UNIVERZITA PARDUBICE
FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2010 Vít Řanda

Univerzita Pardubice
Fakulta ekonomicko-správní

Zneužití informačních technologií při páchání trestné činnosti

Informační kriminalita a její odhalování

Vít Řanda

Bakalářská práce

2010

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: **2009/2010**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vít ŘANDA**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informatika ve veřejné správě**
Název tématu:	**Zneužití informačních technologií při páchání trestné činnosti - informační kriminalita a její odhalování**

Zásady pro vypracování:

Vymezení trestné činnosti na úseku informačních technologií.
Rozdělení informační kriminality používané v mezinárodních dokumentech a podle kriminalistickotaktických hledisek.
Informační kriminalita a její odhalování:
- porušování autorského práva - softwarové pirátství,
- poškození a zneužití záznamu na nosiči informací,
- další typy trestné činnosti související s informační kriminalitou (e-commerce).

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

MATĚJKA, M. Počítačová kriminalita. Praha : Computer Press, 2002. ISBN 80-7226-419-2.

PORADA, V. Kriminalistická metodika vyšetřování. Aleš Čeněk - vydavatelství a nakladatelství, 2007. ISBN 978-80-7380-042-0.

PORADA, V., KONRÁD, Z. Metodika vyšetřování počítačové kriminality. Praha : Policejní akademie České republiky, 1998. ISBN 80-85981-75-0.

Vedoucí bakalářské práce: **doc. Ing. Jitka Komárková, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **5. října 2009**

Termín odevzdání bakalářské práce: **30. dubna 2010**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 5. října 2009

Prohlašuji:
Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 29.4.2010

Vít Řanda

Poděkování:

Děkuji vedoucí bakalářské práce doc. Ing. Jitce Komárkové, Ph.D., za vedení mé práce, její ochotu podílet se svými radami a připomínkami na zpracování mé práce. Dále pak děkuji mým kolegům z Odboru informační kriminality při Úřadu služby kriminální policie a vyšetřování, Policejní prezidium ČR, za poskytnutí cenných informací k problematice informační kriminality.

ANOTACE

Práce je věnována problému současné společnosti ve smyslu zneužívání informačních technologií při páchání trestné činnosti, tj. informační kriminalita a její odhalování, se zaměřením na kriminalitu páchanou na Internetu nebo za využití Internetu. Vedle popisu odhalování této trestné činnosti je práce dále věnována i rozdělení této informační kriminality dle různých způsobů a stručnému popisu jednotlivých podskupin.

KLÍČOVÁ SLOVA

Informační kriminalita, Internet, phishing, počítačová kriminalita, skimming, softwarové pirátství

TITLE

The misuse of information technologies for a crime commissioning - The Cybercrime and its detection

ANNOTATION

The thesis deals with a problem of information misusing in modern society where its important part is the cybercrime which focus on commissioning of a crime using internet. Apart from characterization of crime detection the thesis is dedicated to a classification of such criminality according to the different ways of doing the crime with a general description of each sub class.

KEYWORDS

Cybercrime, Internet, phishing, computer crime, skimming

OBSAH

Úvod

Současná společnost ve stále větší míře využívá informační systémy a technologie pro nejrůznější oblasti činností. Je možné bez nadsázky říci, že společnost dvacátého prvního století, a především její ekonomika, bude zcela postavena na informačních technologiích a na vzájemném propojení informačních systémů do sítí, kdy dominantní roli bude hrát veřejná informační a komunikační síť - Internet. Internet nemá právní subjektivitu, není hmotným předmětem, nemá majitele a je informačním systémem skládajícím se ze subjektů práva. Prostředí Internetu je jiné, než prostředí reálného světa. Ruku v ruce s vývojem informačních technologií a jejich následného využití jako prostředku ulehčující běžný život se objevuje zneužívání těchto technologií pro trestnou činnost, resp. kořistění za využití těchto technologií.

Cílem této práce je popsat a zdokumentovat problém současné společnosti ve smyslu zneužívání informačních technologií při páchání trestné činnosti, tj. informační kriminalita a její odhalování, se zaměřením na kriminalitu páchanou na Internetu nebo za využití Internetu, neboť nás informační technologie obklopují na každém kroku a je třeba se zamyslet nad svým konáním v tomto „elektronickém“ světě a uvědomit si možná rizika plynoucí z tohoto jednání.

Toto téma jsem si zvolil záměrně, neboť v rámci svého zaměstnání se zabývám odhalováním této kriminality, přičemž od roku 2000 jsem v rámci Policie ČR služebně zařazen na Odboru informační kriminality při Úřadu služby kriminální policie a vyšetřování na Policejním prezidiu ČR. Za dobu mého působení na této součásti jsem se setkal s odhalováním různých případů informační kriminality, a proto pro názornost uvedu některé tyto případy v obecné rovině dále v následující práci.

1. Informační a počítačová kriminalita

pojem

Označení „informační kriminalita“ je výrazem pro určitou trestnou činnost obdobně, jako je využíván např. výraz násilná kriminalita, drogová kriminalita apod. Jedná se tedy o skupinu trestných činů, která v sobě zahrnuje určitý společný faktor.

definice

Tento pojem v sobě tedy zahrnuje páchání trestné činnosti, která je páchána přímo v prostředí informačních technologií (dále jen IT), kdy předmětem útoku je přímo oblast IT nebo jiná oblast, ale za převážného využití IT.

Počítačová kriminalita je podmnožinou informační kriminality a je fenoménem dnešní doby. V odborné literatuře se setkáváme s mnoha pojmy, které projevují snahu o vymezení pojmu počítačová kriminalita. Žádná z těchto formulací však nevymezuje celkově celou škálu oborů a zaměření, pouze zohledňuje konkrétní směr přístupu k věci. Jako příklad lze uvést definici dle [15]: „*Počítačovou kriminalitou z kriminalistického hlediska rozumíme skupinu trestných činů (společensky škodlivých jednání) páchaných prostředky výpočetní techniky v podmínkách komunikačních sítí, systémů, programového vybavení a databází výpočetní techniky*“. Jako další definici lze zmínit [12]: „*Mezi běžné názvy pro tuto problematiku patří počítačová kriminalita, kriminalita informačních technologií, v tisku se lze setkat i s anglickými termíny cybercrime, IT crime a computer crime. Leckdy je kriminalita informačních technologií vnímána jako širší pojem než počítačová kriminalita a má zahrnovat mj. i kriminalitu v oblasti telekomunikací“.*

Jednou z dalších definicí počítačové kriminality je definice akceptovaná v rámci Evropské unie [14], která zní: „*Počítačová kriminalita je nemorální a neoprávněné jednání, které zahrnuje zneužití údajů získaných prostřednictvím informačních a komunikačních technologií nebo jejich změnu*“.

Osobně bych se tedy přikláněl k definici počítačové kriminality, jak uvádí [13], kdy: „*Pod pojmem počítačová kriminalita je třeba chápat páchání 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 jako předmět této trestné činnosti, ovšem s výjimkou majetkové trestné činnosti, nebo jako nástroj trestné činnosti.“

Byly i snahy nazývat počítačovou kriminalitu jako informatická kriminalita, ale myslím si, že tento pojem se moc neujal. V poslední době dochází k prolínání informační kriminality s počítačovou kriminalitou a nelze již striktně určit meze rozlišení, a proto z pohledu orgánů činných v trestním řízení lze označovat oběma pojmy stejný druh kriminality. Za dobu mé praxe v oboru boje s informační kriminalitou (od roku 2000) jsem se setkal pouze se dvěma případy, kdy pachatelem nebyly použity prostředky výpočetní techniky. Jednalo se o zneužití hlasových služeb v sítích GSM ve smyslu zneužití a blokace linek TCTV 112 (***T****elefonní* ***C****entrum* ***T****ísňového* ***V****olání - linka 112*), kdy pachatel za využití několika mobilních telefonů zablokoval tato centra, a hrozilo nebezpečí nemožnosti se dovolat na tato centra v případě nouze. Nicméně v poslední době se prosazuje spíše termín informační kriminalita i u oblasti počítačové kriminality, zvláště pokud se chce zdůraznit, že trestný čin má vztah k software, k datům, resp. uloženým informacím, nebo šířeji k IT. Důvodem tohoto posunu je prolínání výpočetní techniky s komunikačními technologiemi a nabalování dalších aktivit na dosud poměrně úzce vymezenou oblast výpočetní techniky. Tím dochází k vytváření kompaktnějšího systému, kdy se do informační kriminality zahrnuje oblast výpočetní techniky, komunikačních technologií a další technicky vyspělá odvětví jako například elektronické platební prostředky. [13]

Proto z výše uvedených důvodů bude nadále v textu používán pojem informační kriminalita, bez ohledu na to, zda se jedná o samotnou počítačovou kriminalitu nebo o celek včetně počítačové kriminality.

Z pohledu odhalování této trestné činnosti vyvstává problém, kdy informační kriminalita je charakteristická obrovskou dynamikou a vysokou latencí (bez velkých projevů navenek), přičemž oba tyto znaky ztěžují práci vyšetřovatelů. S ohledem na uvedenou dynamiku není snadné udržet s pachateli krok. Vyšetřovatel bude vždy vůči pachateli o krok zpět. Dalším problémem při odhalování je složitost informačních systémů a z toho vyplývající nutnost znalostí z oblasti výpočetní techniky, kdy pachatelé této kriminality jsou velmi inteligentní a dokážou za sebou velmi dobře likvidovat stopy.

2. Dělení informační kriminality

2.1 Dělení používané v mezinárodních dokumentech

Počítačová a informační kriminalita dosahuje globálních, celosvětových měřítek. Proto při jejím rozdělení z různých úhlů pohledů lze vycházet i z mezinárodních dokumentů Evropských společenství, jejichž snahou je sjednotit úpravu trestního práva hmotného, procesního i mezinárodního. Jako jedním z nejdůležitějších dokumentů lze považovat „Úmluvu o počítačové kriminalitě“, která byla přijata dne 23. listopadu 2001 v Budapešti na Mezinárodní konferenci o počítačové kriminalitě v rámci činnosti Rady Evropy (dále jen Úmluva). Tato Úmluva vstoupila v platnost dne 1. července 2004. Ke dni 22. dubna 2008 Úmluvu podepsalo 44 států, z nichž ji však ratifikovalo jen 22 států. Česká republika podepsala Úmluvu dne 9. února 2005, avšak k její ratifikaci prozatím nedošlo. V této Úmluvě je následující dělení podle znaků trestných činů [3], [11]:

1. Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
    a. neoprávněný přístup
    b. neoprávněné zachycení informací
    c. zásah do dat
    d. zásah do systému
    e. zneužití zařízení
2. Trestné činy související s počítači
    a. falšování údajů související s počítači
    b. podvod související s počítači
3. Trestné činy související s obsahem
    a. trestné činy související s dětskou pornografií
4. Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu
    a. trestné činy související s porušením autorského práva a práv příbuzných autorskému právu

V oblasti počítačové kriminality byla v posledních letech také aktivní přímo Evropská unie. Význačným činem je akční plán *e*Europe 2002 (dále jen Plán), který

byl přijat v červnu r. 2000. Plán zdůrazňuje velkou důležitost bezpečnosti počítačových sítí a boje proti kyberzločinu. Jeho cílem je zvýšit bezpečnost informačních infrastruktur a zajistit, aby orgány činné v trestním řízení měly veškeré přiměřené prostředky k činnosti. Zároveň požaduje plné respektování základních práv člověka. V tomto Plánu jsou počítačové zločiny rozděleny na [13]:

1. zločiny porušující soukromí (ilegální sbírání, uchovávání, modifikace, zveřejňování a šíření osobních dat),
2. zločiny se vztahem k obsahu počítače (pornografie, zvláště dětská, rasismus, vyzývání k násilí apod.),
3. ekonomické (neautorizovaný přístup a sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové padělání a podvody apod.),
4. zločiny se vztahem k duševnímu vlastnictví (autorské právo apod.)

2.2 Dělení podle kriminalisticko-taktických hledisek

V současnosti je možno z kriminalistického hlediska provést základní dělení informační kriminality takto [19]:

1. porušování autorského práva - počítačové pirátství (§ 152 trestního zákona),
2. poškození a zneužití záznamu na nosiči informací (§ 257a trestního zákona), a to jako
    a. útok z vnějšku subjektu,
    b. útok zevnitř subjektu,
    c. útoky kombinované (z vnějšku i zevnitř),
3. ostatní počítačová, resp. "informační" trestná činnost, tj. trestné činy, které výpočetní techniku využívají jako prostředek k páchání trestných činů, nikoliv jako přímý objekt zájmu pachatele, i když není vyloučeno, že objektem zájmu mohou být počítačová data.

Toto dělení vychází z již v současnosti neúčinného trestního zákona, tj. zákona č. 140/1961 Sb., ve znění pozdějších předpisů (dále jen trestní zákon). Od 1. ledna 2010 nabyl účinnost nový trestní zákoník, tj. zákon č. 40/2009 Sb., ve znění pozdějších předpisů (dále jen trestní zákoník).

V novém trestním zákoníku je informační kriminalita řešena již ve třech paragrafech místo jednoho paragrafu v trestním zákoně (§ 257a). Jedná se o [17]:

- § 230 - neoprávněný přístup k počítačovému systému a nosiči informací,

- § 231 - opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat,
- § 232 - poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

a dále sem lze zařadit i oblast ochrany autorského práva:

- § 270 – porušení autorského práva, práv souvisejících s právem autorským a práv k databázi,

kdy toto jednání bylo v trestním zákoně postihováno dle § 152.

