Počítačová kriminalita

Zdeněk Martínek, Aleš Vyhnálek

Vedoucí práce: doc. Dr. JUDr. Jan Hejda

Úvod

Za počítačovou kriminalitu se obvykle označuje činnost, při které je počítačové vybavení či počítačová sí nástrojem, cílem nebo místem uskutečňování trestné činnosti. V širší definici se tímto termínem někdy označují i tradiční trestné činy, jen uskutečňované pomocí počítače. Může se jednat o vydíraní, podvody, padělání atd. V této práci se ale těmito činy nebudeme zabývat, zaměříme se na počítačovou kriminalitu v užším slova smyslu.

V posledních letech se jedná o nejdynamičtěji se vyvíjející druh trestné činnosti. Na začátku rozvoje počítačů se jednalo o izolované činy jedinců s cílem hlavně upozornění na sebe. S posunem výpočetní techniky směrem ke spotřební elektronice a s rozšířením uživatelské základny na v podstatě všechny druhy lidí ale můžeme pozorovat výrazný posun k cílevědomé snaze získat od obětí nějaký osobní prospěch. Jedná se hlavně o peníze, ale může se jednat i o osobní informace, přístupová hesla, chráněné dokumenty apod. Další formou osobního prospěchu je využití dat chráněných autorskými právy – hudba, video a software.

U každé nelegální aktivity jsme se vždy snažili poskytnout nějaký praktický příklad, který dobře danou problematiku ilustruje. Také jsme se snažili poskytnou přehled možných prevenčních opatření, by to jedno nejdůležitější se v nich opakuje vždy dokola: lidská opatrnost.

Na jedné internetové stránce o virech jsme našli zajímavý citát, který by mohl být jakýmsi mottem naší práce:

Jenom dvě věci jsou nekonečné: vesmír a lidská hloupost.
A tím vesmírem si nejsem úplně jistý.
Albert Einstein

Vymezení

V práci budeme postupně probírat jednotlivé formy této trestné činnosti. Při klasifikaci těchto činností se můžeme setkat s několika členěními, často používané je například členění Rady Evropy, které člení tyto činnosti do dvou seznamů:

Minimální seznam:

počítačové podvody,

počítačové falzifikace,

poškozování počítačových dat a programů,

počítačová sabotáž,

neoprávněný přístup,

neoprávněný průnik,

neoprávněné kopírování autorsky chráněného programu,

neoprávněné kopírování fotografie.

Volitelný seznam:

změna v datech nebo počítačových programech,

počítačová špionáž,

neoprávněné užívání počítače,

neoprávněné užívání autorsky chráněného programu.

Dělení je platné pro evropské země. V minimálním seznamu jsou vyjmenovány činy, které by měly být zapracovány v právních řádech jednotlivých zemí. Ve volitelném seznamu jsou činy, které Rada Evropy pouze doporučuje do nich zahrnout.

Můžeme uvést i členění z učebnice Kriminalistika (Viktor Porada a kol.) [1]

1. **Neoprávněné zásahy do vstupních dat.** Jedná se o změnu vstupních dat pro zpracování počítačem, či o změnu v množství přijatého zboží atd. Může se např. jednat o změnu čísla účtu k provedení určité operace apod.
2. **Neoprávněné změny v uložených datech.** Pachatel využije změny dat k dosažení svého cíle. Po realizaci často pro zamaskování vše vrátí na původní stav.
3. **Neoprávněné pokyny k počítačovým operacím.** Pachatel dává přímý nebo zprostředkovaný pokyn (přes své programové prostředky) k neoprávněným operacím. Velmi často se jedná o převádění peněz.
4. **Neoprávněné pronikání do počítačů, počítačového systému a jeho databází.** Situace, kdy se pachatel přes počítačovou sí neoprávněně připojí na cizí systém. Pachatel sleduje buď své osobní uspokojení (dokazuje si, že je schopen překonat různé ochranné prostředky), nebo může zpřístupněné informace dále využít. Viz hacking.
5. **Napadení cizího počítače, jeho programového vybavení a souborů dat v databázích.** Pachatel pomocí počítačového viru či jiného software (viz malware) napadá cizí počítače. Cílem může být zablokování počítače, vymazání dat, získání dat pachatelem apod.

Tato členění nejsou běžnému člověku podle našeho názoru srozumitelná. Vytvořili jsme proto členění vlastní. Šlo nám o to, aby si běžný člověk dovedl ihned představit, o co se jedná. Naše řazení není vlastně ničím jiným než výčtem, bez nějakého hlubšího vnitřního členění.

Do přehledu jsme také zařadili softwarové pirátství a kopírování audiovizuálních děl. Do počítačové kriminality, tak jak se definuje, pravděpodobně tyto činnosti nepatří, jedná se ale o tak rozšířené a diskutované jevy, že jsme je do přehledu zařadili.

Související právní předpisy

V souladu se zadáním jsme se dále v textu nezabývali zákony, které se této problematice věnují – snažili jsme se, aby byla práce srozumitelná pro každého. Je ale nutné je na počátku alespoň uvést.

- Trestní zákon, č. 140/1961 Sb., hlavně hlava IX – Trestné činy proti majetku.
- Zákon o ochraně osobních údajů, č. 101/2000 Sb.

- Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), č. 121/2000 Sb.
- Zákon o regulaci reklamy, č. 138/2002 Sb.
- Zákon o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech, č. 124/2002 Sb.
- Zákon o elektronickém podpisu a o změně některých dalších zákonů, č. 227/2000 Sb.
- a další…

Typický pachatel a motivy jeho jednání

Počítačové kriminalita je typicky páchána zaměstnancem poškozené organizace. Oproti vžitým představám se nejedná o vysoce inteligentního počítačového odborníka, ale spíše je to člověk hamižný, bezohledný s touhou po moci.

Převládající skupinou motivů jsou **zištné** motivy, tedy snadno a rychle získat velké objemy prostředků. Dále se může jednat o motivy vyplývající z konfliktů v mezilidských vztazích, touha po získání moci, touha dokázat si intelektuální převahu, touha překonat pocit nedocenění svých schopností, krycí motivy k zamaskování jiné trestné činnosti, snaha o vyniknutí v obchodní činnosti, politické motivy.

