste potvrdili příjem této částky, máte podle instrukcí v e-mailu kliknout na uvedený odkaz a zadat vaše přihlašovací údaje.



obr.1. Případ Citibank

Po kliknutí na odkaz se skutečně otevře stránky Citibank, nicméně k tomu dojde přesměrováním z domény czechrepublic-online.com a kromě hlavního okna se skutečnými stránkami Citibank se otevře i vyskakovací okno, které však již nemá se Citibank nic společného. Zde jste pak vyzváni k zadání přístupových údajů do Citibank a tyto údaje jsou poté odeslány podvodníkovi, který může váš účet zneužít. Jediná cesta je nedůvěřovat, přemýšlet nad každou zvláštností a informace si ověřovat.

5.7 Dialer

Dialer je program, který změní způsob přístupu na Internet prostřednictvím modemu. Místo běžného telefonního čísla pro internetové připojení přesměruje vytáčení na čísla se zvláštní tarifací, např. 60 Kč / minutu tzv. „žluté linky“. V některých případech se tak děje zcela nenápadně nebo dokonce automaticky. Dialer může být na PC vypuštěn návštěvou „nevhodné stránky“ např. pornografické, například za využití technologie ActiveX, takže problémy mohou nastat především uživatelům Internet Exploreru. V jiném případě může jít o nenápadný spustitelný soubor *.EXE, který je nic netušícímu uživateli vnucován ke stažení klasickým dialogem (mluvíme-li o prohlížeči Internet Explorer). Z trestního hlediska je možno tuto činnost kvalifikovat jako trestný čin podle § 250 TrZ (podvod) nebo § 257a (poškození a zneužití záznamu na nosiči informací).

5.8 Sniffing - neoprávněné monitorování elektronické komunikace

Sniffing je technika, při které dochází k ukládání, následnému čtení a odposlechu datové komunikace, subjektem, který není jejím adresátem. Cílem této činnosti je získání přístupu k veškerému obsahu nešifrované komunikace jako jsou např. přístupová hesla a jména, obsah e-mailů a další soubory posílané pomocí internetu. Tato činnost je trestná podle § 239 TrZ, (porušování tajemství dopravovaných zpráv), případně podle § 240 TrZ. Jestliže však pachatel užije tyto informace pouze pro vlastní potřebu, je jeho odhalení velmi složité. Ochrana je tedy závislá především na samotném uživateli v důsledné prevenci, především v šifrování své komunikace po internetu.

5.9 Doménové pirátství

Co vlastně doména neboli doménové jméno z právního hlediska znamená? Obecně řečeno, jedná se o způsob označení internetových stránek. Doména je nesporně součástí duševního vlastnictví a podle našeho názoru se řadí na úroveň ostatních označení, jako jsou obchodní firma či ochranná známka. Vždyť koneckonců právě tyto instituty jsou používány při ochranně doménových jmen tam, kde praxe ochrany doménových jmen nestačí.

Doménové pirátství spočívá v tom, že si vyhlédnete zaregistrovanou doménu, která je výhodná pro obchodní či jinou činnost. Avšak místo toho, abyste kontaktoval jejího majitele a pokusil se doménu koupit, zamíříte na Úřad průmyslového vlastnictví⁴⁶. Tam si zaregistrujete ochrannou známku stejného jména, jako je jméno domény.

Mezi nejznámější případy patří zřejmě spor o doménu oskar.cz, kterou měla zaregistrována firma Comfor. O tuto doménu měla zájem firma Český mobil. Comfor požadoval za převedení této domény deset miliónů korun. 28. dubna 2003 se stal držitelem domény oskar.cz Český Mobil. Nestalo se tak však vítězstvím v soudním sporu, ale v rámci mimosoudního vyrovnání, které mezi Českým Mobilem a původním majitelem domény proběhlo.

⁴⁶ Úřad průmyslového vlastnictví rozhoduje o poskytování ochrany na vynálezy, průmyslové vzory, užité vzory, topografie polovodičových výrobků, ochranné známky a označení původu výrobků.

