Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Veronika Paukertová

Elektronická informační kriminalita

Diplomová práce

Praha 2006

Vedoucí diplomové práce: PhDr. Richard Papík, PhD.

Oponent diplomové práce: Ing. Martin Sonnek

Datum obhajoby: 26. 5. 2006

Hodnocení: výborně (1)

Vysoká škola: Univerzita Karlova v Praze Fakulta: Filozofická fakulta

Součást: Ústav informačních studií a knihovnictví Školní rok: 2004/2005

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

pro Veronika Paukertová

obor Informační studia a knihovnictví

Název tématu: Elektronická informační kriminalita

Zásady pro vypracování:

Cílem práce je analyzovat vztah informační společnosti a informačních systémů k současnému fenoménu elektronická informační kriminalita.

Práce bude připravena podle následujících bodů:

1. Úvod do problematiky elektronické informační kriminality (historie a současnost, klasifikace a kategorizace-trestné činy, motivace a cíle pachatelů)
2. Zásady informační bezpečnosti(důvěrnost-integrita-dostupnost, informační bezpečnostní politika, bezpečnostní směrnice a standardy)
3. Informační kriminalita (porušování autorského práva – softwarové piráctví, poškození a zneužití záznamu na nosiči informací, další typy)
4. Opatření proti informační a počítačové kriminalitě (legislativní opatření, organizační opatřenít, technická opatření)
5. Srovnání českého a zahraničního prostředí
6. Informační a počítačová kriminalita z pohledu informační společnosti

Rozsah grafických prací:

Rozsah průvodní zprávy:

Seznam odborné literatury:

1. SMEJKAL, Vladimír. *Informační a počítačová kriminalita v České republice* [online]. [Cit. 2005-04-19]. Dostupný z WWW: <http://www.mvcr.cz/casopisy/studie/diskuse/analyza.html>
2. SMEJKAL, V.;SOKOL, T.; VLČEK, M. *Počítačové právo*. Praha : C.H. Beck, 1995. 220 s. ISBN 80-7179-009-5
3. BRYANT, John. *Information Crime* [online]. [Cit. 2004-12-05]. Dostupný z WWW: <http://www.thebirdman.org/Index/Intro/Intro-InfoCrime.html>

Vedoucí diplomové práce: PhDr. Richard Papík, Ph.D.

Datum zadání diplomové práce: 19.4.2005

Termín odevzdání diplomové práce:

L.S.

PhDr. Richard Papík, Ph.D.

Vedoucí součásti-ředitel ÚISK FF UK

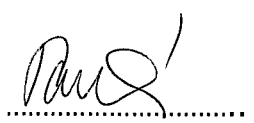
Děkan FF UK

V Praze dne 19.4.2005

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a že jsem uvedla všechny použité informační zdroje.

V Praze, 16. dubna 2006



podpis diplomanta

Identifikační záznam

PAUKERTOVÁ, Veronika. *Elektronická informační kriminalita [Electronic information crime]*. Praha, 2006. 114 s., 6 s. příl. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví 2006. Vedoucí diplomové práce PhDr. Richard Papík, PhD.

Abstrakt

Tématem diplomové práce je elektronická informační kriminalita (EIK) - fenomén dnešní doby. Cílem textu je popis a analýza daných jevů, patřičných technologických, legislativních a organizačních opatření.

Úvodní kapitola podává poměrně obsáhlé informace o historickém vývoji, konceptualizaci a pachatelích EIK. Dále je rozebírána tematika informační bezpečnosti, která je s touto problematikou velmi úzce spjata. V rámci EIK jsou delikty rozděleny na porušování autorských práv, útoky na data a internetové obtěžování a podvody. Práce se dále věnuje porovnání českého a zahraničního prostředí. Problematika je zakončena pohledem informační společnosti na daný jev a krátkým zamyšlením nad vizí EIK.