Z výše popsaného lze tedy nastínit nové dělení a to takto:

1. neoprávněný přístup k počítačovému systému a nosiči informací,
2. opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat,
3. poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti,
4. porušení autorského práva, práv souvisejících s právem autorským a práv k databázi,
5. ostatní počítačová, resp. "informační" trestná činnost, tj. trestné činy, které výpočetní techniku využívají jako prostředek k páchání trestných činů, nikoliv jako přímý objekt zájmu pachatele, i když není vyloučeno, že objektem zájmu mohou být počítačová data.

Jelikož dělení podle nového trestního zákoníku zatím není moc vžité a veškeré metodiky a postupy a i statistiky jsou zaměřeny na „staré“ dělení dle již neúčinného trestního zákona, bude dále v textu pod pojmem „poškození a zneužití záznamu na nosiči informací“ myšleno jednání kvalifikované v § 257a trestního zákona, což v sobě zahrnuje veškeré jednání, které je podle nového trestního zákoníku kvalifikováno ve třech paragrafových ustanoveních, jak je již výše uvedeno.

3. Informační kriminalita a její odhalování

„Kriminalita spojená s výpočetní technikou prodělala od poloviny 20. století obrovský vývoj. Zatímco před několika desítkami let byly počítačové systémy těžko napadnutelné trestnou činností, postupně začalo docházet k přibližování výpočetní techniky uživatelům a spolu s tím i k masivnímu nárůstu trestné činnosti. Útoky na počítačová data se začaly prudce zvyšovat především po roce 1989. Před tímto byly pouze sporadické jako výsledek malé rozšířenosti výpočetní techniky a síťových propojení. Dokonce se v těch dobách vyskytly útoky spočívající v ručním poškozování dat přejížděním nosiče magnetem. Pro specifickou trestnou činnost zaměřenou na informační technologie je nutné určité prostředí, které se rozvíjí až v posledních letech. Například útoky po Internetu vyžadují nejen existenci sítě, ale další množství technologií a určitý stupeň propojení, kterého okolo roku 1990 ještě nebylo možno dosáhnout.“ [4].

V současné době lze vidět značný nárůst informačních technologií a s tím spojené pronikání výpočetní techniky, nutně vybavené softwarem, do celé společnosti. Spolu s nárůstem počtu počítačů v komerční sféře i v domácnostech je zde i nárůst porušování autorského práva k programovému vybavení - softwarového pirátství. V současnosti je na území republiky nelegálně užíváno značné množství softwaru, což staví ČR mezi země, které musí ve větší míře pracovat na ochraně duševního vlastnictví v této oblasti. Protože je nutné snížit množství nelegálního softwaru na úroveň vyspělých zemí je odhalování a dokumentování této trestné činnosti potřeba věnovat značnou pozornost.

Při vyšetřování většiny trestných činů je největším zdrojem informací místo činu. Již z ohledání místa činu a vyhodnocení jeho výsledků lze usuzovat, zda došlo ke spáchání trestného činu a tento čin právně kvalifikovat. Vzhledem k charakteru způsobů páchání informační kriminality a jejich projevů ve stopách nemá místo činu leckdy zásadní význam jako zdroj informací. Při vyšetřování informační kriminality se lze setkat s celou řadou kriminalistických stop, z nichž některé jsou typické právě pro informační kriminalitu. Množství, různost a rozmístění stop závisí na konkrétních okolnostech případu. Vyskytují se jak stopy materiální a jiné soudní důkazy, tak stopy paměťové. Po mých několikaletých zkušenostech s odhalováním informační kriminality si dovoluji tvrdit, že největší přínos mají stopy paměťové, a to ve smyslu změny na nosiči informací, vzniklou v souvislosti s trestným činem, při jehož

spáchání byla využita výpočetní technika. Změny jsou zjistitelné a využitelné pomocí současných metod, prostředků, postupů a operací, např. logové záznamy při síťovém provozu, zbytkové datové fragmenty na paměťových médiích atd.

3.1. Porušování autorského práva – softwarové pirátství

Softwarovým pirátstvím jsou všechny útoky na právo autora a další práva k počítačovým programům a databázím uvedená v autorském zákoně. Jedná se pouze o jednu ze součástí problematiky informační kriminality. [18]

Velmi zvláštním problémem je Internet - světová informační síť. Jako každý lidský produkt, i Internet je zneužíván k softwarovému pirátství. Různé servery obsahují a různé osoby nabízejí nelegální software k stažení na počítač napojený uživatelem na Internet. Umístění nelegálního počítačového programu získaného na Internetu na pevný disk počítače je tak možno chápat jako **užívání** ve smyslu autorského zákona [18].

V oblasti neoprávněného užívání software se v praxi vyskytují dvě základní formy této trestné činnosti [5]:

1. *Tzv. **domácí uživatel** (fyzická osoba), který získal, případně dále získává různým způsobem software pro svou osobní potřebu.*
2. *Užívání nelegálního softwaru pro **komerční účely**. Obvyklým případem je podnikatel nebo společnost, která z důvodu neochoty k investicím nebo nedostatku finančních prostředků buď získala běžnou cestou pirátský software a užívá ho nebo, a to je nejčastější případ, bylo zakoupeno menší množství licencí, než je ve skutečnosti užíváno.*

Jak je již výše uvedeno, Internet je světová síť vzájemně propojených počítačů (serverů), které využívají různí uživatelé ke komunikaci, získávání informací a k práci. Získávání informací je obvykle vyhledání požadovaných volně dostupných dat a jejich vytištění nebo zkopírování na pevný disk.

Možnou variantou legálních aktivit je získání a instalace softwaru nabízeného počítačovými výrobci a dalšími firmami uživatelům Internetu. Běžně jsou nabízeny programy na zkoušku – shareware, a volné programy – freeware. Součástí takto šířeného softwaru je vždy licenční ujednání (obvykle v anglickém jazyce). Řada

programů má různé způsoby oprávněného užívání, mnoho softwaru při spuštění nebo v průběhu práce upozorňuje na způsob užití jako sharewaru.

Dle [18] je útokem na autorská práva zkopírování, instalace a užívání nelegálního softwaru. V absolutní většině případů je takový software jednoznačně jako nelegální označen (Warez - obvyklý software, Gamez - hry). V podstatě každý, kdo takový software kopíruje a užívá, tento software již vědomě vyhledal jako nelegální.

V této oblasti v ČR dochází k řadě nelegálních aktivit. Skupinami lidí vyvíjejících aktivní činnost při porušování autorských práv jsou prováděny především tyto aktivity, jako např. vyhledávání nekontrolovaných serverů s kvalitním připojením na Internet a jejich zneužití jako tzv. elektronických skladů. Obvykle v adresáři např. nazvaném „INCOMMING“ je na takovém počítači připojeném k Internetu pomocí protokolu FTP postupně různými osobami umisťováno značné množství počítačových programů a řádově vyšší počet osob je kopíruje na pevný disk svého počítače. Tato činnost probíhá ve dvou variantách [5]:

- volně dostupné adresáře nekontrolované chybou správce, umístění je volně šířeno k zajištění co největšího přísunu a zároveň možnosti získání množství programů,
- utajené počítače, obvykle s vědomím správce, přístup má omezená skupina osob, které se vydávají za profesionály.

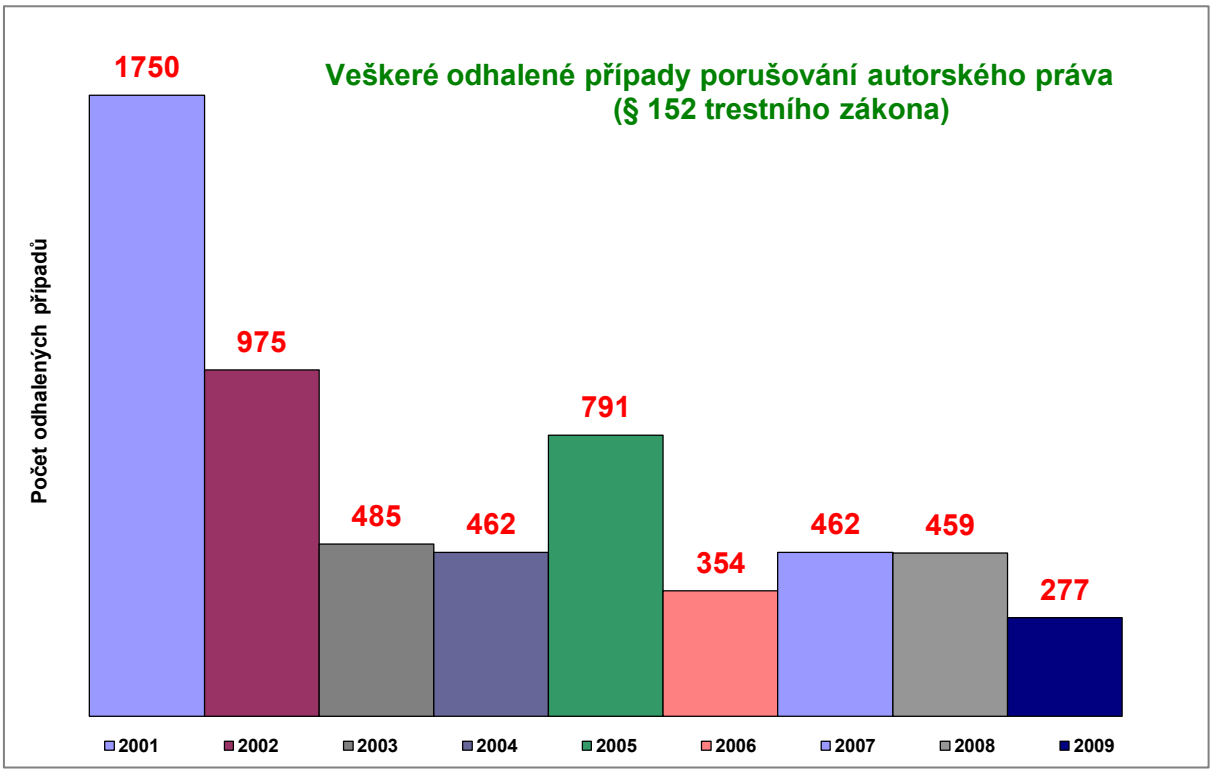
Na území ČR je řada míst, kde se masivně "stahuje" nelegální software z Internetu a nabízí dalším uživatelům. Tato činnost vyžaduje neomezené, kvalitní a rychlé připojení k Internetu. Často je taková činnost vyvíjena na vysokých školách (viz případ Strahovských kolejí ČVUT v Praze).

Pochopitelně nelegální software na Internetu je i záležitostí jednotlivců, kteří si na své domácí počítače takto získávají software k užívání.

V poslední době k této činnosti přistupuje v hojné míře i nelegální kopírování a následné šíření audio a video děl. Tento nárůst je zapříčiněn masivním rozšířením počítačů do domácností a následného připojení do sítě Internet (ADSL a WiFi připojení) a poklesem cen u zálohovacích mechanik z několika tisíc na stovky Kč a dále i poklesem cen paměťových médií (CD-R, DVD-R apod.).

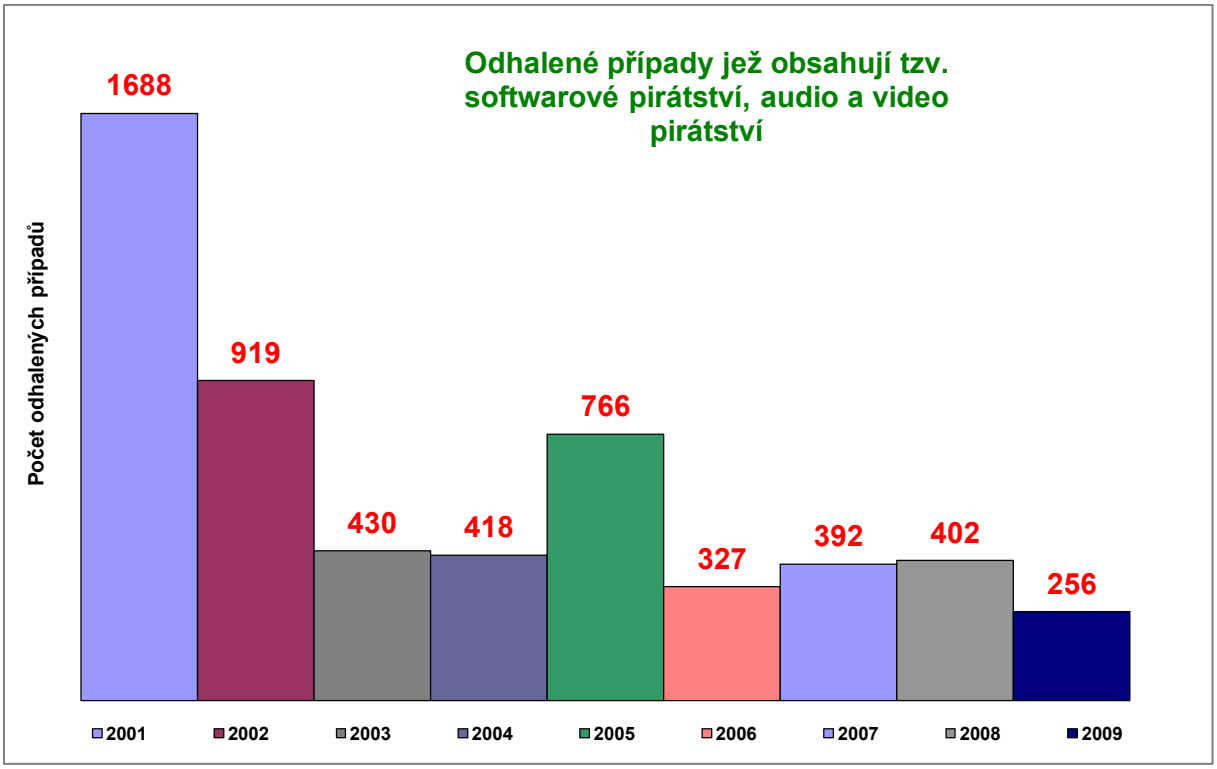
Níže jsou pro názornost uvedeny výstupy ze statistik „Evidenčně statistického systému kriminality“ (dále jen ESSK), kdy tento systém obsahuje údaje o všech

skutcích a jejich pachatelích, ke kterým prováděly policejní orgány trestní řízení. Informace do systému ESSK jsou získávána při plnění úkolů Policie ČR na úseku předcházení a odhalování trestné činnosti, zjišťování pachatelů a konání vyšetřování o trestných činech. Statistické údaje z tohoto systému jsou využívány prostřednictvím výstupních sestav. Zpracováním výstupních sestav k informační kriminalitě vznikly níže uvedené grafy, ze kterých je patrný vzestup podílu softwarového pirátství (včetně audio a video pirátství) na celkovém počtu zjištěných případů porušování autorského práva dle § 152 trestního zákona [8]. Ze systému ESSK nelze detailně rozčlenit, resp. vyčlenit ze zjištěných případů pouze samotné softwarové pirátství a proto je pod tento pojem zahrnuto i tzv. audio a video pirátství.