Malware

Malware je software, který byl vytvořen aby infiltroval nebo poškodil počítačové systémy bez vědomí uživatele. Je to složenina ze slov „malicious“ (zákeřný) a „software“. Většinou bývá tento termín použit obecně pro jakýkoliv software, který má nepřátelský, dotěrný nebo obtěžující charakter.

Viry

Infikuje nejčastěji spustitelné soubory tím, že se tělo viru k nim připojí nebo přepíše část souboru tak, aby se nezměnila velikost souboru. Při spuštění takového souboru dojde k aktivování viru. Také se viry často zapisují do boot sektorů disků a registrů. Virus pak provádí další činnosti. Původní soubor lze v některých případech vyléčit odstraněním těla viru.

Prevence

Proti virům se můžeme účinně bráni velkou škálou antivirových programů, které se neustále zdokonalují a doplňují informace o nových virech. Základem prevence je kvalitní antivirový program. Dále je velmi důležité udržovat virovou databázi antivirového programu v aktuálním stavu.

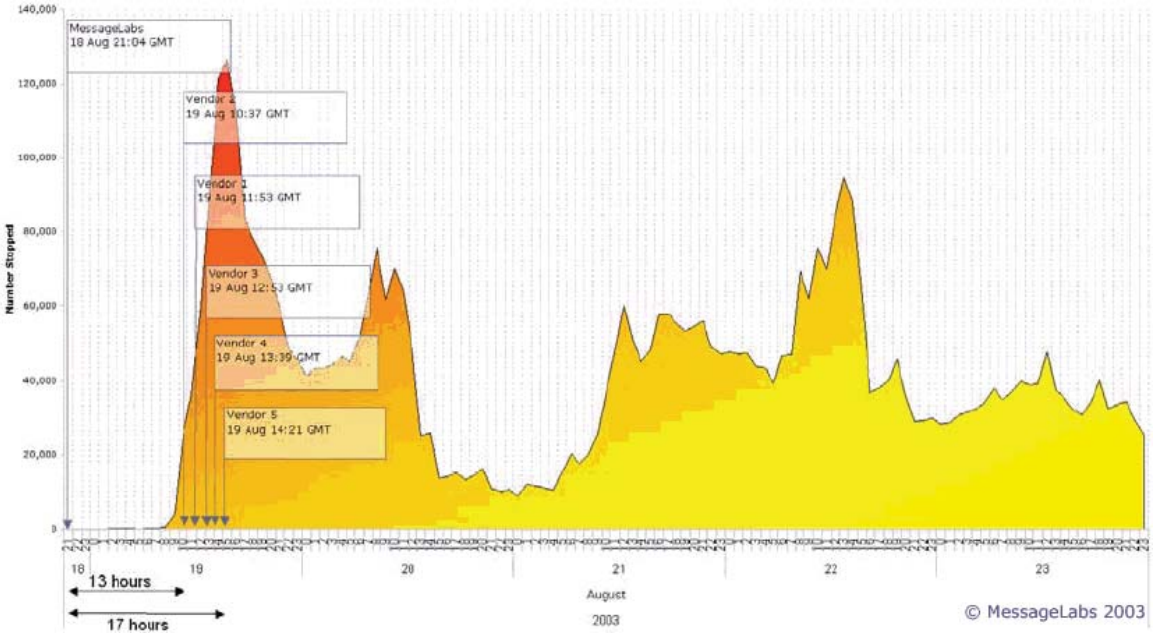
Praktický příklad

Společnost Computer Economics vytvořila hodnocení nejškodlivějších virů v uplynulých šesti letech. Nejvíce škod způsobil vir s názvem Love Bug, který zaznamenal největší vrchol v roce 2000 a jímž napáchané škody byly celosvětově odhadnuty na 8,75 miliardy dolarů [3]. Druhé místo obsadil vir s názvem MyDoom se škodou ve výši 5,25 miliardy. Vir

MYDOOM je považován také za nejrychleji se šířící vir (napadl 12 000 systémů za hodinu).

Průběh šíření viru

Obr. č. 1: Průběh šíření viru



Tento graf převzatý z [2] ukazuje průběh šíření viru WIN32/Sobig. F v prvních hodinách od jeho vzniku. Vertikální osa znázorňuje množství nakažených e-mailů a na horizontální ose je čas. Poprvé byl virus zachycen ve 21:00. Hlavní nárůst infikace tímto virem bylo až druhý den ráno kolem deváté hodiny. Virus byl rozpoznán až antivirovým programem s aktualizací v 10:37, přičemž byl virus nejaktivnější po 14:00. To nám dokazuje nutnost včasné aktualizace antivirového programu.

Zde uvádíme tabulku, která nám ukazuje procento infikovaných emailů za časové období 21. 3–27. 3 – zdroj: <www.virusovyradar.sk>.

Obr. č. 2: Infikace emailů

Červi

Počítačový červ je označován jako zvláštním typ počítačového viru. Šíří se prostřednictvím nakažených souborů či paketů počítačové sítě. Po infikaci počítače dochází k odeslání kopie červa prostřednictvím internetu na další systémy a tak se červ velmi rychle šíří a způsobuje především zahlcení systému. Princip šíření červů je stejný jako u počítačových virů a to skrz bezpečnostní díry v operačních systémech nebo aplikacích. Nejčastěji se červy šíří jako příloha emailových zpráv.

Prevence

Stejná jako v případě počítačových virů a to prostřednictvím antivirových programů. Dále je velmi důležité neotvírat podezřelé emaily.

Praktický příklad

V roce 2003 se začal masově šířit červ s názvem **Win32/Blaster** (jinak označován také jako Win32/Lovsan). Zrádnost červa spočívá v tom, že se nešíří jako příloha v e-mailu a uživatelé nevědí, že byli infikováni. Tento červ využívá k šíření bezpečnostní díru v systému Microsoft Windows NT,XP,…. Červ se projevuje v počítači tak, že se objeví okno s tím, že počítač bude za minutu restartován a po uplynutí doby se počítač restartuje. V kódu viru byl také schován text: *„Bille Gatesi, přestaň dělat prachy a sprav si svůj software.“* Proti Blasteru byla vydána speciální programová „záplata“ a program na jeho likvidaci. [6]

Trojany

Je to speciální druh viru, který odesílá data z počítače bez vědomí uživatele. Jde o program, který tajně provádí škodlivou činnost v počítači a tváří se jako legální program. Od viru se liší především tím, že se v počítači objevuje pouze v jednom souboru, ve kterém je ukryt a nemá schopnost se přenášet na jiné soubory.