6 VYŠETŘOVÁNÍ POČÍTAČOVÉ KRIMINALITY

V trestním právu ČR jsou zásady trestního řízení stanoveny již základními zákony, další zásady stanoví trestněprávní předpisy, především Trestní zákon a Trestní řád⁴⁷.

Počítačová kriminalita je páchána skrytě ve specifickém prostředí počítačových systémů a počítačových sítí a jako taková má i svá specifika.

6.1 *Pachatelé počítačové kriminality*

Pachateli trestných činů bývají obvykle osoby se středoškolským, jiným vyšším nebo vysokoškolským vzděláním, zejména v technických oborech, speciálně v oboru informačních technologií, často nadprůměrně inteligentní, vynalézavé, zejména ve specifické programátorské oblasti, zneužívající svého vyššího výsadního postavení v zaměstnání s tomu odpovídající pravomocí, ve svém pracovním zařazení nebo ohodnocení neuspokojení, jejich protiprávní jednání je vzdáleno tradičním hrubým formám delikvence, neobsahuje prvky násilí. Pokud se jedná o motiv jejich jednání, u nás zatím zcela jednoznačně převažuje touha po zisku.. Existují však i jiné motivy např.pocit beztrestnosti , kompenzace nedostatečného ocenění práce, ale i touha po riziku a dobrodružství.

Z hlediska vztahu pachatelů k informacím bychom je mohli dělit na amatéry a profesionály

6.1.1 Amatéri

Jsou to osoby pronikající náhodně nebo cílevědomě do informačních systémů tak, že vyhledávají zranitelná místa.

Jejich cíle nebo motivace jsou různé. Pak je lze rozdělit na⁴⁸:

Hackeri (průnikáři) - osoby, které pronikají do zabezpečených systémů, přičemž jejich cílem je prokázat své vlastní schopnosti, kvality, aniž by měly ve většině případů zájem získat informace nebo systém narušit.

Tzv. „Neúspěšní kritikové“, kteří většinou opakovaně poukazují na závady a nedostatky v informačních systémech, zejména v jejich ochraně. Svou činností chtějí

⁴⁷ Zákon č. 140/1961 Sb., Trestní zákon, ve znění pozdějších předpisů
Zákon č. 141/1961 Sb., Trestní řád, ve znění pozdějších předpisů

⁴⁸ Látal, I., Počítačová (informační) kriminalita a úloha policisty při jejím řešení, materiál z přílohy časopisu Policista č. 3/1998, Policejní akademie České republiky Praha,1998

upozornit na naléhavost situace a nutnost jejího řešení. Tuto činnost považují za krajní prostředek řešení.

Mstitelé, jejichž motivace vyplývá ze msty vůči zaměstnavateli, který je z různých, pro ně ovšem nespravedlivých, důvodů propustil ze zaměstnání nebo jinak poškodil.

Crackeři, osoby, kterým se nejedná jen o překonání ochranných překážek, ale po průniku různým způsobem nabourávají informační systémy, získávají data, aniž by snad měli zájem je využít pro svůj prospěch.

6.1.2 Profesionálové

Získávání, shromažďování, analyzování a využívání informací je jejich zaměstnáním, takže mají v podstatě neomezené prostředky. Tuto činnost nevykonávají většinou pro sebe, ale pro zaměstnavatele (špionáž, boj s konkurencí apod.). Z hlediska počítačové kriminality není tato kategorie příliš zajímavá, pokud se tyto osoby nedopustí protiprávního činu. Do této kategorie však patří i softwaroví piráti, jejichž cílem je neoprávněný zisk z prodeje nelegálně získaného softwaru.

Teroristé - jsou zvláštní skupinou organizovaného zločinu, mající většinou vlastní zpravodajské sítě jak pro získávání potřebných informací, tak i pro vlastní ochranu. Mohou být velmi vysoce kvalifikovaní, obdobně jako pracovníci oficiálních zpravodajských služeb, jen jejich zaměření, cíle a pochopitelně způsoby a prostředky dosažení těchto cílů jsou naprosto jiné.