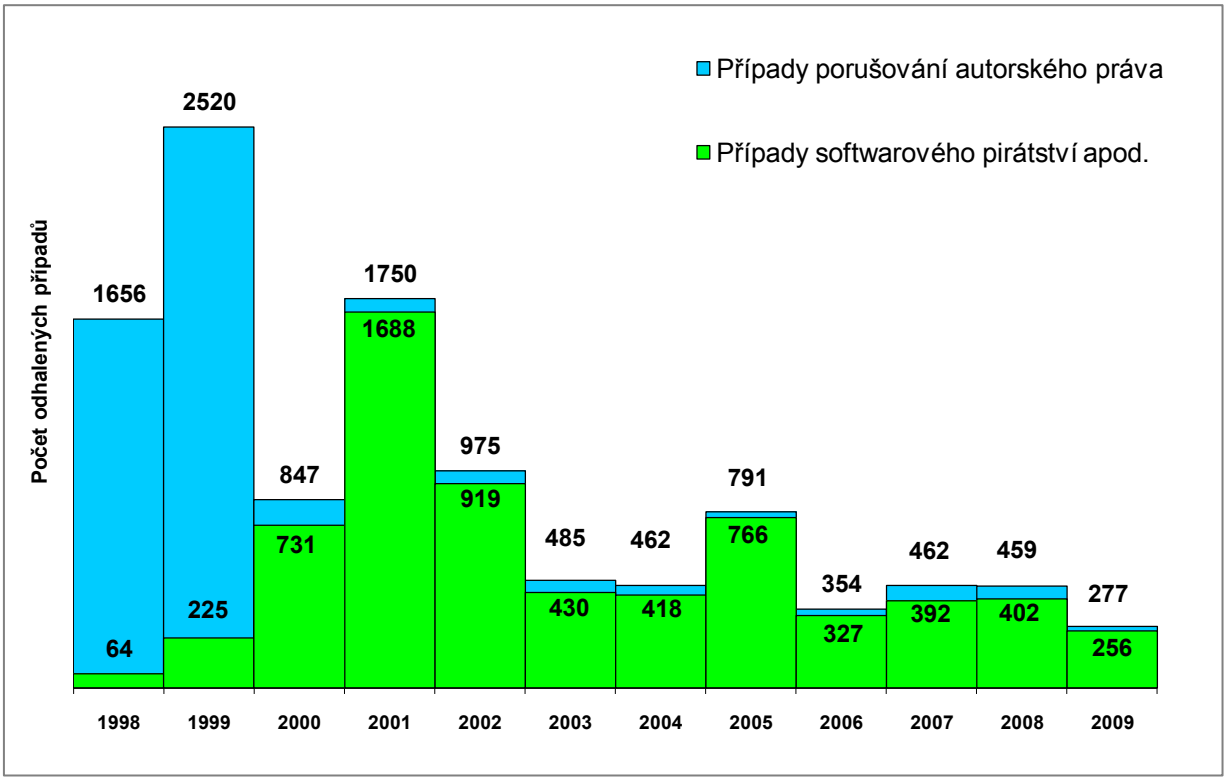


Obrázek 1 - veškeré odhalené případy porušování autorského práva, (zdroj: vlastní – zpracováno na základě [8])

Na obrázku č. 1 je graf veškerých odhalených (zjištěných) případů porušování autorského práva, tj. veškeré jednání naplňující znaky trestného činu dle § 152 trestního zákona [19] v závislosti na sledovaném období (kalendářní rok). Období roku 2001 vykazuje enormní počet odhalených případů, což bylo způsobeno špatným vykazováním této trestné činnosti v systému ESSK.



Obrázek 2 - odhalené případy softwarového pirátství, audio a video pirátství, (zdroj: vlastní – zpracováno na základě [8])



Obrázek 3 - porovnání poměru softwarového pirátství na celkovém porušování autorského práva, (zdroj: vlastní – zpracováno na základě [8])

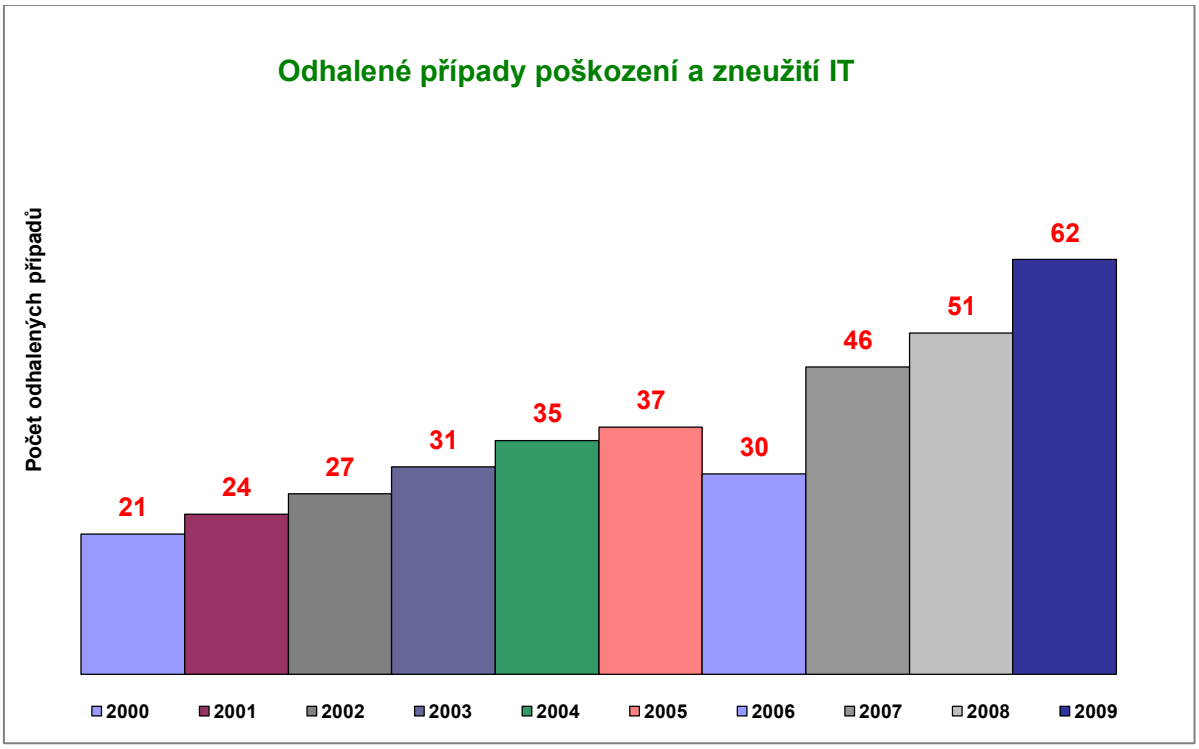
Na obrázku č. 3 je grafické vyjádření poměru odhalených případů softwarového pirátství na celkovém počtu odhalených případů porušování autorského práva. Z porovnání jasně vyplývá nárůst podílu případů softwarového pirátství na celkovém porušování autorského práva v období let 1998 až 2002, což bylo zapříčiněno větší dostupností vypalovacích mechanik a médií CD-R a poklesu finančních nákladů na jejich pořízení i pro obyčejné koncové uživatele. Dále jsou vysoké hodnoty zjištěných případů softwarového pirátství zapříčiněny i nízkým právním povědomím uživatelů počítačů v oblasti autorského práva, kdy ne každý uživatel byl srozuměn s tím, že užívání software v rozporu s licenčním ujednáním je protiprávní. V dalších letech lze pozorovat pokles, resp. ustálení na konstantní hodnotě. Toto je zapříčiněno již zmíněným právní povědomím, kdy došlo ke zvýšení tohoto povědomí na základě masivních kampaní prováděných Ministerstvem vnitra ČR a dalších subjektů, jako např. BSA (**B**usiness **S**oftware **A**lliance) apod., a dále došlo ke snížení cenových hladin u komerčních softwarových produktů. Dle BSA dochází v ČR k meziročnímu poklesu softwarového pirátství: „*Softwarové pirátství na tuzemských osobních počítačích (PC) je opět na ústupu. Mezi roky 2007 a 2008 míra pirátství poklesla o jeden procentní bod. V Česku se v roce 2008 užívalo nelegálně pouze 38 procent softwaru. Česká republika se tak stále drží mezi 30 zeměmi s nejnižší mírou softwarového pirátství. Průměrná míra pirátství v Evropské unii činí 35 procent*“ [2].

Dokumentování a objasňování této trestné činnosti je závislé na trvalém nebo alespoň občasném přístupu k Internetu a elektronické poště (e-mail). Trvalým vyhledáváním (tzv. surfováním) na Internetu lze získávat poznatky k různé trestné činnosti využívající možnosti volného šíření informací, tedy i porušování autorského práva. Obvykle dochází k uveřejnění nabídky (inzerce) nelegálního softwaru na serveru umožňujícím anonymní činnost, obvykle v zahraničí.

3.2. Poškození a zneužití záznamu na nosiči informací

Zatímco před několika desítkami let byly počítačové systémy těžko napadnutelné trestnou činností, postupně začalo docházet k přibližování výpočetní techniky uživatelům a spolu s tím i k masivnímu nárůstu trestné činnosti. Zatím co softwarové pirátství je trestným činem ve své podstatě jednoduchým, trestný čin

poškození a zneužití záznamu na nosiči informací je obvykle komplikovaně a obtížně objasnitelný a ne každý napadený subjekt je ochoten přiznat napadení s ohledem na svoji pověst, čemuž odpovídá i počet zjištěných případů tohoto jednání, jak je patrné z níže uvedeného obrázku č. 4.



Obrázek 4 - odhalené resp. zjištěné případy poškození a zneužití záznamu na nosiči informací, (zdroj: vlastní – zpracováno na základě [8])

V trestním zákoně či zákoníku se hovoří o nosiči informací a záznamu či informaci na něm. Jako nosič informací je chápáno jakékoliv datové médium určené pro informační techniku i když jsou občas zaznamenávány pokusy vydávat za nosič informací i jiná média jako například list papíru popsaný textem, který má být informací jak ji uvádí zákon. Zmíněné zákonné ustanovení je tedy jediným ustanovením, které je určeno pro informační technologie jako takové a postihuje vysoce kvalifikovanou trestnou činnost. Trestný čin, chápán jako útok na zákonem chráněný zájem, je možno rozdělit na tři formy a to na útok z vnějšku a útok zevnitř subjektu, který je cílem útoku a dále na ostatní formy. Toto dělení je možno považovat za základní, protože jak pachatelé, tak způsoby spáchání trestného činu se v obou formách podstatně liší stejně jako způsob objasňování trestného činu.

Z hlediska složitosti je možno říci, že útoky z vnějšku vyžadují podstatně větší kvalifikaci orgánů činných v trestním řízení i odborných znalců. [4]

3.2.1. Útoky z vnějšku subjektu

Touto formou útoku je myšlen tzv. hacking (hacker – osoba), což je výraz převzatý z americké angličtiny a rozumí se jím "násilné" tj. neoprávněné získání přístupu k datům. Ve své postatě se touto činností rozumí překonání ochrany počítače pachatelem, který není u počítače fyzicky přítomen, a který se obvykle nachází ve značné vzdálenosti od cíle útoku.

Útokem z vnějšku napadeného subjektu je myšlena činnost, kdy výpočetní technika nějakým způsobem umožňuje připojení z jiného počítače, obvykle po pevné, telefonní nebo jiné lince (např. mikrovlnné spoje).