Prevence

Stejně jako u virů spočívá prevence v kvalitním antivirovém programu, který je potřeba pravidelně aktualizovat. Dále neotvírat a nestahovat podezřelé zprávy a aplikace.

Praktický příklad

Nejznámějším trojským koněm je v současnosti trojský kůň Gozi, který přišel z Ruska. Dle časopisu Computerworld má již na kontě asi 10 000 záznamů osobních údajů, jejichž cena se odhaduje kolem 2 miliony dolarů. Tento trojský kůň nepracuje typicky na principu záznamu všech úhozů na klávesnici, ale usadí se v prohlížeči MS Internet Explorer). [7]

Adware

Program, který lze zařadit do kategorie neškodných. Tyto aplikace mají spíše obtěžující charakter ve formě vyskakovacích pop-up reklamních oken při navštívení webových stránek či nechtěná změna domovské stránky v prohlížeči. Někdy bývá ADWARE doprovázen „EULA“ – End User License Agreement – licenčním ujednáním.To znamená, že

uživatel při instalaci programu musí souhlasit i s instalací adware, který je jeho součástí, jinak budou zablokovány některé funkce programu.

Prevence

U pop-up oken je možné v nastavení prohlížeče zakázat jejich spouštění při návštěvě takové stránky. V případě změny adresy domovské stránky je dobrý způsob obrany prostřednictvím speciálních programů (př. Ad-Aware).

Praktický příklad

Obr. č. 3: Pop-Up

(Obrázek je převzatý ze stránky http://computer.howstuffworks.com/web-advertising5.htm)

Dialery

Dialer je program, který využívá dial-up připojení k internetu. Princip programu spočívá ve změně telefonního čísla pro přístup na Internet. Program zamění telefonní číslo pro Internetové spojení za číslo se zvláštním tarifem (tzv. žluté linky – 60 Kč / min.). Tento program se dostane do počítače především návštěvou nevhodných stránek (př. pornografické ,nabízející nelegální software,…) a zcela nenápadně bez vědomí uživatele. Dialer existuje ve dvou typech – legální a nelegální. Legální dialery jako platba za užívání služeb dané webové stránky. A pro tyto dealery byla dohodnuta konkrétní pravidla [8], která by měla vstoupit v platnost:

- Maximální délka hovoru je 60 minut či dosažení částky 4200 korun
- Zvýraznění ceny za minutu, která je placená za připojení a cena musí být zvýrazněna
- Zobrazení plných podmínek a kontaktních údajů na poskytovatele.
- Souhlas uživatele musí být vyjádřený prostřednictvím checkboxu „Souhlasím s cenou".
- Nastavení volání je možné jen pro jedno konkrétní připojení a ne natrvalo
- Dialer nesmí zůstat v počítači uživatele.
- Pomocí služby se nebude možné připojit k ostatním službám Internetu.

Nelegální jsou takové, které přesměrují uživatele, bez jeho vědomí, na telefonní čísla, která jsou zpoplatněná vysokým tarifem.Toto hrozí jen u uživatelů, kteří používají pro přístup na Internet vytáčeného spojení prostřednictvím modemu. Toto připojení se v dnešní době již skoro nevyužívá a proto dialer nepředstavuje velké nebezpečí.

Prevence

Způsob obrany proti dialerům je velmi složitý a účinná ochrana ve formě počítačového programu neexistuje. Jak jsem již zmínil jsou dva typy dialerů – legální a nelegální a proto se nelze bránit prostřednictvím antivirových programů, protože by docházelo ke střetu výrobců antivirových programů a firem, které provozují placené webové stránky s vyšším tarifem. Nejúčinnější ochrana je zablokování odchozího volání se zvýšeným tarifem. Dále pak nenavštěvovat neprověřené a nedůvěryhodné stránky (př. pornografické, nabízející nelegální software, …).

Praktický příklad

V roce 2003 byla podávána velká množství reklamací na Český Telecom pro vysoké telefonní účty. Mluví se až o 2000 poškozených. K tom došlo přesměrováním vytáčeného připojení na čísla začínající 900, 906 prostřednictvím dialerů. Jedná se o skupiny telefonních čísel, které jsou určeny pro audiotextové služby. Po velkém množství reklamací Český telekomunikační úřad zakázal pro přístup na Internet používat pouze čísla ze skupiny 90x (tedy například již zmíněné 900, 906, 909). Ale to nebylo dostatečné a umožnilo to, že se dialery vrátily v roce 2004 přes předčíslí 976. [8]

Phishing

Termín vznikl spojením anglických slov *fishing* (rybaření) a *phreaking* (zneužívání telefonní sítě – termín je opět složenina ze slov *phone* a *freak*). V češtině se občas používá termín rybaření, častější je ale používání originálního termínu.

Jedná se o činnosti, které prostřednictvím podvržených zpráv od různých (nejčastěji finančních) institucí.se snaží získat citlivé údaje od obětí. Nejčastější formou je asi podvržený dopis od banky s žádostí o aktualizaci databáze čísel kreditních, časté jsou taky pokusy o získání přístupových hesel k internetovému bankovnictví. Obě zadá požadované údaje, ty se ale pak odešlou útočníkovi.

Podvodníci se snaží napodobit grafický styl zvolené instituce, často si i registrují internetové domény podobné těm originálním. Některé pokusy také dokáži zešvindlovat i zobrazenou adresu v prohlížeči a zobrazují skutečnou doménu napadané instituce.

Díky využití spammerských databází se odeslaný mail dostane na obrovské množství adres. Při odhadované úspěšnosti okolo 5 % se jedná o velice výnosný obchod, zvláště když náklady jsou velice nízké.

Celosvětově nejzneužívanější světovou službou je internetová aukční síň eBay. Pro útočníky je její zneužití snadné – uživatelé očekávají komunikaci v angličtině (není nutné vytvářet jazykové mutace) a navíc všichni její zákazníci používají platební karty. V ČR již také došlo k mnoha pokusům, byly zaměřeny hlavně na internetové bankovnictví. Banky to vedlo k lepšímu zabezpečení, dnes je tato služba většinou jištěna přes potvrzovací sms kódy, což minimalizuje možnost podobných zneužití.