Klíčová slova

autorská práva, crackeři, e-mail, hackeři, hacking, informační bezpečnost, informační kriminalita, informační společnost, internet, legislativní opatření, malware, P2P, pirátství, počítačová kriminalita, technologická opatření, WWW, warez

Obsah

Seznam použitých zkratek

AP	autorské právo
AutZ	autorský zákon
AVD	audiovizuální díla
BBS	Bulletin Board System
EIK	elektronická informační kriminalita
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HW	hardware
IB	informační bezpečnost
IBP	informační bezpečnostní politika
ICT	informační a telekomunikační technologie
IE	Internet Explorer
IFPI	International Federation of Phonographic Industry
IRC	Internet Relay Chat
IS	informační systém
IT	informační technologie
MPAA	Motion Picture Association of America
MS	Microsoft
NSA	National Security Agency
OS	operační systém
RIAA	Recording Insdustry Association of America
SW	software
TrZ	trestní zákon
WWW	World Wide Web

Předmluva

Práce se věnuje problematice elektronické informační kriminality (dále EIK), která se bohužel stává běžnou součástí života uživatele ICT. Jde o jev, jehož příchod musel díky neudržitelné informatizaci a zároveň určitým životním postojům společnosti nevyhnutelně přijít. Tento fenomén dnešní doby pokrývá poměrně širokou oblast a troufám si tvrdit, že každá z popisovaných kapitol by vydala na samostatnou práci. Cílem této přehledové práce je seznámit čtenáře s tajemstvími, která v sobě tento jev skrývá.

Téma EIK jsem si vybrala z prostého důvodu - jde o aktuální problematiku, která má spád; téměř každý den se objeví nové hrozby, které ohrožují nás uživatele i celou informační společnost. Asi každý si v souvislosti s pojmem EIK vytvoří určitou představu - vybaví se mu některé medializované případy internetových bankovních podvodů, přeplněná e-mailová schránka či zavirovaný počítač. Takovými a mnoha dalšími případy se zabývám v této práci. Problematiku jsem již zpracovala v roce 2005 ve formě studijně rozborové práce a bibliografické rešerše. Mojí další motivací pro výběr tématu byl fakt, že šlo o dosud nezpracovanou problematiku na Ústavu informačních studií a knihovnictví.

Práce je rozdělena do šesti kapitol. Úvodní kapitola se věnuje seznámení se základními pojmy, které se týkají zločinu v kybernetickém světě. Zmiňuji zde historické mezníky elektronické informační kriminality, trestné činy a jejich pachatele.

Druhá kapitola se věnuje zásadám informační bezpečnosti, jejichž dodržování je nezbytné jak pro instituce, tak pro jednotlivce. V této kapitole uvádím též nezbytné kroky k vytvoření informační bezpečnostní politiky a potřebné standardy.

Třetí stěžejní kapitola popisuje typy a metody páchání elektronických informačních trestných činů. Dále jsou zde zmíněny problémy vznikající při odhalování EIK. Kapitolu jsem rozdělila na oblast porušování autorských práv, útoků na data a oblast internetového obtěžování a podvodů. K jednotlivým trestným činů je v případě existence uváděna trestněprávní úprava.

Čtvrtá kapitola charakterizuje situaci elektronické informační kriminality v České republice a vybraných zahraničních zemích. Uvádím legislativní opatření, zajímavé případy a institucionální zajištění prevence či represe EIK. Není opomíjena ani zahraniční spolupráce, která je v této oblasti nezbytná.

Pátá kapitola analyzuje EIK z pohledu informační společnosti. Zamýšlí se nad možnými příčinami, které vedou společnost k páchání trestných činů v kyberprostoru.

Dále jsou zde uvedeny současné technologické hrozby v podobě tzv. HypeCycle diagramu a prognóza letošních informačních hrozeb.

V šesté kapitole je formulován stručný závěr věnující se rekapitulaci problematiky s doporučeními, která by mohla vést k redukci kybernetických hrozeb. Tato závěrečná kapitola se také krátce zamýšlí nad vizí EIK.

Vzhledem k dynamickému vývoji této oblasti pochází většina použité literatury z internetových zdrojů (články, sborníky, webové stránky, rozhlasové příspěvky). České knižní publikace zabývající se tématem EIK v porovnání se světem poněkud zaostávají; např. v USA je za letošní a loňský rok v katalogu *Library of Congress* evidováno již osm publikací.

Chtěla bych poděkovat vedoucímu mé diplomové práce PhDr. Richardovi Papíkovi, PhD. za všechny cenné připomínky a rady při psaní diplomové práce.