Výše uvedená klasifikace je pouze orientační, protože ve skutečnosti se jednotlivé kategorie prolínají a jsou vzájemně propojeny.

6.2 Podněty k vyšetřování

Základním úkolem je shromáždění dostatečného množství skutečností svědčících o tom, že se určitý skutek stal, je trestným činem a že je možno určit osoby, proti kterým lze vést trestní stíhání.

6.2.1 Oznámení kontrolních, inspekčních a revizních orgánů

Z logického hlediska by tyto podněty měli být nejčastějšími a nejúplnějšími. Praxe však dokazuje že skutečnost je jiná neboť tyto subjekty sice mají potřebné odborné znalosti, ale nejsou dostatečně motivovány a většinou zde převládá strach z ohrožení dobré pověsti.

Tyto organizace se pak většinou místo oznámení snaží odhalené delikty řešit sami v rámci pracovně právních kompetencí.

6.2.2 Oznámení občanů

Tyto podněty bývají málo konkrétní a trpí značným informačním deficitem, ale i přesto mají pro odhalení velký význam. Jakákoliv informace, byť i málo konkrétní zvyšuje míru odhalení trestných činů této kategorie, které by jinak zůstaly nepotrestány.

Motivem k podání stále však zůstává nejčastěji individuální zájem na náhradě škody a na potrestání konkrétního pachatele. Hlavním důvodem je především nízká citlivost obyvatelstva k těmto deliktům, které ani mnohdy nepovažují za trestnou činnost.

6.3 Dokazování

Úspěšné vyšetření každého trestného činu závisí na správném určení okolností, které jsou nezbytné pro posouzení věci. To znamená, aby bylo zajištěno takové množství důkazního materiálu, aby mohl být pachatel nad veškerou pochybnost usvědčen a tedy shledán vinným a odsouzen. Bohužel ve virtuálním světě je právě tento požadavek klíčovým problémem dokazování počítačového zločinu.

Předmět dokazování počítačové kriminality obecně vymezuje ustanovení § 89 odst. 1 TR⁴⁹. Zvláštnosti předmětu vyšetřování jsou navíc určovány jednotlivými způsoby páchaní.. Spočívají zejména v tom, že je potřeba zjišťovat zejména⁵⁰:

- zda se jedná o jeden či více skutků;
- na kterém počítači byla provedena delikventní operace;
- jakým způsobem a postupem byla delikventní operace provedena;
- způsob zapojení počítače do sítě, jeho periferní vybavení a konfigurace, jeho programové vybavení;
- obsah pevného disku, disket, CD (DVD) nosičů a jiných paměťových medií zajištěných u pachatele nebo příslušejících k zájmovému počítači;
- zda je při spáchání trestného činu součinnost dalších osob;
- rozsah a oprávnění pachatele nakládat s počítačem a jeho komponenty;
- rozsah oprávnění pachatele provádět dané typy operací;

⁴⁹ Zákon č. 141/1961 Sb., Trestní řád, ve znění pozdějších předpisů

⁵⁰ Straus, J. a kol., Kriminologická metodika, Plzeň, Aleš Čeněk s.r.o, 2006, str.279

- rozsah znalostí pachatele o výpočetní technice, programech, komunikačních sítí a jejich využití;
- pravidla režimu práce s výpočetní technikou v poškozené organizaci;
- zda byla výpočetní technika a paměťová média zajištěna po události a s jakým časovým odstupem;
- zda jsou zajištěné informační soubory původní, upravované (v jakém rozsahu a kým);
- zda a jaká vznikla škoda nebo jiné neoprávněné výhody získané trestným činem;
- motiv;
- okolnosti, které umožnily spáchání skutku atp.