Prevence

První pravidlo prevence je stejné jako u virů a dalších forem – uživatelova ostražitost. Neklikat na nic podezřelého, jakékoliv žádosti o odeslání citlivých dat raději konzultovat s helplinkou dotčené instituce apod. Dnes už navíc existují archivy těchto útoků, kam má uživatel možnost se podívat (např. http://www.antiphishing.org/phishing_archive.htm, nebo v češtině na serveru www.hoax.cz).

Pokud uživatel již data odeslal, nezbývá než zablokovat účet či kreditní kartu. Banky často pro tyto případy zřizují speciální linky.

Praktický případ

Phishing si ukážeme na příkladu, kdy se útočník zfalšovaným mailem od České spořitelny pokusil získat přístup k telefonickému bankovnictví (text mailu a obrázek jsou převzaté z phishingového archivu na serveru www.hoax.cz).

Dopis měl následující podobu:

Předmět: *Ceska sporitelna – Pozor! Nove bezpecnostni standardy*

Text mailu:

Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci.

Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku.

Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu.

S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem.

Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu.

Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.

Vy jste byl (a) zvolen (a) jako jeden z ucastniku finalniho stadia testovani systemu.

V soucasne dobe Vam navrhujeme vyuzit odkaz https://www.servis24.cz/ebanking-s24/ a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system.

V aktualnim stadiu provozu jsou mozne nektere nesrovnalosti.

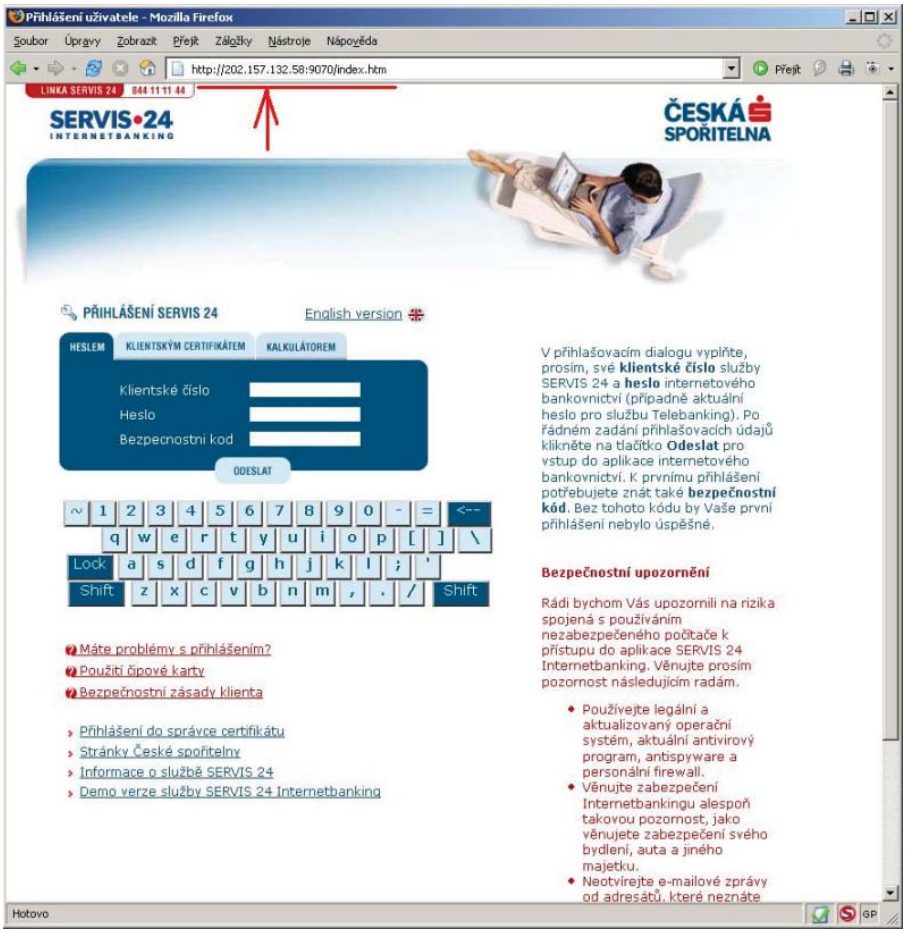
Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji.

Musime Vas informovat o bezpodminecnem pouziti noveho systemu od listopadu, v opacnem pripade budou Vase ucty zablokovany do okamziku uplne identifikace Vasi osoby. Proto doporucujeme v nejkratsi mozne dobe prejit na novy bezpecnostni standard.

S pozdravem, Oddeleni Banky pro ochranu pred frodem.

Po kliknutí na odkaz byl uživatel přesměrován na následující stránku:

Obr. 4: Phishing



Spam

Je hromadně rozesílané sdělení, většinou reklamní. Nejprve se začal objevovat ve formě emailů, ale dnes se s ním můžeme také setkat na diskusních fórech.

Prevence

Zákon upravující problematiku spamu byl vydán 7. září 2004 a tento zákon vyžaduje prokazatelný souhlas příjemce zprávy. Tento zákon byl vytvořen dle norem EU a ta definuje spam jako „*všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby*“. Dohled nad dodržování zákona spadá do kompetence Úřadu pro ochranu osobních údajů.

Vstupem ČR do EU přineslo výhodu v boji proti spamu a to v podobě možnosti postihnout odesílatele spamu i v případě, že sídlí v některé ze zemí EU. Ale je zde velký problém a to, že značná část spamů pochází z jiných částí světa a vymáhání práv je proto prakticky nemožné.

Prevence

Uživatelé se mohou chránit proti spamu hned několika způsoby:

a) neuvádět emailovou adresu na nedůvěryhodných serverech

b) mít kvalitní antivirový program, protože mnoho spamů je rozesíláno distribuovaně prostřednictvím virem infikovaných počítačů.

c) a dále různé formy filtrace přijatých zpráv

Praktický příklad

Asi největší pobouření uživatelů vyvolal hromadně rozesílaný spam společnosti Media Online, s. r. o. Tato společnost v něm seznamovala příjemce zprávy se svým webem Tvujdum.cz.. V textu emailu byl také následující text:

„Tento e-mail je Vám zasílán na základě pečlivého výběru a globální rešerše uživatelů, kteří své webové stránky věnují tématice bydlení, stavebnictví. Předem se omlouváme za nevyžádaný e-mail“.