1 Úvod do problematiky elektronické informační kriminality

Informační a komunikační technologie (dále ICT) jsou nasazeny snad do všech oblastí společenského a soukromého života – ekonomika, veřejná správa, armáda, průmysl, zdravotnictví, vzdělání atd. Informace, které se týkají těchto a dalších oblastí jsou implementovány do informačních systémů (dále IS). Jde o informace, které jsou pro jednotlivé subjekty hodnotou, a ne ledajakou - často jde o velmi citlivé údaje, obchodní informace atd. Následky zcizení nebo ztráty těchto dat jsou nedozírné a mnohdy jen těžko vyčíslitelné. EIK se však dotýká velmi významným způsobem i jednotlivce. Ukradená data, ať už méně či více sofistikovaným způsobem, jsou dále využívána k podvodným transakcím (e-commerce, e-banking), internetovému obtěžování atd. A nejde jen o útoky na data, jde také o velmi významnou oblast ochrany autorských práv, která jsou v prostředí internetu masivně porušována.

V následujících kapitolách jsou vymezeny základní pojmy, popsáni pachatelé trestných činů, jejich motivace a cíle. Kapitola také obsahuje historický exkurz do světa elektronické informační kriminality.

1.1 Terminologie

V českém prostředí se nejčastěji setkáváme s termínem **počítačová kriminalita**, kterou můžeme chápat jako páchání trestné činnosti, v níž figuruje počítač jako souhrn technického a programového vybavení včetně dat, či pouze některá z komponent počítače, případně více počítačů propojených do počítačové sítě. Počítač může být jak **předmětem** (majetková a informační kriminalita), tak **nástrojem** trestné činnosti (hospodářská kriminalita).

Vzhledem k tomu, že delikty v této oblasti jsou páchány s využitím moderních IT se již delší dobu hovoří o **kriminalitě informační** či **informatické**. SMEJKAL [122] ji definuje jako kriminalitu, která by mohla zahrnovat trestněprávní, autorskoprávní a občanskoprávní (osobnostní) aspekty, prováděné veškerými technologiemi pro zpracování a přenos informací. U informační kriminality jsou prostředkem nebo cílem informace, bez ohledu na způsob zpracování a použití. Informatická kriminalita je širší variantou kriminality počítačové – nástrojem nebo cílem zločinného útoku jsou informační systémy a jejich komponenty (počítače, software, data, telekomunikace). Výše jmenované pojmy pozvolna nahrazují původní termín kriminalita počítačová.

V zahraničí jsou ustáleny termíny **computer crime, high-tech crime** či **cybercrime**[1], tedy doslovně kriminalita kybernetická. Rada Evropy zavedla pojem „**computer related crime**", který definuje jako nelegální a nemorální jednání zahrnující užití nebo změnu dat získaných prostřednictvím výpočetní techniky.

Pro účely zpracování této aktuální problematiky je zde používán složený termín – **elektronická informační kriminalita** – pro zdůraznění páchání trestné činnosti v oblasti elektronických informací a to zejména prostředí v internetu, coby druhu kyberprostoru[2]. V počítačových sítích, ať už privátního, firemního či celosvětového rázu, se vyskytuje nepřeberné množství důležitých informací, citlivých údajů (přihlašovací údaje, e-mail), utajovaných skutečností (firemní údaje, různé databáze, know-how) či zdrojů zábavy (hudba, video, hry), které jsou v ohrožení před čím dál sofistikovanějšími útoky. Tato data v digitální podobě jsou v podstatě duševním vlastnictvím, na které se vztahuje právní ochrana, a jejich poškozování a zneužívání vede k rozporu se zákonem a tudíž vzniku elektronické informační kriminality.

Elektronická informační kriminalita je alarmujícím fenoménem dnešní doby, a to díky stále se rozšiřujícímu zavádění IT do všech oblastí našeho života. Aniž bychom ji museli dlouze analyzovat, můžeme po krátkém zamyšlení konstatovat, že jde o určitou modifikaci standardních trestných činů. K tomu ovšem musíme dodat, že má řadu výrazných charakteristik, které ji od kriminality klasické odlišují (absence násilí, zbrání či fyzické újmy na zdraví). U klasické kriminality se měří doba spáchání trestného činu na minuty, hodiny, dny, kdežto trestný čin v kyberprostoru kriminality může být spáchán v několika tisícinách sekundy a pachatel ani nemusí být přímo na místě činu. Další významnou charakteristikou jsou poměrně značné ztráty, ať již přímo v podobě finančních částek, nebo v podobě zneužití získaných údajů. EIK také provází určitá diskrétnost trestné činnosti. Z uvedeného vyplývá, proč bývá tato kriminalita pro svou povahu označována jako kriminalita "bílých límečků". [73]

1.2 Historie a současnost

S trochou nadsázky můžeme prvopočátky „počítačového „ zločinu datovat k začátku 19. století (tedy 150 let před vynalezením prvního skutečného počítače), kdy došlo k sériím sabotáží automatizovaného tkalcovského stavu. [85]

---

1 Podle manuálu OSN „United Nations Manual on Prevention and Control of Computer-Related Crime" sem řadíme podvod, padělání, sabotáž počítačů, neoprávněný přístup k počítačovým programům a jejich neoprávněné kopírování.