6.4 Typické stopy

Charakter počítačové stopy je dán změnou na nosiči informací, vzniklou v souvislosti s trestným činem, při jehož páčání je využívána výpočetní technika, přičemž tato stopa je zjištělná pomocí současných metod, operací a prostředků. Tyto stopy můžeme nalézt především na pevném disku, vyměnitelných paměťových mediích (Flash paměti, paměťové karty, diskety), CD nebo DVD nosičích⁵¹.

Při vyšetřování počítačové kriminality má počítačová stopa výsadní postavení, ale pro komplexnost je nutné zajistit řadu dalších významných stop. Těmito stopami může být celý počítačový systém, jednotlivé komponenty i jejich vzájemné propojení. Za zmínku stojí i celá řada písemností, účetních a jiných dokladů, které mohou vést k usvědčení pachatele. Jako stopu můžeme označit stopy ve vědomí osob, což jsou skutečnosti vnímané osobami zainteresovaných do případu.

Je velmi důležité, aby tyto stopy byly zajištěny v co nejkratším čase, jelikož zničení počítačových stop lze provést během několika sekund. Trestné činy toho to typu pak zůstávají dlouho neodhaleny, což umožňuje pachatelovi nerušeně pokračovat v trestné činnosti.

6.5 Počáteční úkony

Hlavní cílem počáteční etapy vyšetřování je zabránit zničení počítačových stop a jiných kriminalisticky relevantních informací. To znamená nasadit co nejvíce kvalifikovaných

⁵¹ Straus, J. a kol., Kriminalistická metodika, Plzeň: Aleš Čeněk s.r.o, 2006, str.275

sil a nejmodernějších dostupných prostředků tak, aby rozhodující výkony byly provedeny za momentu překvapení a je-li to potřebné na více místech současně.

Typické počáteční úkony

- vyžádání potřebných vysvětlení;
- zajišťovací úkony (domovní prohlídky, prohlídky jiných prostor, vydání a odnětí věci a ohledání výpočetní techniky);
- vyžádání expertíz (nařízení znaleckého zkoumání, dožádání o odborné vyjádření).

Je třeba počítat s tím, že pachatelé počítačové kriminality jsou vysoce kvalifikováni a jejich počítačová gramotnost přesahuje obvykle znalosti řadových policistů. Již od počátku je tedy nezbytná jejich spolupráce s počítačovými experty. Dalším problémem, který vzniká v souvislosti s těmito delikty je fakt, že řada těchto skutečností podléhá režimu utajovaných informací a je tedy nutné snížit stupeň utajení informace v souladu se zákonem nebo zabezpečit provedení bezpečnostních prověrek u osob, které se budou s utajovanými informacemi seznamovat. To však naráží na časovou náročnost, zejména při vyžadování bezpečnostních prověrek. Je tedy nutné výhledově u osob, u kterých je předpoklad seznamování se s utajovanými informacemi včas vyžádat provedení bezpečnostních prověrek v souladu se zákonem č.412/2005 Sb.⁵² tak, aby už v době vyšetřování byly držiteli Osvědčení s daným druhem bezpečnostní prověrky.

Po provedení a vyhodnocení všech počátečních úkonů je potřeba vytýčit vyšetřovací verze a to ke způsobu spáchání trestného činu, k pachatelům počítačové kriminality, jejich organizovanosti, počtu a postavení a také k motivu pachatele.

6.6 Následné úkony

6.6.1 Výslech obviněného

Při výslechu jsou kladeny značné nároky na znalosti a schopnosti vyslychajícího. Je nezbytná přítomnost znalce nebo specialisty z oblasti informačních technologií, který bude nápomocen při otázkách týkajících se odborných oblastí.

⁵² Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

6.6.2 Výslech svědků

Tyto svědky můžeme rozdělit do dvou kategorií. V první kategorii jsou osoby vypovídající o otázkách z oblasti výpočetní techniky, druhá kategorie nám poskytuje informace o způsobu života obviněného, jeho majetkových poměrech atp.