Nejdříve se společnost, po kritice uživatelů, snažila masivní spaming obhajovat, ale později vydala společnost tiskovou zprávu, v níž se omluvila všem uživatelům. A výkonný ředitel společnosti přislíbil finanční dar nadaci Člověk v tísni v hodnotě 50 tis. Kč. Tato společnost také dostala pokutu ve výši několika desítek tisíc korun.

Hoax

Je anglické slovo pro podvod nebo žert. Jedná se o emailovou či ICQ zprávu, která varuje uživatele před virem, nebezpečím atd. Hoax obvykle obsahuje žádost o rozšíření na další uživatele a proto se někdy také označuje jako řetězový email. Škodlivost hoaxu spočívá v šíření poplašné zprávy, přetěžování serverů, nebezpečné rady, které mohou poškodit systém nebo jiné aplikace a ztráta důvěryhodnosti uživatele. Pokud lidé zprávě uvěří, může dojít k poškození dobrého jména firmy, k poklesu tržeb či i k ohrožení života (hlavně v našem druhém praktickém příkladě).

Praktické příklady

Dne 2. 4. 2004 se dostalo do 2000 výrobků Coca-Cola látka,která způsobuje bolesti hlavy,zvracení,vysušování kuže.

Jedná se o látku Hybriochalutor která se používá k dezinfekci lahví Společost Coca-Cola vydala prohlášení kde varuje lidi aby si skontrolovaly Datum výroby pokud to bude 2. 4. 2004 v 21:39–23:16 nekupujte nebo vyměnte v obchodě.

Prosíme ochrantě více lidí touto formou a rozpošlete to všem co znáte.I vy můžete pomoct.

Tato zpráva je přímo zaměřena proti společnosti Coca-cola. Jedná se o poškození dobrého jména společnosti a o šíření poplašné zprávy.

Ak sa ocitnete v situacii a musite pod natlakom vybrat peniaze z bankoveho automatu na poziadanie/prinutenie nasilnika, zadajte svoje PIN opacne:

to je od konca – ak mate napr. 1234 tak zadate 4321

automat vam peniaze stale vyda, ale tiez privola policiu ktora vam pride na pomoc tato sprava bola pred nedavnom vysielana v TV pretoze malo ludi vyuzivalo tuto skutocnost pretoze o tom nevedeli preposlite co najviac ludím. Zdroj: [10]

V tomto případě může být zpráva již přímo nebezpečná. Uvedený postup je nesmysl a bankomat peníze nevydá. Pokud bude špatný PIN zadán 3x, pak nevydá ani kartu. Chování útočníka v takovém případě nelze předvídat.

Nigerijský dopis

Tímto termínem se označují všechny možné dopisy, v kterých cizinec žádá od českých osob možnost převést větší množství peněz na jejich účty. Obvykle se jedná o miliony až desítky milionů (často v USD), přičemž odměnou je nějaké procento z této částky. Jediné co musí obě udělat je poslat nějakou řádově nižší částku na účet odesílatele, která má sloužit na administrativní vyřízení celé věci (nebo na úplatky úředníkům). Poté co obě tyto peníze pošle, přeruší odesílatel veškerou korespondenci. Tyto dopisy pocházejí obvykle z některé z afrických zemí. Často je to právě Nigérie, dále JAR, Sierra Leone, Zimbabwe atd.

Tyto dopisy mívají trojí podobu:

1. Odesílatelem je dědic po nějakém zemřelém představiteli minulého režimu, přičemž předst avitelé současného režimu nedovolí disponovat jeho prostředky.
2. Odesílatelem je bankovní úředník cizí banky, který nesmí vlastnit bankovní účty v zahraničí, a proto žádá někoho, aby mohl použít jeho účet na převedení prostředků (po nějaké mrtvé osobě). Obvykle obsahuje apel na rychlé jednání z důvodu možného propadnutí prostředků.
3. Odesílatelem je advokát, který je správcem dědictví po mrtvé osobě, která nemá žádné příbuzné v zahraničí. V dopise se tvrdí, že adresát má stejné příjmení jako zemřelá osoba a mohl by se tedy za dědice vydávat.

Dopisy byly v běžné podobě velice časté hlavně počátkem devadesátých let. Adresátem byly jak fyzické, tak právnické osoby. V dnešní době se šíří většinou již jen mailem na spamovém principu (odesílatelé čekají, že z obrovského množství odeslaných dopisů se některé ujmou). Skutečný rozsah této trestné činnosti, jako i počet obětí je velice těžké zjistit, protože postižení se obvykle stydí škodu nahlásit.

Prevence

Prevence je velice jednoduchá – neodpovídat a hlavně nikam neposílat žádné finanční prostředky.

Příklad tzv. nigerijského dopisu

Dopis je v původním anglickém jazyce k nalezení na adrese http://www.pooh.cz/pooh/a.asp?a=2004023&db=1001, přeloženo do češtiny.

Drahý pane/paní

Z důvodů, které vysvětlím později a detailněji, hledám spolehlivého partnera, který by mi asistoval při zajištění a investování sumy 25 000 000 USD (dvacet pět milionů dolarů) zděděných z obchodní rezervy mého otce.

Jsem jediné žijící dítě zesnulého pana Sekou Janeha, Liberijského obchodníka s diamanty. Můj otec zbohatl investicemi do obchodů s diamanty jak v Liberii, tak v Sierra Leone. Byl zavražděn v Monrovii (Libérii) v říjnu 2000 ozbrojenci ve službách Charlese Taylora, když byl na obchodní cestě. Před svou smrtí otec, který věděl o nebezpečí které

nám hrozí kvůli obchodům co dělal a nestabilitě regionu, uložil zmíněnou sumu u soukromé finanční a bezpečnostní firmy v Evropě. Tyto peníze jsou jediným dědictvím naší rodiny po smrti mého otce, a přesto po nás liberijská vláda a její přívrženci kvůli této finanční rezervě pátrali.

Abychom uzavřeli tuto traumatickou záležitost, rozhodli jsme se s matkou nabídnout 20 % této částky, nebo 25% podíl v možné investici každému, kdo nám pomůže peníze zajistit.

Pokud budete mít zájem postupovat za těchto podmínek, prosím pošlete si pro detailnější informace. Pokud tuto nabídku neakceptujete, zachovejte prosím nejvyšší utajení. Rychlou odpověď s vaším telefonem a faxem pro důvěrnější komunikaci velmi oceníme.