2 Prostředí mezinárodních počítačových a telekomunikačních sítí, podle Johna Barlowa, zakladatele Nadace elektronické hranice.

Vznik EIK vyplývá z historického vývoje výpočetní techniky, resp. ICT. Odrazovým můstkem se stalo masové využívání osobních počítačů a jejich propojování do sítí, především internetu. Jeho existence znamená zásadní zlom nejen do kvality, ale bohužel i do kvantity zločinů týkající se EIK.

Vývoj v **České republice** je poněkud odlišný, díky opožděnému zavedení IT. K prvním trestným činům v této oblasti dochází až na konci 80. let, kdy se v tehdejších československých domácnostech začaly objevovat první počítače.

V následujících subkapitolách jsou stručně nastíněna jednotlivá vývojová období spolu s významnými případy či osobnostmi.

1.2.1 1878 – 1969

Již dva roky po vynálezu telefonu A. G. Bellem se pokusila skupina mladíků, která obsluhovala newyorkskou telefonní ústřednu, přerušovat a nesprávně přepojovat telefonní hovory.

První sálový počítač - ENIAC byl sestrojen roku 1946 na pensylvánské univerzitě. Na přelomu 50. a 60. let byly tyto počítače využívány v mnoha společnostech a univerzitách. Údržba těchto strojů byla velmi finančně a časově náročně. Docházelo tedy k zásahům do programů, tzv. „**hacks**", které měly zefektivnit chod operačního systému (dále OS) či aplikací.

První generací hackerů (více v kapitole 1.4.1) byla v 60. letech identifikována skupina studentů MIT[3], která měla přístup k univerzitním sálovým počítačům. Mezi význačné osobnosti tohoto období patří Richard Stallman, zakladatel *Free Software Foundation*[4].

1.2.2 70. léta

V 70. letech se zrodilo opravdové zneužívání telefonních linek. Touto činností se zabývají tzv. **phreakers**, český překlad telefandové (více v kap. 3.2.3)

Roku 1971 počítačový nadšenec **John Draper** (dříve známý pod jménem Captain Crunch) objevil, že plastová píšťalka dodávaná k populárním cereáliím vydává zvuk na frekvenci 2600Hz. Tento kód způsobil odblokování telefonní sítě AT&T a umožňoval hovory zdarma. (Dnes se „Captain Crunch" staví na druhou stranu barikády, roku 2002 vyvinul specializovaný počítač *CrunchBOX*, který má ochránit uživatelská data i celou síť).

---

3 Massachusetts Institute of Technology.

4 Nadace pro svobodný software založená roku 1985, jejím cílem bylo vytvořit systém podobný Unixu, tzv. GNU - nadace se stará o právní a organizační stránky projektu GNU a o rozšiřování povědomí o svobodném software.

Roku 1975 dva členové *Homebrew Computer Club of California* začali vyrábět tzv. „**blue boxes**", zařízení založené na Draperově objevu. Šlo o osobnosti S. Wozniaka a S. Jobse, kteří v roce 1977 založili firmu *Apple Computers*.

Další významnou osobností této subkultury je **Abbie Hoffman**, zakladatel *Youth International Party*, který k obelstění telefonní komunikace používal různé způsoby a techniky, které následně publikoval v newsletteru *Youth International Party Line*.

Na konci 70. let došlo k důležité události, a to sestrojení první **BBS**[5], díky němuž se uživatelé vybavení počítačem s telefonní linkou mohou stát součástí kyberprostoru. K rozšíření těchto technologií došlo až s představením osobních počítačů firmou IBM, které s sebou přinesly jednoduchý operační systém (dále OS), binární kompatibilitu programů a hlavně masovou výměnu dat a programů mezi uživateli.

V **České republice** se objevují ojediněle trestné činy v podobě sabotáží podnikových záznamů či technického vybavení.