Dalšími typickými úkony při vyšetřování počítačové kriminality jsou expertizy z oboru účetnictví, ekonomiky, grafologie a dalších odvětví.

Pokud je nutno ověřit zda určitým způsobem za určitých podmínek bylo možno spáchat trestný čin, lze použít vyšetřovací experiment. Dalším vhodným úkonem je i využití rekonstrukce za účasti znalce z oboru výpočetní techniky.

7 PREVENCE

Je třeba přesunout daleko více sil do oblasti prevence, ochrany počítačů a informačních systémů, neboť jedině tak lze účinně bojovat proti tomuto druhu trestné činnosti, patřícímu do stále sílícího objemu kriminality bílých límečků a organizovaného zločinu⁵³.

Prevence počítačové kriminality je celospolečenským zájmem. Její přínos v boji s těmito delikty je nezastupitelný. Nelze očekávat že takový typ zločinu lze vyřešit jen změnou zákonů a vytvořením speciálních složek., je nutné zapojit do této činnosti nejrůznější subjekty, počínaje již výukou na základních školách, kde již můžeme vidět náznaky této trestné činnosti po nejrůznější státní i nestátní organizace. Aby byla prevence dostatečně účinná, je třeba zaměřit ji jak na osoby přicházející do styku s výpočetní technikou, tedy na potenciální pachatele, tak na vnitřní a vnější ochranu výpočetní techniky a informací jí zpracovávaných. Medializace a informování široké veřejnosti, napomáhá k ucelenému obrazu o této trestné činnosti ve vědomí veřejnosti. Při prezentaci pozitivních výsledků činnosti policie a soudů dojde u řady možných budoucích pachatelů ke změně postavení vůči jejich potenciální činnosti a to buď z důvodu strachu z možné represe nebo uvědomění si jejich morálního prohřešku.

Dále je nezbytné realizovat konkrétní metody působení zaměřené především ke komplexnímu zabezpečení systému, tam kde se apely minuly účinkem. Jde především o přesné vymezení organizačních řádů, pracovních náplní zaměstnanců a konkrétní nakládání a manipulací s daty. Souběžně s vývojem programového vybavení se snaží výrobci softwaru (např. Microsoft) vyvinout důkladnější a důmyslnější ochrany svých produktů. Jsou zde patrné kladné výsledky. Mezi ně například patří ověřování legálnosti softwaru nebo použití sofistikovaných kryptografických klíčů.

⁵³ Smejkal, Vl., Informační a počítačová kriminalita v České republice, MV ČR, 1999

8 ZÁVĚR

Cílem mé bakalářské práce bylo upozornit na nebezpečnost počítačové kriminality. Počítačová kriminalita může postihnout značnou šíří osobního i společenského života. Výpočetní technika je nasazena do řízení a správy státu, v armádě, policii, ekonomice, průmyslu i zemědělství, ve zdravotnictví a jinde. V počítačových systémech jednotlivých institucí se soustřeďují informace ze všech oblastí života společnosti i jednotlivce. Proto poškození funkce počítačových systémů, nejen celostátně budovaných, ale i lokálních může vést k dezorganizaci v mnoha sférách lidské činnosti.

Jak již z mé práce vyplývá počítačová kriminalita svou podstatou přesahuje teritoriální hranice jednotlivých států a stává se tak nadnárodním zločinem a jako k takovému k ní musíme přistupovat.

Prvním požadavkem je tedy, aby byla co nejrychleji vytvořena taková legislativa, která by pomohla potírat tento druh trestné činnosti. Komplexní řešení problému je možné pouze na základě mezinárodní spolupráce ve vyšetřování, obžalobě a odsouzení pachatelů této trestné činnosti a sjednocení legislativy v oblasti počítačové kriminality na základě Úmluvy Rady Evropy o počítačové kriminalitě. Proto je i u nás věnována velká pozornost rekonstrukci trestního zákoníku, jehož současná právní úprava neumožňuje vypořádat se v potřebné míře s rostoucím množstvím právních problémů v této oblasti.