Stupeň ochrany ani teoretická nemožnost neoprávněného připojení nemají význam, protože neexistuje naprostá bezpečnost a žádný systém na celém světě není schopen čelit všem útokům vedeným po síťovém připojení. Doslova jedinou možností jak uchránit počítač je jeho fyzické odpojení od sítě.

Dle [4] je možno objekty útoku rozdělit na:

a. komerční subjekt - obvykle právnická osoba, včetně nevýdělečných organizací,
b. nekomerční subjekt - fyzická osoba,
c. subjekt státní správy - od subjektů státní správy na úrovni obcí až po ministerstva a vládu,
d. bezpečnostní složky - Policie ČR, Armáda ČR apod.

Útoky na data, stejně jako jiné trestné činy, dělíme na úspěšné a neúspěšné. Zatímco v hmotném světě je poměrně snadno zjistitelný i neúspěšný útok na majetek a je možno ze strany policie či objektu pokusu přijmou opatření k zamezení dalších útoků nebo zadržení pachatele při dalším pokusu, je ve světě datové komunikace situace diametrálně odlišná. Internetové počítače, které jsou "přitažlivé" pro útočníky (hackery), zaznamenávají řádově stovky pokusů o proniknutí do systému za 24 hodin. Tyto pokusy spočívají obvykle v testování přístupu na počítač (port scan). Takovou činnost je možno přirovnat k chování potencionálního pachatele vloupání do objektu, který zkouší uzavření jednotlivých oken a dveří.

Samotným útok na data probíhá obvykle po přípravě, která spočívá v předběžném otestování bezpečnostních opatření a vstupů (scannování portů). Cílem útoku je téměř vždy proniknutí do systému a získání práva správce počítače (serveru). Následně může dojít k útoku na data uložená na počítači nebo zneužití počítače.

Ze získaných informací při analýzách dokončených hackerských útoků vyplývá, že hacker provádí svojí nelegální činnost z několika různých důvodů. Jedná se především o:

1. zviditelnění jeho konkrétní osoby ve vnějším světě (upozornění na svou osobu) a pozvednutí svého sebevědomí ("dokážu to, jsem lepší než ostatní") - při tomto důvodu nejde hackerovi o způsobení škody poškozenému, ale o dokázání okolí, že je lepší než správce napadeného počítačového systému (v ČR viz případy napadení serverů Ministerstva vnitra a Ministerstva zemědělství apod.). Výše uvedené platí i pro autory počítačových virů. Při tomto důvodu lze najít tzv. "podpisy" hackerů (nick, jméno nebo příslušnost k určité hackerské skupině nebo komunitě),
2. finanční důvod - hacking na zakázku (fyzická krádež na mediu, odposlouchávání dat, útoky na konkrétní počítače) nebo hacking pro svoji potřebu (bankovní hacking),
3. u vývoje, naprogramování a následné rozšiřování počítačových virů lze spatřit dva důvody a to:
    - ad bod 1,
    - finanční obohacení na základě rozšíření viru a následné distribuce antivirového softwaru za úplatu.

Ke své činnosti používají hackeři konkrétní softwarové utility vytvořené pro tyto účely a jedná se především o packet sniffery, backdoorové utility (trojské koně), port scannery, prolamovače hesel, keyloggery apod. Dále využívají známých bezpečnostních chyb v operačních systémech (Windows, Linux, atd.)

Hackeři jsou většinou osoby ve věku 15 až 25 let a jedná se o studenty středních odborných škol nebo vysokých škol se zaměřením na výpočetní techniku. Hackeři se svojí činností končí přibližně v období již zmíněného 25 roku věku a to z důvodu nedostatku času po ukončení vzdělávacího procesu a následného zapojení do všedního života a z toho vyplývajících potřeb řešit všeobecné životní problémy

(obživa, zabezpečení rodiny apod.). K hackerské činnosti je třeba neustále získávat nové poznatky o informačních technologiích a hlavně mít dostatek času, což při zapojení do všedního života přestává být dostupné.

Při šetření této nelegální činnosti je třeba zvýšené spolupráce s napadenými subjekty za účelem dokonalého zadokumentování datových obsahů na napadených systémech a jejich následných analýz na výskyt datových stop po útocích a dále z důvodu minimalizování ekonomických ztrát pro napadený subjekt (většinou nelze na delší dobu zajistit počítač pro účely zkoumání a analýzy dat).

Jako příklad lze uvést případ, kdy pachatel užívající konektivitu od nejmenovaného poskytovatele kabelové TV, přeskenoval segment IP adres jeho poskytovatele, včetně port scannu, čímž zjistil otevřené porty na konkrétních IP adresách a následně přistoupil na jednu konkrétní IP adresu (počítač) uživatele využívajícího stejného poskytovatele za pomocí znalosti bezpečnostních chyb (bezpečnostních „děr“) u instalace operačního systému MS Windows XP, na kterém nebyl aplikován „service pack“. Po přístupu na takto zkompromitovaný počítač zde vykopíroval dokumenty a zanechal zde „wordovský“ dokument s odkazem s tím, že jestli poškozený chce nazpět své dokumenty, tak ať pošle SMS na zanechané mobilní telefonní číslo. Po následné SMS komunikaci mezi poškozeným a pachatelem bylo zjištěno, že ze strany pachatele byly SMS zprávy zasílány pomocí Internetu, čímž následně provedeným šetřením u mobilního operátora poškozeného byla zjištěna IP adresa počítače, ze kterého byly SMS zasílání. Při šetření u poskytovatele internetového připojení dle získané IP adresy byla ztotožněna konkrétní kabelová přípojka, resp. konkrétní byt. Následným šetřením byla ztotožněna i konkrétní osoba, která se ale k této činnosti nedoznávala. Po tomto zjištění byl od osoby pachatele zajištěn počítač, který byl následně znalecky zkoumán. Při znaleckém zkoumání bylo zjištěno, že v tomto počítači je nainstalován kancelářský balík MS Office a jako uživatel je zde zadán textový řetězec „miminko“. Při zkoumání zanechaného „wordovského“ dokumentu v počítači poškozeného bylo zjištěno, že dokument byl vytvořen uživatelem „miminko“. Tato informace (stopa) byla použita jako jeden z důkazů proti zjištěné osobě, která se nakonec přiznala ke svému protiprávnímu jednání.

3.2.2. Útok zevnitř subjektu

V některých aspektech se útok zevnitř systému může podobat útoku z venku, ale jinak se ve většině ohledů jedná o zcela jinou formu trestného činu. V posledních letech bylo zaznamenáno celé spektrum útoků na data zevnitř systému obvykle motivovaných finančním prospěchem pachatele. Z toho plyne i skutečnost, že častým objektem zájmu pachatelů jsou společnosti pracující s velkými finančními prostředky, jakými jsou finanční ústavy. Zaměstnanci těchto subjektů jsou vystaveni značnému pokušení relativně jednoduchým způsobem získat značný finanční prospěch. Relativní jednoduchost takového činu spočívá ve znalosti systému a přístupovým právům ve spojitosti s vědomostmi o bezpečnostních nedostatcích. Navíc značné nasazení výpočetní techniky umožňuje provést útok na majetek použitím několika stisků klávesnice.

V první řadě zde zklamává personální faktor. Ve všech případech minulých let nedošlo ke kvalifikovanému napadení vnitřního systému banky, ale zneužití znalostí ze strany zaměstnance. K tomu se přidávají další faktory obvykle též spočívající v personální rovině, kdy zaměstnanci zodpovědní za bezpečnost a výpočetní techniky nesplnili své povinnosti nebo podcenili hrozící nebezpečí. V řadě případů je spáchání trestného činu skutečně jednoduché, ale nelze daný konkrétní způsob použít jinde, protože je pro konkrétní trestný čin specifický. Často se jedná o zneužití určitých zvláštností na jediném pracovišti, či narušení systému ochrany dat vlivem specifického výkonu činnosti určitého pracovníka nebo pracoviště. [4]

Na druhém místě stojí nedodržování bezpečnostních standardů či chybějící bezpečnostní projekt nebo kontrola jeho dodržování. Některé trestné činy byly spáchány jednoduchým způsobem, který ve svém důsledku téměř znemožnil odhalení pachatele. Je velmi problematické šetřit útok na data, pokud přístup k terminálu vnitřního systému není kontrolován, a taktéž není kontrolován pohyb zaměstnanců v bezpečnostních zónách. V takovém případě se sice jedná o trestný čin poškození a zneužití záznamu na nosiči informací, ale v souběhu s dalšími trestnými činy majetkové povahy. I když je pachatelem konkrétní osoba, spáchání trestného činu bylo umožněno nedokonalým vnitřním bezpečnostním systémem napadeného subjektu.

Někdy je naopak přeceňován stav vnitřní bezpečnosti a zaměstnanci jsou vlivem bezpečnostních opatření pod trvalým tlakem, a pak dojde k trestnému činu tím, že si pachatel odnese data na přenosném médiu.

Bezpečnost dat je plně v kompetenci subjektu a při správném nastavení komplexní bezpečnosti je možno rizika minimalizovat. Žádný systém však nemůže mít 100 % bezpečnost, jak si to někdy představují neinformovaní vedoucí pracovníci. Tomuto stavu se lze jen přiblížit.

Osoba pachatele je podstatně odlišná od osoby útočící z vnějšku subjektu. Téměř vždy se jedná o zaměstnance (bývalého zaměstnance) subjektu, který je cílem útoku nebo o osobu, které pro takový subjekt vykonává nějakou činnost. Pachatel vychází ze znalosti vnitřního systému, což ho podstatně odlišuje od mimo stojícího útočníka, který disponuje jen s těmi informacemi, které sám při testování systému nebo při útoku zjistí. Pozice pachatele stojícího uvnitř subjektu je podstatně jednodušší. Obvykle má navíc, z podstaty své zaměstnanecké pozice, i určitou úroveň oprávnění přístupu k výpočetní technice, případně informačního systému. Těchto znalostí a oprávnění pak zneužívá k samotnému trestnému činu. Pachateli uvnitř subjektu mnohdy nahrává i znalost bezpečnostních problémů nebo jejich nalezení vlastní aktivitou. [4]

3.2.3. Ostatní

Bez ohledu na předchozí základní rozdělení dochází ke stálému vývoji různých technik útoku na data, které nemusí vždy znamenat plnohodnotný útok na finanční prostředky nebo citlivá data. Lze sem zařadit:

- odposlech dat (sniffing),
- výroba a šíření počítačových virů a
- DoS útok.

Nejjednodušším způsobem průniku do cizího počítače nebo sítě je získání přihlašovacího jména a hesla konkrétní osoby. Toho se v případě trestné činnosti spojené s informačními technologiemi dosahuje dle [4] různými způsoby:

- “odposlechem” přihlašovacích dat na dálku, tj. použití programu, který “hlídá” komunikační kanál a monitoruje určitá data,

- infikování počítače programem (virem), který má za úkol monitorovat činnost počítače nebo např. po určitou dobu údery do klávesnice a odesílat zachycená data e-mailem nebo jiným způsobem.

Podobným způsoben dochází i ke kopírování určitých souborů v počítači (například aktuálních dokumentů) a k jejich odesílání.

Počítačový vir je vlastně počítačový program, který byl vytvořen člověkem. Veškeré vlastnosti a možnosti tohoto programu byly někým definovány. V současnosti se počet virů blíží k miliónu. Základní vlastností virů je jejich šíření, a proto došlo k prudkému rozvoji až s Internetem. První počítačový virus v pravém slova smyslu, vytvořil americký student v době, kdy Internet teprve začal svůj rozvoj v USA. Tento malý program dokázal dělat pouze dvě věci, odeslat se počítačovou sítí a po příchodu na další počítač udělat svou kopii a odeslat ji dál. Během několika hodin začaly kolabovat první síťové počítače, následně celá síť v USA. Trvalo několik dní, než se podařil obnovit provoz. Zmíněný studen byl stíhán a odsouzen. Z hlediska trestně právní kvalifikace je zde možno vidět trestný čin tehdy, kdy je počítačový vir úmyslně zaslán na počítač s cílem poškození nebo zničení dat. Zaslání může být provedeno jako útok na konkrétní počítač nebo může pachatel rozšířit virus na Internetu nebo uvnitř sítě nějakého subjektu s vědomím následků, které tato činnost přinese. Při cíleném šíření viru lze využít i tzv. sociální inženýrství. V minulosti byly zaznamenány případy, kdy byl vir cíleně zaslán jako příloha v e-mailové zprávě, která se tvářila jako zaslání fotek z dovolené apod. Po otevření přílohy došlo k aktivaci viru, který následně odeslal z napadeného počítače veškeré dokumenty (soubory s příponou *.doc*) na konkrétní počítač.

Tzv. DoS útoky (Denial of Service), které spočívají v přetížení internetového počítače požadavky na služby a jeho následný kolaps nebo alespoň nemožnost poskytovat služby internetovým uživatelům, jsou v poslední době dost rozšířeným způsobem útoků. Cílem pachatele není proniknutí do počítače nebo systému a ani toho nelze touto formou útoku dosáhnout. Veškerá činnost se odehrává a probíhá mimo datovou oblast. Data nejsou ani pozměna nebo jinak narušena. Útok probíhá synchronizovaně z mnoha počítačů umístěných v různých zemích světa, které na základě programů vloženého a spuštěného pachateli, začnou výše popsanou činnost. Majitelé těchto počítačů o této činnosti nevědí. [4]

3.3. Další typy trestné činnosti související s informační kriminalitou

3.3.1. Zneužití platebních karet a skimming

Platební karta umožňuje svým držitelům jednoduše a bezpečně platit za zboží a služby v obchodech, v restauracích, v hotelích a dokonce i na Internetu. Navíc umožňuje také vybírat hotovost z bankomatů, na bankovních přepážkách nebo ve vybraných směnárnách a jiných finančních institucích. Z hlediska funkčnosti lze rozlišit dvě základní verze platebních karet a to karty **debetní** a karty **kreditní**.