Upřímně váš,

Andrew Janeh

Při psaní práce jsme narazili na celou řadu těchto dopisů. Obvykle jsou psány v anglickém jazyce, s velmi nízkou úrovní jazyka a velkým počtem gramatických chyb.

Zdroj mailu: [12]

Zneužití osobních dat

Spočívá v získání a zneužití různých osobních dat oběti. Do této problematiky bychom mohli zařadit i phishing, jedná se ale o tak rozšířený a významný fenomén, že ho uvádíme samostatně.

Získávat osobní data lze několika způsoby. Jednak můžou útočníci použít podobné techniky jako u phishingu, jednak mohou opět využít škodlivý software. Často se jedná o tzv. keyloggery, které zaznamenávají každý stisk klávesy a v pravidelných intervalech jejich seznam odesílají.

Citlivými daty jsou v tomto případě hlavně čísla kreditních karet, ale může se jednat o rodná čísla, hesla k internetovému bankovnictví, přístupová hesla k serverům apod.

Prevence

Prevence je velice obtížná. Keyloggery se dovedou velice dobře v systému maskovat a nezkušený uživatel je nemá šanci odhalit. Hlavní díl prevence tedy spočívá na antivirových programech, které musí účinně zabránit zanesení a spuštění keyloggerů. Někteří také používají různé techniky na jejich zmatení, například vkládání části textu hesel myší přes schránku.

Hacking

Hackeři je skupina lidí, která proniká do počítačových systémů prostřednictvím svých znalostí nebo pomocí vytvořených speciálních aplikací a získává ze systémů údaje nebo zde páchá četné škody. Hackery bychom rozdělili na dvě skupiny. První skupina hackerů se „prolamuje“ do systémů za účelem získání slávy mezi hackerskou komunitou, ale také se

snaží upozornit na chyby v systémech. Druhou skupinu bych označil jako škodlivou a nebezpečnou. Tito hackeři se „prolamují“ do systémů za účelem průmyslové špionáže a páchají mnohamiliardové škody.

Prevence

Obrana proti hackerům je velkým problémem. Hackeři jsou velmi chytří a sami si tvoří programy, kterými se pak velmi snadno „nabourají“ do vašeho pc.

Základní možnosti obrany:

1. kvalitní firewall (= program, který skenuje příchozí a odchozí spojení)
2. hesla neukládat v počítači (např. do textových souborů)
3. volit složitější hesla včetně čísel, velká písmena a dostatečně dlouhá
4. nestahovat data z nedůvěryhodných zdrojů

Praktický příklad

Za celosvětově nejznámějšího hackera je považován Kevin Mitnick. Počítači se začal zabývat na střední škole a zde již začal s neoprávněným průnikem do systémů a získávání hesel. Vše to považoval za zábavu a v oblasti hackingu se začal zdokonalovat. Za svůj život byl několikrát chycen a potrestán. V posledním procesu byl Kevin Mitnick obviněn z napáchání škody 300 mil. dolarů, ale nikdy mu nebylo prokázáno obohacení. Celý proces byl velmi silně medializovaný. Mitnick byl v médiích označován jako „nebezpečný společnosti, je-li vybaven klávesnicí“. Dalším přitěžující okolností bylo, že v době soudního procesu s Mitnickem se začalo obchodovat prostřednictvím internetu a vláda Spojených států chtěla získat určitou kontrolu nad internetem. Úřady, v boji proti hackerům, hledaly „obětního beránka“, který by zastrašil ostatní hackery a tím beránkem se stal právě Kevin Mitnick. Tyto faktory sehrály klíčovou roli ve stanovení tvrdého trestu. V tomto procesu byl odsouzen k pěti letům vězení a celé 3 roky po propuštění měl zákaz použití počítačů a mobilních telefonů. Přitom Kevin Mitnick nepatří mezi nebezpečné hackery. Nikdy nepronikal do systémů za účelem obohacení či páchání škod, ale pouze zde získával zdrojové kódy, aby je mohl prostudovat (tzv. pro vlastní potřebu).

V současnosti Kevin Mitnick pracuje pro společnost Defensive Thinking, která provádí bezpečnostní školení pro firmy a také soudní expertízu po hackerském útoku.

Kopírování programů

Kopírování programů také bývá označováno jako počítačové pirátství, nebo softwarové pirátství. Jedná se o užití softwarového produktu bez splnění podmínek stanovených výrobcem software (obvykle tedy bez zaplacení).

Celosvětová míra softwarového pirátství se odhaduje na 35 procent. V České republice je to dokonce 41 procent. Co se týče finančních ztrát, tak se jedná o 34,3 mld. USD (v ČR 132 mil. USD). Tato čísla jsme převzali z výroční zprávy organizací BSA a IDC (*Třetí výroční zpráva organizací BSA a IDC o globálním softwarovém pirátství*). Organizace ale vychází z podle nás mylného předpokladu, že každou zkopírovanou kopii software by si jinak její neoprávněný uživatel zakoupil.

Míra pirátství se obvykle odvíjí od vyspělosti ekonomiky dané země. Zemím z vrcholu tabulky se někdy s nadsázkou říká „single copy countries“, tedy země, kde k tomu, aby software všichni používali, stačí jediná legální kopie.

Tab. č. 1: Míra pirátství

Země	Míra pirátství
Vietnam	90 %
Zimbabwe	90 %
Indonésie	87 %
Čína	86 %
Pákistán	86%
…	
Dánsko	27 %
Finsko	26 %
Rakousko	26 %
Nový Zéland	23 %
USA	21 %