V novém trestním zákoně jsou skutkové podstaty trestných činů neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací (§ 207), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 208) v osnově upraveny na základě Úmluvy o počítačové kriminalitě, Budapešť, ze dne 23. listopadu 2001, kdy bylo třeba zapracovat zejména články 2 až 11, které stanoví kriminalizaci nezákonného získání přístupu k počítačovému systému, nezákonného odposlechu počítačového systému technickými prostředky, neoprávněného poškození, vymazání, snížení kvality, pozměnění nebo potlačení počítačových dat, ve kterých jsou zahrnuty i počítačové informace, omezování funkčnosti počítačového systému pomocí manipulace s počítačovými daty, počítačového padělání, dále výroba, prodej, opatření za účelem použití, držení, dovoz, distribuce a zpřístupňování zařízení, která jsou vytvořena nebo uzpůsobena k páčání uvedených trestných činů podle článků 2 až 5 uvedené Úmluvy, nebo přístupových hesel, kódů a podobných počítačových dat. V souvislosti s tím osnova na základě požadavků z praxe upravuje i trestný čin poškození

záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle § 209.

Druhý požadavkem je *prevence*. Je nezbytné vytvořit takový systém právní výchovy a propagace v boji proti informační a počítačové kriminalitě, který zahrne celou veřejnost. Právě informovanost společnosti a její zapojení do této problematiky může být velmi přínosné. Nemůžeme samozřejmě předpokládat, že každý z nás se stane počítačovým expertem ale pokud budeme vědět jak alespoň základním způsobem chránit svá data, a nebudeme laxně přistupovat k porušování autorského zákona ve všech jeho směrech, můžeme rozvoj této trestné činnosti omezit nebo alespoň výrazně zpomalit. Bohužel tato činnost je stále považována za něco, co je společností tolerováno.

Za třetí požadavek, jak účinně bojovat s počítačovou kriminalitou bych označila potřebu věnovat větší pozornost výzkumu v oblasti počítačové kriminality, který bude pružně reagovat na nové jevy a vývoj informačních technologií. Není možné potírat tyto delikty bez potřebného vybavení a nových poznatků. Nezbytným předpokladem úspěchu je samozřejmě i zvyšování kvalifikace vyšetřujících složek a překonání jazykové bariéry.

Následující vývoj a směr počítačové kriminality lze jen těžko přesně předpovědět. Problémem jsou nerozvinuté země, které se stávají ať už reálným nebo virtuálním útočištěm pachatelů této kriminality. Není možné předpokládat, že tyto země budou schopny svoji legislativou reagovat na vznik tohoto druhu trestné činnosti, což dává pachatelům prostor pro jejich trestnou činnost. Je však na místě říci, že s intelektuálním rozvojem pachatelů narůstají i odborné znalosti vyšetřovatelů a tím se výrazně zvyšuje procento úspěšně vyřešených případů.

9 RESUMÉ

The aim of my diploma paper is to show and discuss the evolution and growth of Information Technology, also including the relative growth in Computer Fraud and Piracy, which became a phenomenon of 21st century.

The first part of my work is aimed at general characteristics of Computer Fraud its classification and a historical background.

As previously mentioned in my papers, computer fraud was first committed by individuals purely as statement in both their own ability to do so and to demonstrate the susceptibility of organisations and programmes. After a period of time the large financial gain to be made became a major factor. The main reason was the vision of easily earned money and only a little chance of being discovered and punished for this activity. However, with the growth of new technologies this activity is becoming more and more dangerous for society as a whole, not only in the home environment but also on an international front.

In the second part we are focusing on individual kinds of Computer Crime. I would like to mention particularly the growing problem with the Internet connection. Thanks to continued growth in internet usage most computer crime is committed via the internet. We can only expect it to continue increasing! I would also like to point out that there is not adequate control over key people in the environment and quite often these people are aware of the weak links in these technologies.