Debetní kartou lze čerpat finanční prostředky pouze do výše zůstatku na běžném účtu (či do výše disponibilního zůstatku na účtu s kontokorentním úvěrem). Tím se debetní karty liší od karet kreditních, ze kterých se finanční prostředky čerpají výhradně na úvěr.

Na lícní straně platební karty je vždy uvedeno logo a název platebního systému, ke kterému daná karta náleží, logo banky, která kartu vystavila, číslo platební karty, její platnost a jméno držitele karty popř. elektronický čip. Na rubu je pak místo pro podpis držitele na podpisovém proužku a magnetický proužek. Podle technologie záznamu dat a systému ověření platby se platební karty dělí na **elektronické (čipové a s magnetickým proužkem)**, **embossované a internetové** a jejich možné kombinace**.** Elektronickou kartou lze platit pouze prostřednictvím elektronických terminálů, zatímco kartou embossovanou je možné platit také pomocí ručních imprinterů (tzv. žehliček), tzn. neelektronicky. Internetové karty se používají pouze pro platbu na Internetu a mimo identifikačních údajů nenesou další informace. Platební karty se zpravidla vyrábějí ze tří vrstev netoxického PVC o rozměrech 85,6 x 54 x 0,76 mm (mezinárodní norma ISO 3554).

Pro použití v mechanických snímačích (imprinterech) se na kartu vyrazí nezbytné identifikační údaje (embossing), a to písmem OCR 7B (Optical Character Recognition) velikosti 3,63 mm. Pro ně je určena dolní polovina přední části karty, kterou norma (ISO 7812-1) dělí na čtyři řádky [16]:

1. řádek - **Account Number Line** – obsahuje číslo karty. Prvních 6 číslic určují druh karty a identifikaci vydavatele karty tzv. IIN (**I**ssuer **I**dentification **N**umber), přidělovaná orgány ISO. Zbývajících 8 až 13 míst je určeno pro identifikaci konkrétního klienta. Poslední místo je určeno pro

kontrolní číslici, která se při výrobě karty vypočítává podle tzv. Luhnovy formule pro modulo 10. Umožňuje ověřit, zda bylo číslo karty správně přeneseno do autorizačních a zúčtovacích systémů. Pro karty určené pouze k elektronickým transakcím (bankomaty, platební terminály), jako jsou karty VISA Electron a Maestro, se od první poloviny 90. let nahrazuje reliéfní písmo hladkým tiskem (Indent Printing) nebo laserovým paprskem. Toto opatření vylučuje riziko použití karty na mechanickém snímači (imprinteru).

2. řádek - **Valid Data Line** – uvádí se v ní období platnosti karty (měsíc a rok), a to buď v podobě uvádějící začátek i konec platnosti, nebo jen konec platnosti. Navíc je v této oblasti uváděno u karet MasterCard čtyřmístné identifikační číslo banky (ICA - **I**nterbank **C**ard **A**ssociation). Počet znaků - max. 19.
3. řádek - je určen pro jméno držitele karty. Počet znaků - max. 27.
4. řádek - obsahuje u služebních karet jméno společnosti, k jejímuž účtu je karta vydána. Počet znaků - max. 27.

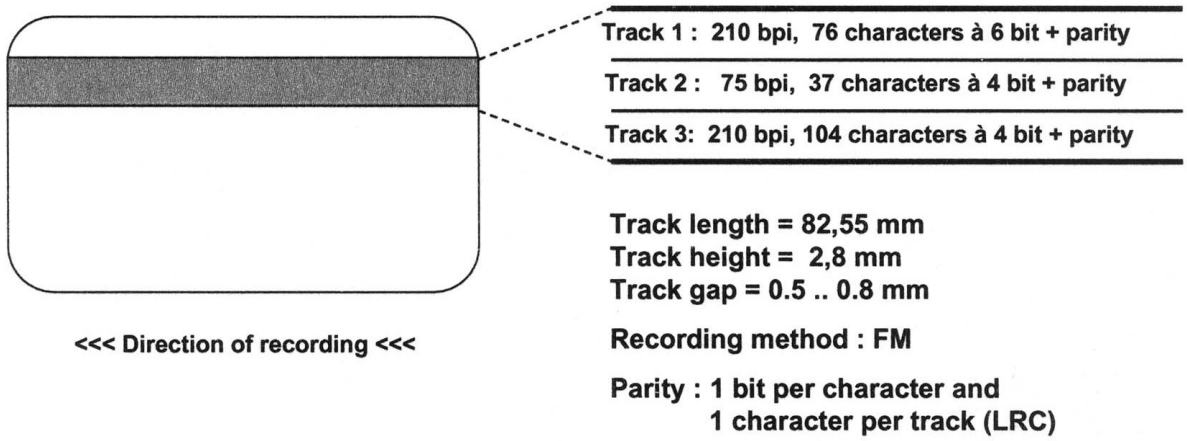
Aby mohla být platební karta použita při elektronickém zpracování, jako např. výběr hotovosti z bankomatů, platby přes POS (**P**oint **O**f **S**ale) terminály apod., musí obsahovat informace jednoznačně identifikující kartu. Ty jsou zaznamenány buď na magnetickém proužku, nebo na tzv. čipu. Čipové karty se začínají čím dál více uplatňovat vedle klasických karet s magnetickým proužkem. Na obrázku č. 5 je zobrazena přední strana čipové platební karty. Základem čipové karty je integrovaný obvod umístěný v plastovém nosiči, obsahující kryptografický koprocesor, paměť a software. Aby mohla být karta považována za čipovou, musí také splňovat podmínky standardu pro čipové platební karty, který definuje, jak má karta vypadat, jakým způsobem má komunikovat s terminály, určuje požadavky na terminály, popisuje bezpečnostní mechanismy a stanovuje obecné požadavky na platební aplikace.

Obrázek 5 - čipová platební karta, (zdroj:[16])

Jak je výše uvedeno u čipových karet, je nutné, aby mohla být platební karta použita při elektronickém zpracování (výběr hotovosti z bankomatů, platby přes POS terminály apod.), musí obsahovat informace jednoznačně identifikující kartu. U klasických karet jsou tyto informace zaznamenány na tzv. magnetickém proužku. Ten má ale své nevýhody, jako např. značné omezení pro množství ukládaných dat a dá se relativně snadno okopírovat. Na obrázku č. 6 je zobrazen vzor zadní strany platební karty s magnetickým proužkem.

V roce 1974 zavedla American Bankers Association normu, která definovala magnetický proužek pro bankovnictví. Tato norma se v roce 1974 stala základem mezinárodních norem ISO, které se používají dodnes. Pro magnetické karty platí norma ISO 7811 a pro čipové karty norma ISO 7816. Norma ISO však ponechává dostatek prostoru pro to, aby např. bankovní platební systémy využívaly některá definovaná pole podle svých potřeb. Snadná výroba a flexibilita standardu umožnily, aby se magnetický proužek rychle rozšířil. Magnetický proužek má dvě nebo tři stopy pro záznam identifikačních údajů, jak je patrné z obrázku č. 7. Zde je elektronicky zaznamenáno číslo karty, její časová platnost, informace, zda se jedná o kartu tuzemskou nebo mezinárodní, zda je možné ji použít v platebních terminálech, v bankomatech nebo v obou zařízeních a jsou zde ještě další doplňující údaje jako např. bezpečnostní kód CVV (**C**ard **V**erification **V**alue) nebo CVC (**C**ard **V**erification **C**ode) a další. [16]

Obrázek 6 - zadní strana platební karty s magnetickým proužkem, (zdroj:[16])



Obrázek 7 - parametry magnetického proužku, (zdroj:[16])

Skimming je forma ilegální činnosti, jejíž podstatou je skutečnost, že zloději umístí skimmovací zařízení (čtečku) na bankomat a vyčkají, až někdo přijde využít jeho služeb. Pokud si nainstalovaného zařízení nikdo nevšimne a výběr se uskuteční, podvodníci z této čtečky, která se zaměřuje na magnetický proužek karty, snadno získají veškeré informace potřebné k tomu, aby mohli vyrobit duplikát platební karty a následně uskutečnit podvodný výběr. Výjimkou nebývá ani miniaturní

kamera umístěná na vhodném místě, odkud lze vypozorovat a zaznamenat PIN kód a další možná data. Na níže uvedených obrázcích č. 10 až č. 12 je zachycena fotodokumentace z případu, kdy na bankomatu byla využita výše popisovaná čtečka.

V případě skimmingu u peněžních automatů (bankomatů) je pro pachatele zásadním problémem získání PIN kódu ke skimmované kartě. Tento problém řeší buď „průklepovou“ klávesnicí nebo, jak je výše zmíněno, umístěním miniaturní kamery na vhodné místo na bankomatu.

V případě využití „průklepové“ klávesnice, tj. tenké klávesnice připevněné nad originální klávesnicí na bankomatu, zobrazeno např. na obrázku č. 8 a č. 9, dojde při stisku klávesy na falešné klávesnici k promáčknutí až na originální klávesnici a následně ke stisku originál klávesy. Budoucí oběť při zadávání PIN kódu nic nepozná, neboť falešná klávesnice je připevněna na bankomatu takovým způsobem, že při běžném pohledu jí nelze poznat. Tato klávesnice je použita pouze pro jeden pokus, jelikož je třeba po zadání PIN kódu blíže nespecifikovaným způsobem sejmout (přečíst) zadaný PIN kód (např. za využití jemného prášku).

Obrázek 8 - falešná klávesnice na bankomatu, (zdroj: vlastní)

Obrázek 9 - vyjmutá falešná klávesnice, (zdroj: vlastní)

Obrázek 10 - skimmovací zařízení připevněné na bankomatu, (zdroj: vlastní)

Obrázek 11 - detailní pohled na skimmovací zařízení, (zdroj: vlastní)

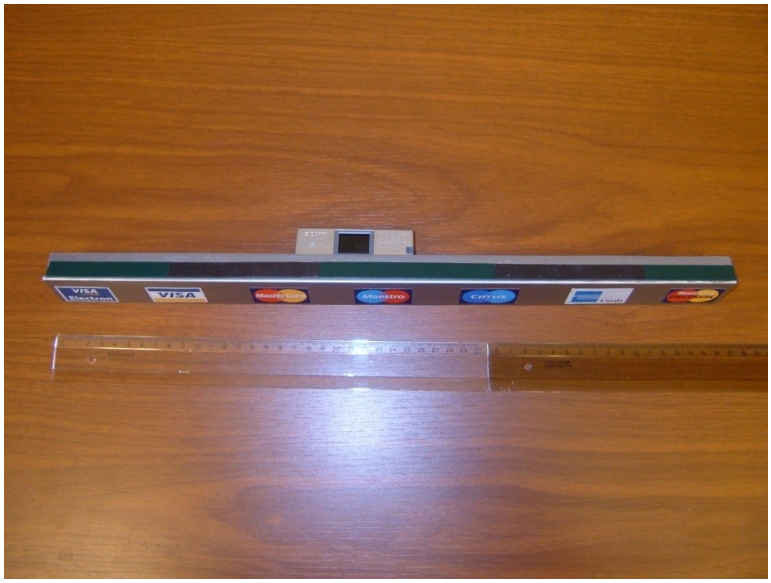
Obrázek 12 - vyjmuté skimmovací zařízení, (zdroj: vlastní)

V případě využití miniaturní kamery vyvstává problém s přenosem video signálu směrem k pachateli a dále s napájením kamery. Většinou to je řešeno tak, že kamera snímá klávesnici pouze malý časový úsek (pouze několik klientů) a poté dojde k demontování kamery a následnému zpracování záznamu. Využívá se buď digitálních fotoaparátů, nebo zařízení „po domácku“ vyrobených. Využití digitálního fotoaparátu je názorně ukázáno na obrázcích č. 13 až č. 15. Taktéž se s úspěchem využívá bezdrátového přenosu ze snímacího zařízení směrem k osobě pachatele a to např. za využití technologie Bluetooth, kdy pachatel se nachází v blízkosti bankomatu a na svém mobilním telefonu přijímá signál ze snímacího zařízení. Dále musí pachatel vhodně zamaskovat toto záznamové zařízení. Využívá se buď různých horních lišt na bankomatu, nebo účelně připevněných různých schránek na bocích, jako např. papírové schránky s reklamními letáky. V příloze č. 1 této práce

jsou na ukázku uvedeny další snímky z případu, kdy bylo využito „po domácku“ vyrobeného zařízení.

Níže je uveden příklad využití digitálního fotoaparátu a jeho maskování do horní lišty s různými logy typů karet.