Formy softwarového pirátství

1. **Pirátství koncových uživatelů** (End User Piracy). Asi nejrozšířenější forma pirátství. Zahrnuje všechny možnosti kopírování, které činí koncoví uživatelé, tedy vícenásobné používání jedné kopie, půjčování si CD s programy, provozování distribučních fór apod.
2. **Pirátství prodejců** (Reseller Piracy). Forma, kdy prodejce dodává počítač s již přeinstalovaným nelegálním systémem. Nevadí, zda o tom zákazník ví či ne. Pokud o tom neví, dopouští se prodejce navíc ještě podvodu.
3. **Pirátství na internetu**. Někdy se také označuje jako BBS Piracy (označení pro diskusní fóra). Zahrnuje všechny formy přesunu zkopírovaných programů po internetu.
4. **Pirátství podniků** (Corporate Piracy). Kopírování programů umístěných na lokální sítě zaměstnanci. Podniky si často na lokální sítě kvůli usnadnění instalací ukládají kompletní instalační balíčky (často včetně sériových čísel)., pro zaměstnance je pak velice snadné si pro osobní potřebu nějaký software zkopírovat.
5. **Poškození nebo narušení obchodního jména nebo obchodní známky**. Tohoto přečinu se dopouští ten, kdo o sobě neoprávněně prohlašuje, že je autorizovaným prodejcem či servismanem určitého softwarového řešení. K poškození dobrého jména často souvisí s nízkou kvalitou takto poskytovaných služeb.
6. **Porušení patentových a autorských práv**. Zahrnuje porušování těchto práv mezi prodejci navzájem. Časté jsou také spory mezi výrobci komerčního software a programátory svobodného software (viz například spory mezi Microsoftem a firmami okolo svobodného operačního systému Linux.).
7. **Průmyslové pirátství.** Distribuce nelegálních kopií ve velkém. Prodejci často tisknou falešné certifikáty pravosti, instalační příručky apod. Před několika lety mohli tito prodejci inzerovat i v tisku apod., dnes je tato forma poměrně silně potlačovaná.

Zdroj: [13]

Důsledky nelegálního užívání programů:

Nejvýznamnější jsou asi ekonomické důsledky. Kopírování má vliv nejen na jednotlivé softwarové společnosti (jejich ztráta byla,jak už bylo zmíněno, 35 mld. USD), ale i na ekonomiku jako celek. Odhaduje se, že 1 USD utracený za software ještě vygeneruje 1,25 USD na doprovodných službách (prodej, instalace..). Škody tedy nevznikají jenom softwarových společnostem, ale i jejich partnerům. Navíc je třeba vzít do úvahy i daňové škody a potenciální dopad na zaměstnanost. Pirátstvím trpí celá ekonomika.

Dalším často zmiňovaným dopadem je dopad na chování lidí. Souvisí to s tím, že pokud člověk pravidelně krade software, nemá daleko ke krádežím jiného druhu. Na tento jev je ale podle našeho názoru nutno nahlížet poněkud s odstupem.

Může mít kopírování nějaké pozitivní důsledky? Nepochybně má pozitivní dopad na počítačovou gramotnost – uživatel se učí používat i programy, za které nezaplatil. Pro výrobce software má kopírování také jeden pozitivní dopad – každý pirát je potenciální kupující. Některé firmy otevřeně přiznávají, že je lepší, pokud si uživatelé nelegálně zkopírují jejich software, než software konkurence.

Kopírování audiovizuálních děl a textů

Tento druh činnosti je dnes velice rozšířenou, a také diskutovanou oblastí počítačové kriminality. S nárůstem dostupnosti rychlého internetu její objem stále narůstá a způsobuje tak velké ztráty majitelům autorských práv.

Typy tohoto pirátství (dle serveru www.filmynejsouzadarmo.cz, dá se ale vstáhnout i na hudbu a texty):

- **Výrobkové pirátství:** Rozšiřování nelegálních kopií autorsky chráněných děl. Postihuje se i nekomerční rozšiřování těchto kopií.
- **Internetové pirátství:** Poskytování chráněných děl ke stažení v síti internet. Postihováno je opět i nekomerční sdílení.
- **Nekalé pomůcky:** Zařízení nebo programové vybavení, které umožňuje vyřadit z činnosti nebo obejít ochranu proti kopírování.
- **Neoprávněné veřejné projekce:** Promítání bez souhlasu majitele práv.
- **Krádeže televizního signálu:** Zahrnuje neoprávněný přenos chráněného obsahu přes TV či rádio, vysílání ve veřejných prostorách či neoprávněný příjem chráněného vysílání.

O rozšířenosti tohoto typu kriminality nejlépe vypovídá tento údaj: na jedno legálně prodané CD u nás připadá více než jedno nelegálně vypálené. Celkem se tak jedná o ztrátu ze zhruba čtyř mil. nosičů ročně, v Kč se jedná o stovky milionů. V oblasti filmů se ztráty odhadují na 600 mil. Kč ročně.

Ochrana těchto práv se v poslední době začíná (podobně jako u software) silně rozmáhat. Děje se tak jednak formou mediálních kampaní (např. *„Kopírování zabíjí hudbu“*, nebo *„Filmy nejsou zadarmo“*), ale také zvýšenou aktivitou v oblasti postihu. Organizace na ochranu autorských práv si najímají firmy specializované na vyhledávání nelegálních kopií a na identifikaci pachatelů. Policii pak předají důkazní materiál, ve kterém jsou podrobně zachycena nelegálně distribuovaná data (názvy a další údaje), IP adresy ze kterých bylo nabízeno atd. Posunuje se také zaměření na pachatele. Dříve se postihovaly jen lidé provozující pirátství tzv. průmyslovým způsobem, tedy za úplatu a ve velkém množství. Dnes se začínají postihovat i běžní domácí uživatelé (např. vlastností dnes často používané

výměnné sítě typu torrent je, že uživatel zároveň s downloadem dat tato data nabízí i ostatním, a tak porušuje zákon).

Uživatel, který tato data jen stahuje, zatím podle českého právního řádu není postižitelný – na rozdíl od software – , i když výklady se liší (např. zástupci organizací jako OSA apod. tvrdí, že protizákonné je i samotné stahování).

Podle našeho názoru je vysoká míra pirátství v této oblasti daná z velké části i samotným způsobem distribuce hudby. CD a zvláště DVD jsou většinou extrémně předražená, přičemž autor z této částky uvidí jen malé procento. Pokud si uživatel chce film či album stáhnout z internetu a ušetřit, tak zase naráží na problém DRM (Digital rights management – ochrana práv u digitálních dat), který mu zásadním způsobem brání ve volném užití tohoto díla. DRM je například velkým problémem nového českého portálu na prodej hudby ilegalne.cz. Kódované písně jsou přehrát jen na jednom určitém počítači, v jednom operačním systému (Windows) s jedním programem pro přehrávání hudby (Windows Media player). Uživatelé, kteří používají Linux, Macintosh, nebo si jen chtějí hudbu poslechnout v levných MP3 přehrávačích (těch je hodně), mají smůlu. Pokud DRM z nahrávky odstraníte, dopouštíte se trestného činu (viz *Nekalé pomůcky*).