The third part is dedicated to the investigation of computer fraud. I will be pointing out the differences that exist in the investigation of individual cases. Offenders are generally people with higher or university education who have specialised in either the Technical or IT sectors. The gathering of evidence to prove illegal activity in those cases is both very important and extremely difficult. I would like to stress the importance of preventing such crimes.

In last part of my diploma papers I will to show the importance of International cooperation and the need to change the legislative. Also the need for further research and to extend the general knowledge in IT.

10 SEZNAM POUŽITÉ LITERATURY

- Smejkal, V., Sokol, T., Vlček, M.: Počítačové právo. Praha, C.H.Beck 1995
- Kučera Jan: Počítačová kriminalita v České republice. Brno, Masarykova univerzita, Fakulta informatiky, 2001.
- Matějka, M.: Počítačová kriminalita. Praha, Computer Press, 2002
- McClure, S., Scambray, J., Kurtz, G.: Hacking bez tajemství. Praha, Computer Press, 2004
- Prosise, Ch., Mandia, K.: Počítačový útok Detekce, obrana a okamžitá náprava. Praha, Computer Press, 2002
- Bímová, A.: Počítačová kriminalita a naše doba. Praha, IDG Czechoslovakia, a.s., 1990
- Porada, V., Konrád, Z.: Metodika vyšetřování počítačové kriminality. Praha, PA ČR, 1998
- Straus, J., a kolektiv: Kriminalistická metodika. Plzeň, Aleš Čeněk s.r.o., 2006
- Smejkal, V.: Informační a počítačová kriminalita v ČR, Praha, 1999
- Červeň, P., Cracking a jak se proti němu bránit, Brno: Computer Press, 2003
- Jelínek J. Trestní právo hmotné, Obecná část, Praha: Linde, 2004, str.277
- Michelle Slatalla, Hackers Hall Of Fame, Discovery Online, 1997
- Manuál OSN pro prevenci a kontrolu počítačového zločinu, OSN 1994
- Doc. Ing. Ivo Látal, CSc.: Počítačová (informační) kriminalita a úloha policisty při jejím řešení - časopis POLICISTA č. 3/1998, Policejní akademie České republiky
- Bitto, O., Časopis Computer č.3, Brno: Computer Press, 2006, str. 82

Seznam zákonů:

- Zákon č. 140/1961 Sb., Trestní zákon ve znění pozdějších předpisů.
- Zákon č. 141/1961 Sb., Trestní řád, ve znění pozdějších předpisů.
- Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti.
- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o působnosti Úřadu pro ochranu osobních údajů a o změně některých dalších zákonů., ve znění pozdějších předpisů.

Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.

Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

Vyhláška č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací.

Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.

Vyhláška č. 526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti).

Vyhláška č. 527/2005 Sb., o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti).

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

Internetové zdroje:

Internetové stránka MV ČR, <http://www.mvcr.cz>

Internetové stránka Národního bezpečnostního úřadu. Dostupné z <http://www.nbu.cz>

Internetové stránka Úřadu pro ochranu osobních údajů. Dostupné z <http://www.uouu.cz>

Internetové stránka Úřadu průmyslového vlastnictví. Dostupné z <http://isdvapl.upv.cz/servlet/>

Business Software Aliance. Dostupný z <http://www.bsa.org/czechrepublic/antipiracy/statistiky.cfm>

Kopta, M., Dětská pornografie - problém Internetu, Lupa, 2004. Dostupný z <http://www.lupa.cz/clanky/>

Ambrož, J., Jak silná je naše softwarová policie, Lupa, 2005. Dostupný z <http://www.lupa.cz/clanky/>

Hák, I.: Moderní počítačové viry, 2005. Dostupný z <http://www.viry.cz>

Úmluva Rady Evropy o počítačové kriminalitě, Budapešť, 23. listopadu 2001, Convention on Cybercrime - ETS no. 185. Dostupný z <http://conventions.coe.int/>