Obrázek 13 - horní lišta bankomatu, (zdroj: vlastní)



Obrázek 14 - pohled na horní lištu s digitálním fotoaparátem, (zdroj: vlastní)

Obrázek 15 - detail digitálního fotoaparátu, (zdroj: vlastní)

Skimming jako takový bývá čím dál častěji skloňován ve všech pádech nejen ve spojení s bankomaty. V západní Evropě a v USA se totiž člověk může stát obětí tohoto podvodu i při návštěvě restaurace. Poslední dobou se toto děje i v ČR. Vzhledem k tomu, že je běžné kartou zaplatit třeba i za večeři, množí se případy, kdy číšník nevyužije platební kartu pouze k zaplacení účtu za konzumaci jídla. Za pomocí skimmovacího zařízení si snadno zjistí veškerá data, která potřebuje k výrobě duplikátu platební karty.

Z výše uvedeného tedy vyplývá, že uživatel karty si musí uvědomit, že v případě, kdy platí kartou např. v restauraci, svěřuje svojí kartu do cizích rukou a mnohdy se mu karta ztrácí z dohledu. Proto nesmí nikdy dávat kartu z ruky, tj. požádat obsluhu, zda může přinést terminál ke stolu a osobně provést proces platby přes terminál. Dále je vhodné přejít na platební kartu s čipem, protože skimmování čipu je velice obtížné, resp. zatím mi není znám případ, kdy by došlo k takovému skimmování karty s čipem. Při obsluze bankomatu je třeba si všímat atypických prvků na těle bankomatu a v případě pochybností vyhledat jiný bankomat. Na druhou stránku je dobré, že v poslední době se bankovní ústavy samy snaží bránit skimmingu a proto vybavují své bankomaty plastovými předsádkami kartové štěrbiny. Vždy je dobré se informovat u svého bankovního ústavu na jejich opatření vůči skimmingu u jejich bankomatů.

3.3.2. Phishing

Síla každého systému se určuje od síly jeho nejslabšího článku. Toto platí v případě informačních technologií dvojnásob. V případě vedení cíleného útoku na tento nejslabší článek má pachatel jednodušší práci s překonáváním zabezpečení. Pokud tímto článkem je ne moc zdatný uživatel informačních technologií, má útočník vyhráno. Metoda, která využívá této časté a velmi zranitelné slabiny se nazývá *sociální inženýrství* [1] [1].

Tato metoda útoku je založena na klamu či podvodu, kdy cílem je navození takové situace, která nebude vzbuzovat v napadené osobě žádné podezření z nekalého či podvodného jednání. V tu chvíli je napadená osoba ochotna prozradit osobní nebo firemní důvěrné informace, neboť se domnívá, že je to tak v pořádku. Různé způsoby sociálního inženýrství jsou popsány v [9], např. ve formě e-mailové komunikace, telefonního rozhovoru apod..

Vzhledem k tomu, že v poslední době pronikají moderní komunikační a informační technologie téměř do každé lidské činnosti, není nijak překvapivé, že jako prostředek ke sběru dat slouží počítače a síť Internet. A jednou z nejčastěji používaných elektronických forem metod sociálního inženýrství je právě phishing.

Phishing je v současné době jedním z nejčastěji skloňovaných slov v problematice bezpečnosti informačních a komunikačních technologií. Jako definici phishingu lze uvést formulaci dle [21]: „*Phishing (někdy překládáno do češtiny jako rhybaření) je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od obětí útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku. Tato stránka může například napodobovat přihlašovací okno internetového bankovnictví a uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze*“.

Prostředkem phishingu byly po dlouhou dobu především podvržené e-maily, např. na obrázku č. 16 na straně 38, které jednotlivé uživatele lákaly na falešné stránky, z nichž se následně získané údaje automaticky odesílaly k útočníkovi.

[1] Někdy též uváděno jako sociotechnika - ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že útočník je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace.

Za poslední měsíce však útočníci stále více inklinují k použití tzv. *trojských koňů* [2], zejména se snaží o jejich podstrčení prostřednictvím příloh e-mailů, ve kterých je uživatel vybízen k uložení a spuštění přidané přílohy pod záminkou, např. dosud nepublikované hudby, upoutávce na nový film či ukázky zajímavého programu. Tím se ale do napadeného počítače dostane také malý prográmek - trojský kůň. Po své aktivaci trojský kůň potichoučku čeká, až se uživatel připojí na předem určenou stránku, monitoruje stisknuté klávesy (tzv. *keylogger* [3]) a odešle je útočníkovi. Co se týče výskytů keyloggerů v Internetu, tak [1] uvádí: „*Koncem roku 2005 bylo v průměru odhaleno deset variant nových phishing keyloggerů měsíčně a počet nových stránek distribuujících tento škodlivý kód se pohyboval okolo padesáti měsíčně. Naproti tomu v roce 2007 se měsíční průměr nových keyloggerů pohyboval okolo 250, průměrný počet stránek obsahující tento škodlivý kód byl přes 2000 měsíčně.*“

Pro šíření zmiňovaných keyloggerů se nejvíce používají stránky s pornografickým obsahem nebo s obsahem nelegálního software, které zneužívají známých chyb prohlížeče Microsoft Internet Explorer k tomu, aby bez uživatelova vědomí spustily škodlivý kód. Dále se využívá zpráv *instant messagingu* [4] (IM) a trojské koně pro IM, které lákají uživatele k návštěvě a spuštění kódu na vzdálené webové stránce a nejčastějším způsobem je zaplavování e-mailových schránek zprávami, které obsahují škodlivý kód ve své příloze nebo zasílání e-mailových zpráv s odkazem na nějaký webový server, součástí jehož obsahu je kromě jiného také keylogger.

---

[2] **Trojský kůň** (Trojan) - souhrnné označení pro specifický druh programů vykonávajících jinou činnost než ke které jsou původně určeny. Typickým příkladem trojského koně je například program vydávající se za antivirový program, který ve skutečnosti maže některá data na disku či infikuje systém virem [1].

[3] **Keylogger** je software, který snímá stisky jednotlivých kláves. Existují i hardwarové keyloggery. V případě software se jedná o určitou formu spyware. Keylogger není přímo nebezpečný pro počítač, pouze „pomáhá“ ve zjišťování hesel jiných lidí [25].

[4] **Instant messaging** je internetová služba, umožňující svým uživatelům sledovat, kteří jejich přátelé jsou právě připojeni, a dle potřeby jim posílat zprávy, chatovat, přeposílat soubory mezi uživateli a i jinak komunikovat. Hlavní výhodou oproti používání např. e-mailu spočívá v principu odesílání a přijímání zpráv v reálném čase [1].

Od: Ceská sporitelna [csas@csas.cz] Odesláno: út 11.3.2008 9:02
Komu: Holcik Tomas
Kopie:
Předmět: Varování pred novou verzí podvodných e-mailu
Přílohy:

VERIFIED by VISA

ČESKÁ SPOŘITELNA

Varování pred novou verzí podvodných e-mailu

Vázení klienti,

rádi bychom Vás upozornili na novou verzi podvodného e-mailu (tzv. phishingu). Nová verze e-mailu má jako ty predeslé vzbudit dojem, ze byla odeslána z e-mailové adresy Ceské sporitelny, tentokrát vsak z oficiální e-mailové adresy banky csas@csas.cz. Obsahuje odkaz v tele na údajné webové stránky internetového bankovnictví banky a uzivatel je vyzván k prihlásení, tedy zadání osobních bankovních údaju.

Prosím, verifikujte tuto emailovou adresu kliknutím na spojení níze:

https://www.servis24.cz/ebanking-s24/app/register.pl?code=2E1E-EBB6-EA1N-D1EC&step=vrf_email_actions

Verifikovací spojení je platné do 24 hodin.

Obrázek 16 - ukázka phishingového e-mailu, (zdroj: vlastní)

Pachatele phishingových útoků můžeme dělit například z hlediska jejich vztahu k informacím, a to na [1]:

- *Amatéry* - mezi které se řadí hackeři, crackeři, neúspěšní kritici a mstitelé. Jde o osoby pronikající náhodně nebo cílevědomě do informačních systémů tak, že vyhledávají zranitelná místa. Jejich cíle nebo motivace jsou různé.
- *Profesionály* - sem patří pracovníci speciálních tajných služeb, detektivové, žurnalisté, podnikatelé, specialisté informatici, softwaroví piráti či teroristé (zvláštní skupina organizovaného zločinu).

Často se jedná o velmi dobře organizované a propojené členy skupiny, kteří se mezi sebou neznají. Není nijak výjimečné, když členové těchto skupin pocházejí z různých zemí. Veškerá komunikace probíhá elektronickou formou. Vztahy mezi skupinami, zabývající se tímto druhem trestné činnosti, jsou velmi spletité. Tito lidé

vlastně ani nemusejí mít dokonalé znalosti o zneužívaných IT, v dnešní době není problém si jednotlivé části potřebné k provedení útoku zakoupit v prostřednictvím sítě Internet (tzv. phishing toolkity).

Jako odpověď na sílící ochranu uživatelů před phishingem (identifikace a vzápětí likvidace podvodných webů) vymysleli útočníci nový trik. Útočí pomocí takzvaného rychlého přesměrování, kdy existuje řada podobných podvodných webů, a URL ve falešném e-mailu nasměruje klamaného uživatele na speciální IP adresu. Na této IP adrese je umístěný směrovač, který rychle otestuje dostupnost funkčních podvodných webů a uživatele tam přesměruje.

Odhalování pachatelů phishingu je velice složité. Organizovaný charakter této činnosti mimo jiné znamená i to, že je provozována tak, aby byla prakticky nevystopovatelná. Napomáhají tomu i základní principy fungování Internetu a obrovské rozdíly v legislativě jednotlivých zemí. Ve většině případů je phishingový e-mail rozesílán z napadeného počítače (hackerský útok). Vlastník počítače o této aktivitě ani neví a jediné, co ho může trápit, je zpomalení počítače a pomalé spojení do Internetu. Vyhledat, jakým způsobem byl počítač napaden a kdo to způsobil, je prakticky nemožné. A takto napadené počítače se nacházejí po celém světě. Najdou se jak v domácnostech, tak ve firmách či státních institucích. Takto postižených počítačů jsou odhadem minimálně miliony. Dalším problémem je, že phishingové stránky jsou umístěny na nějakém napadeném webu a jejich umístění se neustále mění - zejména proto, že se daří je po několika dnech či týdnech najít a zlikvidovat. Počty napadených (či díky bezpečnostní chybě volně využitelných) webů se pohybuje běžně ve stovkách tisíc a napadeny byly zpravidla opět automaticky fungujícími programy. Phishingové stránky mohou být v některých případech umístěny na vlastní doméně i hostingu. Útočníci pochopitelně neuvádějí kontaktní údaje, platí zpravidla z ukradené kreditní karty a hosting i doména je v natolik problematických zemích, že je prakticky nemožné legálně (i jakkoliv jinak) dosáhnout likvidace podobných stránek. Phishingové stránky mohou také být umístěny na počítačích, které jsou součástí botnet aktivit. V takovém případě se k nim zpravidla přistupuje přes IP adresu a k nalezení vlastníka počítače bude opět potřeba mezinárodní kontakty a spolupráci příslušných orgánů v dané zemi, např. vyžádat si potřebné informace cestou mezinárodní právní pomoci. Při dožadování mezinárodní právní pomoci však vyvstává jeden zásadní problém a to je doba uchovávání

logových záznamů, kdy každá země má jinak právně upravenu dobu archivace logových záznamů, přičemž při odhalování takovéto trestné činnosti hraje velkou roli včasnost získání relevantních informací a stává se, že poskytovatel některé informační služby v době dožádání již nemá předmětné logové záznamy k dispozici. Jediné, co se daří, je odstranění napadeného počítače, resp. škodlivého obsahu a vystopovat, odkud se tam obsah dostal, je prakticky nemožné.

3.4. Odhalování informační kriminality

Při odhalování informační kriminality je nejdůležitější včasnost zjištění a zajištění elektronických stop na médiích. Čím starší stopy, tím nižší jsou jejich důkazní hodnoty a zároveň i menší využitelnost pro určení následných stop v posloupné řadě zjišťování a zajišťování stop. Jedná se o hodiny, maximálně o dny. Tak jako u trestné činnosti spočívající v zasílání výhrůžných e-mailů, šíření zakázaných materiálů (extrémistické, dětská pornografie apod.), která v této práci není popisována, neboť se nejedná o čistě informační kriminalitu, ale pouze o doprovodnou, tj. jedná se trestnou činnost, která je v souběhu s jinou trestnou činností, tak i u informační kriminality obecně, je třeba v souvislé řadě elektronických stop dohledat prvotní místo, odkud došlo k jednání, ve kterém lze spatřovat spáchání trestného činu. U již zmiňovaného zasílání výhrůžných e-mailů, hackerských útoků, rozšiřování zakázaných materiálů apod. to je vždy konkrétní počítač, který obsluhoval v inkriminovanou dobu pachatel a ze kterého byla páchána předmětná trestná činnost. Tento počítač je vždy identifikovatelný určitými znaky, podle kterých lze dohledat v počítačové síti konkrétní počítač. Jedná se např. o tzv. *MAC adresu* [5], což je jedinečná adresa, přidělená jakémukoliv síťovému zařízení. Jelikož tato adresa se dá podvrhnout a poskytovatelé Internetu (dále jen *ISP* [6]) tyto adresy ve většině případů nelogují, tak z tohoto důvodu se informace o MAC adrese nevyužívá.