Zvláště zahraniční praxe ukazuje, že míra pirátství výrazně klesá, pokud se hudba prodaná po internetu distribuuje bez DRM, a také pokud je jasné, že významné procento z částky putuje k autorovi (lidé mu za dobrou hudbu rádi přispějí).

Závěr

Ve škodlivých činnostech prováděných počítači je zřetelný jasný posun. Od původně destruktivních pokusů jednotlivců se v dnešní době setkáváme s organizovanou činností skupin, zaměřenou hlavně na získávání peněz. Tato činnosti se také výrazně internacionalizuje, hlavně co se týče spamu a podvodů s kreditními kartami.

Posun můžeme také pozorovat v samotných škodlivých kódech. Viry nebo červi bývají spojeny s trojany, keyloggery či backdoory. Není tedy jednoduché je jednoznačně zařadit. Škodlivý kód už na sebe také jako dříve neupozorňuje, ale snaží se zůstat pokud možno v utajení.

Změnily se i typ škody. Dříve bylo újmy dosaženo hlavně zahlcením sítě, či ztrátou produktivity způsobenou výpadkem výpočetní techniky. Dnes je to přímo přesun peněz od oběti k útočníkovi. Z toho důvodu se dnes útoky zaměřují již převážně na domácnosti (přes 80 %).

Újma je dnes způsobena i uživatelům, kteří napadeni vůbec nebyli. Různorodost a vynalézavost škodlivých kódů si žádá i dokonalejší ochranné prostředky. Ty jsou jednak finančně náročnější, ale jsou náročnější i na systémové prostředky počítače nebo sítě, což se odrazí v produktivitě práce.

V budoucnu lze očekávat další integraci škodlivých kódů. Pravděpodobně se budou rozvíjet i jejich polymorfní schopnosti a jiné techniky ke ztížení odhalitelnosti. S tím bude spojena nutnost využívat masivně heuristickou analýzu, což ještě více zatíží chráněné systémy.

Stejně jako v úvodu můžeme konstatovat, že hlavní díl prevence spočívá na uživateli. Na závěr bychom potom rádi uvedli seznam deseti nebezpečných činností, které provádějí uživatelé, a které vedou k infiltraci nebezpečnými kódy. Seznam je k nalezení na serveru Interval (http://www.lupa.cz/clanky/predstavuje-internet-nebezpecne-prostredi)

10 nebezpečných činností, které provádějí uživatelé

1. Kliknutí na neznámou přílohu e-mailu
2. Instalace neautorizované aplikace
3. Vypnutí anebo vyřazení automatických bezpečnostních nástrojů
4. Otevírání zpráv neznámého původu
5. Brouzdání po stránkách, kde existují rizika
6. Sdělení svého hesla
7. Náhodné brouzdání neznámem
8. Připojení se do neznámé bezdrátové sítě
9. Vyplnění webových formulářů, resp. registrací
10. Účast v chatech

Literatura

[1] PORADA, V.: *Kriminalistika.* Brno: CERM, 2001.

[2] HÁK, Igor: Exkurze do světa virů, červů a jiné havěti [online]. [cit. 2004-10-26]. Dostupný z www: <http://www.zive.cz/h/Viryabezpecnost/AR.asp?ARI=119420>.

[3] KUNEŠ, Jan: Největší škoda od viru? Prý 8,75 miliard USD [online]. [cit. 2004-05-27]. Dostupný z www: <http://www.zive.cz/h/Bleskovky/AR.asp?ARI=116643>.

[4] KULHAVÝ Petr: Kevin Mitnick [online]. [cit. 2003-09-26]. Dostupný z www: <http://www.root.cz/clanky/kevin-mitnick-podvodnik-hacker/>.

[5] Wikipedia, the free encyclopedia**:** <http://en.wikipedia.org>.

[6] Technet.cz: Červ WIN32/Blaster vypíná počítače a chystá se zaútočit na Microsoft [online]. [cit. 2003-08-13]. Dostupný z www: <http://technet.idnes.cz/tec_technika.asp?r=bezpecnost&c=A030812_5231285_bezpecnost>.

[7] Computerworld: Gozi Trojan leads to Russian data hord [online]. [cit. 2007-03-20]. Dostupný z www: <http://www.actinet.cz/bezpecnost_informacnich_technologii/j1/l33/no3084/Trojsky_kun_Gozi.html>.

[8] LÉR Martin: Dohoda o kontrole dealerů [online]. [cit. 2005-02-24]. Dostupný z www: <http://www.lupa.cz/clanky/dohoda-o-kontrole-dialeru-dosazena/>.

[9] Nápravník Jiří: Přemrštěné účty za telefon… Odzvoněno? [online]. [cit. 2005-02-24]. Dostupný z www: <http://www.mesec.cz/clanky/premrstene-ucty-za-telefon-odzvoneno/>.

[10] HOAX | podvodné a řetězové e-maily, poplašné zprávy, phising, scam [online]. [cit. 2007-04-12]. Dostupný z www: <http://www.hoax.cz/>.

[11] Igiho stránka o virech [online]. [cit. 2007-06-21]. Dostupný z www: <http://www.viry.cz>.

[12] DOČEKAL, Daniel: Podvodné maily : ANDREW JANEH [online] [cit. 2007-03-20] Dostupný z www: <http://www.pooh.cz/pooh/a.asp?a=2004023&db=1001>.

[13] KREMEROVÁ, Pavla: Softwarové pirátství stokrát jinak [online]. [cit. 2007-04-20] Dostupný z www: <http://www.zive.cz/h/Uzivatel/AR.asp?ARI=3663>.

[14] Čeští piráti nejvíce kopírují hudbu než software [online]. [cit. 2007-04-20] Dostupný z www: < http://www.mpx.cz/ZAJIMAVOSTI/Cesti-pirati-nejvice-kopiruji-hudbu-nez-software.html>.

[14] NYKODÝMOVÁ, Helena: Představuje internet nebezpečné prostředí? [online]. [cit. 2007-04-20] Dostupný z www: < http://www.lupa.cz/clanky/predstavuje-internet-nebezpecne-prostredi>.

[15] BSA – Business Software Alliance [online]. [cit. 2007-04-03]. Dostupný z www: <http://www.bsa.cz>.

[16] Filmy nejsou zadarmo, informace o kampani Filmynejsouzadarmo, novinky [online]. [cit. 2007-04-05]. Dostupný z www: <www.filmynejsouzadarmo>