[5] **MAC adresa** (z anglického „Media Access Control“) je jedinečný identifikátor síťového zařízení, který používají různé protokoly druhé (spojové) vrstvy OSI. Je přiřazována síťové kartě bezprostředně při její výrobě (u starších karet je přímo uložena do EEPROM paměti) a proto se jí také někdy říká **fyzická adresa**. MAC adresa přidělená výrobcem je vždy celosvětově jedinečná [22].

[6] **Internet Service Provider (ISP)** nebo také **Internet Access Provider** (**IAP**) - poskytovatel internetového připojení, firma nebo organizace zprostředkující přístup do Internetu, tj. poskytující telekomunikační služby [23].

Dalším identifikovatelným znakem je tzv. *IP adresa* [7], což je unikátní číselné označení počítače v počítačové síti. ISP logují IP adresy včetně časového údaje vztahujícího se k použití této IP adresy. Tuto zdrojovou IP adresu, identifikující zdrojový počítač, je třeba dohledat v záznamech o telekomunikačním provozu a dále zadokumentovat. Níže je pro názornost přiložen výpis z tzv. „hlavičky“ e-mailu, kde je červeně zvýrazněna IP adresa odesílajícího počítače:

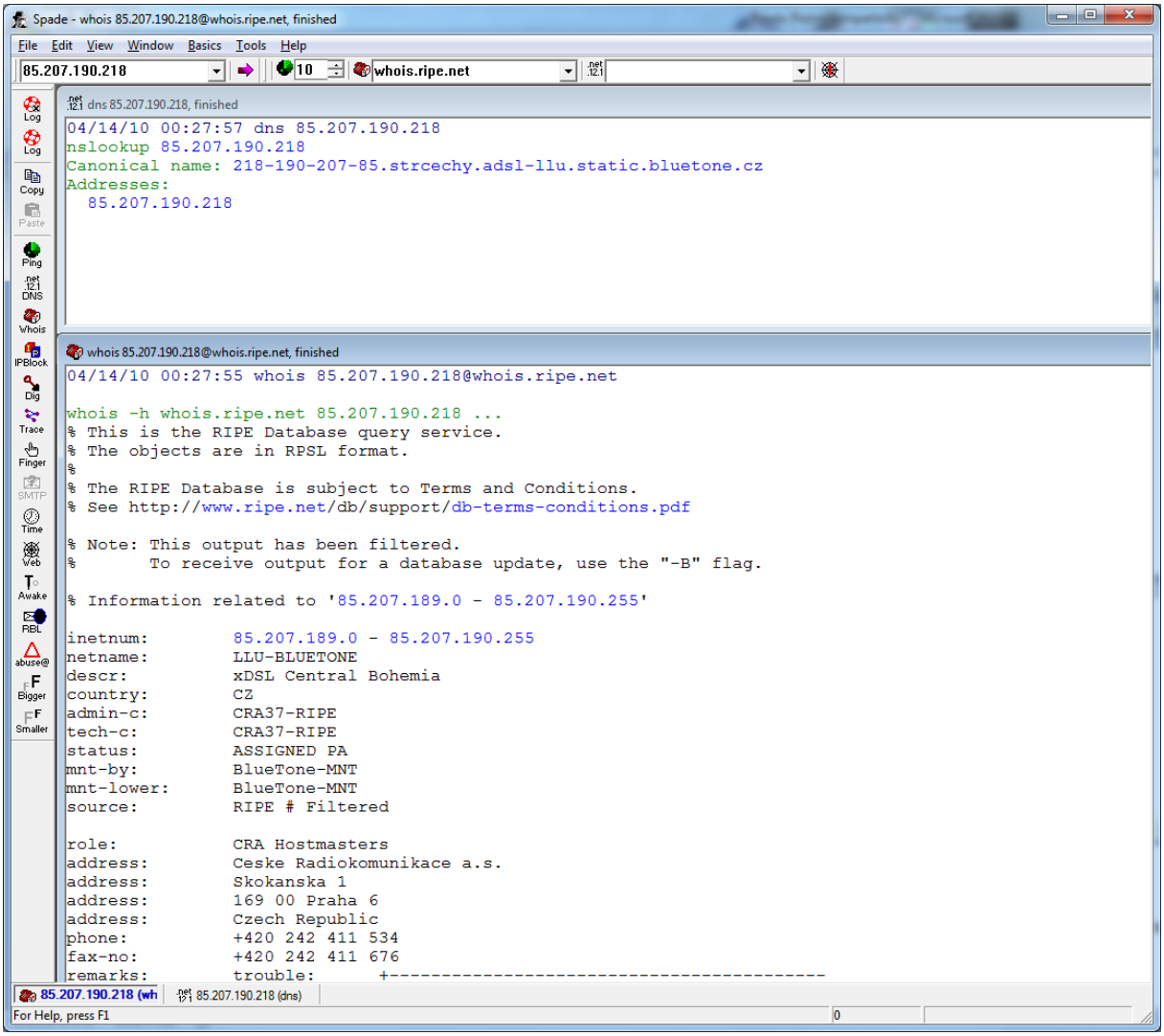
```
From risik.cermak@email.cz Tue Apr 13 22:01:59 2010
Return-path: <risik.cermak@email.cz>
Received: from mxh.seznam.cz ([77.75.72.26])
   id 1O1mHm-00069x-Jk for viki@sedlec.net; Tue, 13 Apr 2010 22:01:59 +0200
To:viki@sedlec.net
Received: from 218-190-207-85.strcechy.adsl-llu.static.bluetone.cz (218-190-207-
85.strcechy.adsl-llu.static.bluetone.cz [85.207.190.218])
   by email.seznam.cz (Email.Seznam.cz) with HTTP for risik.cermak@email.cz;
   Tue, 13 Apr 2010 21:01:37 +0200 (CEST)
Date: Tue, 13 Apr 2010 21:02:03 +0200 (CEST)
From: risik.cermak@email.cz
Content-Type: multipart/mixed;
   boundary="_ca29_-------47cb6b210fec5c862fabee5f2c1338d3"
Subject: Fwd: Fwd: Fwd: : A je to
Mime-Version: 1.0
Message-Id: <30346.191.457-22092-816978371-1271185321@email.cz>
X-Abuse: abuse@seznam.cz
X-Seznam-User: risik.cermak@email.cz
X-QM-Mark: email-qm4<470449454>
X-Spam-Score: -1.9 (-)
Status: R
```

Při analýze elektronických stop je třeba věnovat velkou pozornost určení správné posloupnosti po sobě jdoucích záznamů. U výše uvedeného příkladu je třeba určit prvopočátek elektronické komunikace, což je v tomto případě počítač, ze kterého byl zaslán předmětný e-mail. Zde je třeba věnovat pozornost záznamům začínajících návěštím „Received“ a k nim příslušejícím časovým údajům včetně časových pásem, které jsou vkládány do hlavičky e-mailovými servery, za pomoci

[7] **IP adresa** je číselné označení, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP protokol. V současné době je nejrozšířenější verze IPv4, která používá 32bitové adresy zapsané dekadicky po jednotlivých oktetech. Z důvodu nedostatku IP adres se v současnosti přechází na verzi IPv6, která již používá 128bitové IP adresy [24].

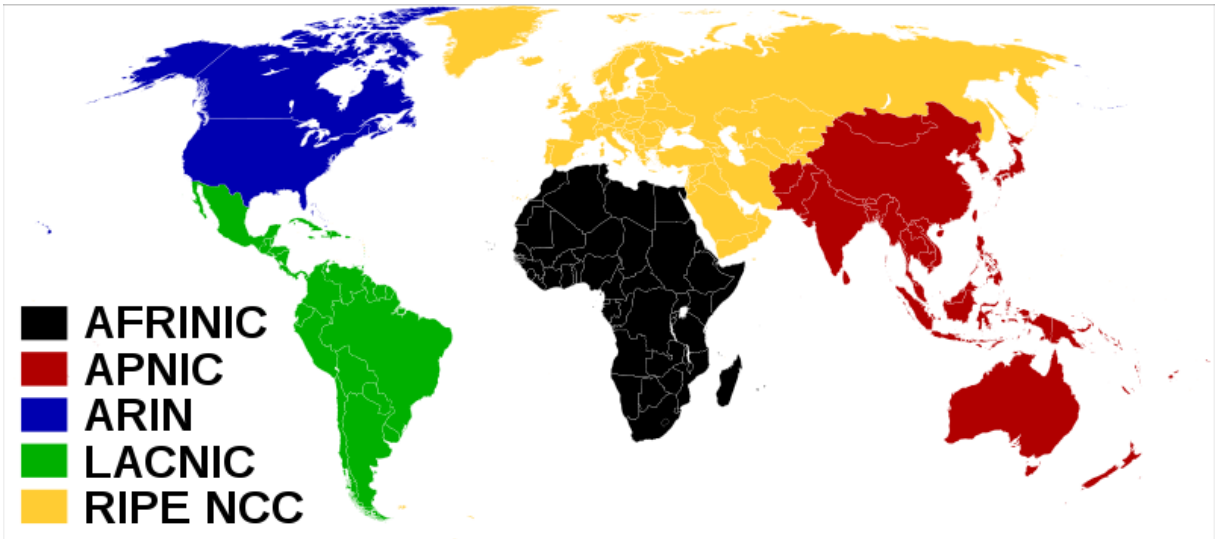
kterých byla tato zpráva poslána. V tomto případě bylo zjištěno, že zpráva byla zaslána dne „**13 Apr 2010 21:01:37 +0200 (CEST)**“ z IP adresy **85.207.190.218**. Následnou lustrací získané IP adresy ve veřejně přístupné databázi RIPE lze zjistit, že tato IP adresa je přidělena xDSL připojení společnosti České Radiokomunikace a.s. Z doménového jména této IP adresy, což je „**218-190-207-85.strcechy.adsl-llu.static.bluetone.cz**“ je patrné, že se jedná o připojení z lokace střední Čechy a že se jedná o staticky přidělenou IP adresu. Tyto informace ale nejsou vždy zjistitelné, vždy záleží na tom, zda ISP tyto informace zahrne do doménového jména. Pro výše uvedenou online lustraci v RIPE a překlad doménového jména se jako jedním z usnadňujících nástrojů osvědčil softwarový produkt „**Sam Spade 1.14**“ od autora Steve Atkinse [8]. Jedná se o freeware produkt sice již z roku 1999, ale pro operativní účely plně vyhovuje. Níže na obrázku č. 17 je uveden screenshot výstupu z tohoto programu, kdy jako dotaz byla vložena výše uvedená IP adresa 85.207.190.218. V horním okně je vidět výsledek překladu doménového jména a ve spodním okně je výsledek dotazu do databáze RIPE, resp. dotaz na server *whois.ripe.net*. Jedná o online dotaz ze dne 14.4.2010.

[8] Internetové stránky produktu jsou na adrese http://samspade.org, přičemž tyto stránky jsou již delší dobu nefunkční. Produkt lze stáhnout např. na adrese http://www.fyxm.net/Sam-Spade-18478.html.



Obrázek 17 - výstup z programu Sam Spade 1.14, (zdroj: vlastní)

Při lustraci v databázi RIPE v tomto programu je třeba věnovat pozornost vhodného zvolení dotazového serveru regionálního internetového registru, neboť při špatném zvolení je výsledkem, že dotazovaná IP adresa je z rozsahu IANA (**I**nternet **A**ssigned **N**umbers **A**uthority), což je organizace která dohlíží celosvětově na přidělování IP adres, správu kořenových zón DNS atd. Následující mapka na obrázku č. 18 ilustruje rozdělení světa na pět regionálních internetových registrů, tj. **ARIN** (USA a Kanada), **AfriNIC** (Afrika), **RIPE NCC** (Evropa, střední Východ a centrální Asie), **LACNIC** (Latinská Amerika) a **APNIC** (Asie a Pacifik) [26]:



Obrázek 18 - mapka rozdělení světa na regionální internetové registry, (zdroj:[26])

Pro ustanovení koncového bodu, resp. osoby pachatele, je nutné dožádat ISP o sdělení údajů o uskutečněném telekomunikačním provozu v souladu s ustanovením § 88a zákona č. 141/1961 Sb. (Trestní řád), jelikož se jedná o telekomunikační tajemství a k prolomení tohoto tajemství je třeba soudního příkazu. ISP se dožaduje o sdělení konkrétního subjektu, který měl v inkriminovaném časovém údaji nebo období přidělenu předmětnou IP adresu. Z důvodu různých světových časových pásem je třeba věnovat velkou pozornost získaným časovým údajům a nadále je uvádět vždy včetně označení konkrétního časového pásma, aby nedošlo k časovému posunu v časovém údaji a tudíž nedošlo k ztotožnění úplně jiného subjektu. ISP mají ze zákona[9] povinnost držet údaje o uskutečněném telekomunikačním provozu (logové záznamy) po dobu 6 měsíců až 1 rok, přičemž praxe ukazuje, že ISP využívají spodní hranici, tj. 6 měsíců a po této době již nemají k dispozici zmíněné logové záznamy.

Výše uvedené zákonné podmínky se ukazují v praxi jako problematické pro vyšetřovatele s ohledem na dostupnost logových záznamů, tj. jediného zdroje elektronických stop využitelných pro další postup v odhalování této trestné činnosti. Z tohoto důvodu je nutné postupovat v šetření rychle a včasně, neboť jakmile dojde k znepřístupnění logového záznamu, tak vyvstává problém s důkazní nouzí.

[9] Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů ze dne 22.2.2005 a dle prováděcích vyhlášek Min. informatiky č. 485/2005 Sb. a č. 486/2005 Sb. ze dne 7.12.2005.

Při odhalování ostatní informační kriminality je postup vyšetřování obdobný, jenom se liší ve vstupních informacích, jako např. při napadení nějakého informačního systému (napadení server či napadení webových stránek) se musí analyzovat logové záznamy přístupů z napadeného systému. Pro ilustraci je níže uvedena část logového záznamu přístupů z napadeného serveru, který byl použit jako mezičlánek při mezinárodní trestné činnosti, spočívající v rozesílání počítačových virů:

67.195.114.218 - - [17/Jan/2010:18:19:45 +0100] "GET /galerie/include/smarty/xceyc/former.php HTTP/1.0" 200 29267 "-" "Mozilla/5.0 (compatible; Yahoo! Slurp/3.0; http://help.yahoo.com/help/us/ysearch/slurp)"
204.8.156.142 - - [17/Jan/2010:18:51:27 +0100] "GET /galerie/include/css/stat.php HTTP/1.1" 200 380 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
85.214.73.63 - - [17/Jan/2010:18:51:38 +0100] "POST /galerie/include/css/stat.php HTTP/1.1" 302 380 "http://fejt.din.cz/galerie/include/css/stat.php" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
77.222.131.40 - - [17/Jan/2010:18:51:42 +0100] "GET /galerie/include/css/stat.php HTTP/1.1" 200 18608 "http://fejt.din.cz/galerie/include/css/stat.php" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
85.214.73.63 - - [17/Jan/2010:18:51:44 +0100] "GET /galerie/include/css/inc/images/dot.gif HTTP/1.1" 304 - "http://fejt.din.cz/galerie/include/css/stat.php" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
78.142.140.194 - - [17/Jan/2010:18:51:45 +0100] "GET /galerie/include/css/inc/images/style.css HTTP/1.1" 304 - "http://fejt.din.cz/galerie/include/css/stat.php" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
65.55.106.204 - - [17/Jan/2010:19:00:34 +0100] "GET /robots.txt HTTP/1.1" 200 286 "-" "msnbot/2.0b (+http://search.msn.com/msnbot.htm)"

Při analýze takovýchto logových záznamů je třeba věnovat pozornost HTTP statusům a HTTP metodám GET a POST. Pro účely vyšetřování jsou zajímavé výsledky HTTP metody POST.

Jak bylo již výše zmíněno, při odhalování trestné činnosti v IT je třeba včasnosti zjištění a následného zajištění elektronických stop. Dále je třeba věnovat velkou pozornost analýze získaných informací a v neposlední řadě i spolupráci od ISP.

Závěr

Informační kriminalita (počítačová kriminalita) je v poslední době velice diskutovaným problémem jak v české společnosti, tak i na mezinárodní úrovni, jelikož tato kriminalita nezná hranic.

Cílem této bakalářské práce bylo popsat a zdokumentovat problematiku zneužívání informačních technologií při páchání trestné činnosti a její následné odhalování. V rámci popisování byly zmíněny i různé typy dělení této kriminality. Pro názornost zde byly blíže popsány případy, u kterých jsem se účastnil jejich odhalování. S ohledem na možný omezený rozsah této práce zde nebyly popsány další jednání nesoucí znaky informační kriminality, neboť veškeré oblasti informační kriminality vykazují stejné obecné znaky a tudíž i odhalování této trestné činnosti (tohoto jednání) je vedeno stejným způsobem.

Závěrem lze shrnout, že prvotním a základním úkolem při odhalování této trestné činnosti je včasné zjištění a zajištění „elektronických“ stop, tedy veškerých stop, dokazujících proběhnuvší telekomunikační provoz mezi útočníkem a obětí. Podle typu spáchaného útoku je tato řada na sobě navazujících stop různě dlouhá a tudíž je i různě náročné zajišťování těchto stop. Dále zde vyvstává problém se zákonem stanoveném období archivování takovýchto stop poskytovateli telekomunikačních služeb, kdy v případě zasahující trestné činnosti mimo území České republiky je třeba vyžádat tyto stopy (údaje o uskutečněném telekomunikačním provozu) od bezpečnostních složek dotčených států, přičemž dle novelizované směrnice EU č. 2002/58/EC je doporučené období 6 měsíců až 2 roky, přičemž každý členský stát si toto období upravuje svým národním právem. Jestliže toto období je 6 měsíců od uskutečnění provozu, stává se, že v tomto období se nestihne včasně zareagovat a dožádat tyto informace mezinárodní právní pomocí, kdy tato pomoc je dožadována cestou několika státních orgánů na obou stranách. Totéž se dotýká i problému v českém právu, kdy vyjde najevo řada po sobě jdoucích stop a je třeba ztotožnit veškeré důležité uzly proběhnuté komunikace (např. u cíleného napadení v řadě za sebou jdoucích serverů apod.), kdy většina poskytovatelů v ČR striktně dodržuje minimální zákonné období, což je zmiňovaných 6 měsíců. Po této době data znepřístupní (učiní anonymní). V minulosti, tj. před účinností zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, nebyla zákonem stanovena zmíněná doba archivace

a většina ISP archivovala tyto údaje po dobu 2 let. Nicméně na druhou stranu neměli povinnost tyto údaje držet. S nárůstem počtu připojených subjektů k síti Internet a z toho vyplývajícího zvětšení datového toku, vyvstaly pro ISP větší finanční nároky na archivování těchto údajů. Na základě připomínek těchto ISP a dále v souladu s výše uvedenou směrnicí EU č. 2002/58/EC byl následně přijat zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, a tím vznikl výše popsaný problém se zákonem stanoveném období archivování. V současné době lze konstatovat, že toto období je pro orgány činné v trestním řízení nevyhovující a je třeba inicializovat jednání o možném zvýšení minimální doby archivace na jeden rok.

Po zajištění výše uvedených elektronických stop a následné analýze nastupuje již standardní kriminalistická praxe, jako např. výslechy osob a z nich plynoucí určení trestní odpovědnosti, domovní prohlídky, prohlídky jiných prostor a pozemků, zajišťování věcí a jejich následné znalecké zkoumání apod.

Seznam použitých zdrojů

[1] BADIN, Jaromír – PÍSECKÝ, Václav. *Problematika phishingu a podobných podvodných technik sběru informací prostřednictvím informačních a komunikačních technologií.* Interní materiál. Praha: Policie ČR, 2008.

[2] Business Software Alliance. *Tisková zpráva - Softwarové pirátství kleslo: v Česku se užívá 38% softwaru nelegálně.* Praha. 12.5.2009. [online]. [cit. 2010-04-21] URL:<http://global.bsa.org/globalpiracy2008/pr/pr_czechrep.pdf>.

[3] Council Of Europe. *ETS No. 185 - Convention on Cybercrime. Budapest. 23.11.2001.* [online]. [cit. 2010-04-21]. URL:<http://conventions.coe.int/Treaty/EN/Treaties/HTML/185.htm>.

[4] DASTYCH, Jiří. *Metodika objasňování trestné činnosti na úseku počítačové kriminality - útok na data.* Interní materiál. Praha: Policie ČR, 2001.

[5] DASTYCH, Jiří. *Metodika odhalování a dokumentace trestných činů podle § 152 trestního zákona - softwarové pirátství*. Interní materiál. Praha: Policie ČR, 2001.

[6] DOČEKAL, Daniel. *Jak se dělá phishing* [online]. [cit. 2009-08-06]. URL:<http://www.lupa.cz/clanky/jak-se-dela-phishing>.

[7] DOSTÁLEK, Libor – KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 4. vydání. Praha: CP Books, 2005. ISBN 80-7226-675-6.

[8] *Evidenčně statistický systém kriminality.* [databáze online]. Praha: Policie ČR, 2010. [citováno 2010-01-14]. Dostupné z Intranetu Policie ČR.

[9] GARFINKEL, Simson – SPAFFORD, Gene. *Web Security, Privacy and Commerce.* 2nd edition. Sebastopol (California): O'Reilly, 2002. ISBN 0-596-00045-6.

[10] GILLELAND, Michael. *Anatomy of Credit Card Numbers.* [online]. [cit. 2010-04-21]. URL:<http://www.merriampark.com/anatomycc.htm>.

[11] GŘIVNA, Tomáš - POLČÁK, Radim. *Kyberkriminalita a právo*. 1. vydání. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

[12] MATĚJKA, Michal. *Počítačová kriminalita.* 1. vydání. Praha: Computer Press, 2002. ISBN 80-7226-419-2.

[13] Ministerstvo vnitra České republiky. *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení* [online]. [cit. 2009-08-06]. URL:<http://web.mvcr.cz/archiv2008/dokument/2006/informacni.pdf>.

[14] Ministerstvo vnitra České republiky. *Základní definice, vztahující se k tématu kybernetické bezpečnosti* [online]. [cit. 2010-04-21]. URL:<http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx>.

[15] PORADA, Viktor – KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality.* 1. vydání. Praha: Policejní akademie České republiky, 1998. ISBN 80-85981-75-0.

[16] ŘANDA, Vít. *Platební karty a skimming*. Pardubice: Univerzita Pardubice, 2008. Semestrální projekt pro předmět Informační a komunikační systémy (KIKS).

[17] *Úplné znění zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.* Ostrava: Sagit, 2010. ISBN 978-80-7208-782-2.

[18] *Úplné znění zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.* Ostrava: Sagit, 2001. ISBN 80-7208-236-1.

[19] *Úplné znění zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů.* Ostrava: Sagit, 2008. ISBN 978-80-7208-666-5.

[20] *Úplné znění zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. Ostrava: Sagit, 2010. ISBN 978-80-7208-782-2.*

[21] Wikipedie: Otevřená encyklopedie. *Phishing* [online]. [cit. 2009-08-06]. URL:<http://cs.wikipedia.org/wiki/Phishing>.

[22] Wikipedie: Otevřená encyklopedie. *MAC adresa* [online]. [cit. 2010-04-13]. URL:<http://cs.wikipedia.org/wiki/MAC_adresa>.

[23] Wikipedie: Otevřená encyklopedie. *Internet Service Provider* [online]. [cit. 2010-04-13]. URL:< http://cs.wikipedia.org/wiki/Internet_service_provider>.

[24] Wikipedie: Otevřená encyklopedie. *IP adresa* [online]. [cit. 2010-04-13]. URL:< http://cs.wikipedia.org/wiki/IP_adresa>.

[25] Wikipedie: Otevřená encyklopedie. *Keylogger* [online]. [cit. 2009-08-06]. URL:<http://cs.wikipedia.org/wiki/Keylogger>

[26] Wikipedie: Otevřená encyklopedie. *Regional Internet registry* [online]. [cit. 2010-04-14]. URL:< http://en.wikipedia.org/wiki/Regional_Internet_registry>.

Seznam obrázků

Seznam použitých zkratek

ADSL	Asymetrická digitální zákaznická linka (angl. Asymetric Digital Subscriber Line)
BSA	Business Software Alliance
CD-R	Kompaktní disk s možností zápisu (angl. Compact Disc Recordable)
CEST	Letní středoevropské časové pásmo (angl. Central European Summer Time)
CVC	Bezpečnostní kód (angl. Card Verification Code)
CVV	Bezpečnostní kód (angl. Card Verification Value)
DoS	Útok za pomocí odmítnutí služby (angl. Denial Of Service)
DVD-R	Digitální optický disk s možností zápisu (angl. Digital Versatile Disc Recordable)
ESSK	Evidenčně statistický systém kriminality
FTP	Protokol pro přenos souborů (angl. File Transfer Protocol)
HTTP	Protokol pro přenos dokumentů (angl. Hypertext Transfer Protocol)
IIN	Identifikační označení vydavatele platební karty (angl. Issuer Identification Number)
IM	Internetová komunikační služba (angl. Instant Messaging)
ISO	Mezinárodní organizace pro normalizaci (angl. International Organization For Standardization)
ISP	Poskytovatel internetového připojení (angl. Internet Service Provider)
IT	Informační technologie
MAC	Identifikátor síťového zařízení (angl. Media Access Control)
OCR	Optické rozpoznání písma (angl. Optical Character Recognition)
PIN	Osobní identifikační číslo (angl. Personal Identification Number)
POS	Bezhotovostní platební terminál (angl. Poit Of Sale)
PVC	chemická zkratka pro Polyvinylchlorid
SMS	Služba krátkých textových zpráv (angl. Short Message Service)
TCTV 112	Telefonní Centrum Tísňového Volání - linka 112
WiFi	Standard pro bezdrátovou síť (angl. Wireless Fidelity)

Seznam příloh

Příloha č. 1

Níže jsou pro ukázku uvedeny snímky z případu tzv. „skimmingu“ u bankomatu, kdy bylo využito „po domácku“ vyrobeného zařízení na skimmování a na záznam stisknutých kláves při zadávání PINu .

Obrázek 19 - pohled na místo činu, (zdroj: vlastní)

Obrázek 20 - bližší pohled na místo činu, (zdroj: vlastní)

Obrázek 21 - pohled na skimmovací zařízení, (zdroj: vlastní)

Obrázek 22 - pohled na vnitřek skimmovacího zařízení, (zdroj: vlastní)

Obrázek 23 - pohled na záznamové zařízení, (zdroj: vlastní)

Obrázek 24 - pohled na vnitřek záznamového zařízení, (zdroj: vlastní)