1.2.3 80. léta

V tomto období došlo díky IBM PC k propojení počítače a telefonní linky. Počítače byly čím dál více propojovány do sítí a tak došlo k rozšíření předchůdce dnešního internetu v podobě systému **BBS**. Jednalo se většinou o servery s textovým rozhraním, na které se připojovalo přímo volbou čísla, zprostředkování přístupu pomocí ISP[6] přišlo až později. [85] Z tohoto undergroundu vzešla hackerská legenda *„Legion of Doom"*[7]. Legie hrůzy, jak zní český překlad, nebyla nikdy organizovaným společenstvím osob, neměla stálé členy, hierarchii ani nic podobného. Jejich nepostradatelnou činností bylo publikování článků v různých undergroundových médiích. Nejznámějším časopisem se stal *Phrack* (http://www.phrack.org), který byl trnem v oku státním orgánům. Ke konci 80. let došlo k enormnímu rozšíření hackerských skupin. Dokladem může být seznam hackerských skupin z roku 1988, který je uveden v příloze č. 1.

S rokem 1982 přichází na svět nové médium pro záznam digitálních dat **CD-ROM** s kapacitou 650 MB, což umožnilo kvalitativně zvýšit pirátské aktivity. K rozvoji dochází v polovině 90. let, kdy se na trhu objevila vypalovací mechanika CD-R.

---

5 Bulletin Board System.

6 Internet Service Provider.

7 Parodické označení inspirované seriálem Superman.

Roku 1983 došlo k prvnímu zatčení hackerů. FBI zatkla mladíky známé jako **„414 Group"**, kteří byli obviněni z více jak 60 nezákonných proniknutí do počítačových sítí, včetně výzkumného střediska v Los Alamos.

Pat Riddle byl prvním hackerem zažalovaným v USA. Několikrát napadl počítačovou síť Ministerstva obrany a kradl počítačové vybavení.

V roce 1984 začal Eric Corley publikovat dosud vycházející časopis **2600: The Hacker Quarterly**, který se stal předním zdrojem informací pro hacking.

V roce 1987 se objevil **první virus** na *University of Delaware*, který způsobil pouze drobné systémové chyby, žádné trvalé poškození.

Neodmyslitelnými osobnostmi tohoto desetiletí byli také vysokoškolský student z *Cornell University* **Robert Morris Jr.**, který poslal roku 1988 do světa svůj virus *InternetWorm* a **Kevin Mitnick**[8], který je znám především svým útokem na počítače společnosti *Digital Equipment*. Téhož roku také došlo ke slavné počítačové krádeži v chicagské *First National Bank*, která tak přišla o sedmdesát milionů dolarů.

V **českém prostředí** dochází k dokladovým deliktům ve formě změn dat v počítači vedoucích k obohacení pachatele či k neoprávněnému užívání počítačů.

1.2.4 90. léta

Pro devadesátá léta je charakteristické masové rozšíření osobních počítačů, zejména s OS MS Windows, čímž vzrůstá i vývoj příslušného SW. Rozvoj počítačových sítí, především **internetu**, nese své důsledky v trestné činnosti. Internet se z akademických kruhů dostává do komerční sféry a stává se tak velmi lákavou příležitostí k páchání nelegálních aktivit, které exponenciálně narůstají. Disketové mechaniky nahrazují CD-ROMy, vznikají **anonymní FTP servery** a začíná se rozvíjet **globální počítačová kriminalita**. Z typického pachatele v předchozích etapách, tedy počítačového nadšence, se stává chladný profesionál, jehož cílem je vlastní obohacení (více v kapitole 1.4.3). Fenoménem konce 90. let se do jisté míry stávají **P2P**[9] **sítě**.

Roku 1990 byli zatčeni čtyři členové **Legion of Doom** za krádež technické specifikace společnosti *BellSouth*, popisující záchranný systém 911, kterou ve zkrácené verzi publikoval Knight Lighting v časopise *Phrack*. Díky dobrému právníkovi byl zproštěn viny. Tento soud se však stal zřetelným signálem pro digitální

8 Kevin Mitnick se stal nejstíhanějším hackerem všech dob, proslul také obratným využíváním sociálního inženýrství (více v kapitole 3.2.2).

9 Peer-to-peer – architektura sítě, ve které spolu komunikují přímo jednotliví uživatelé. P2P sítě slouží ke sdílení a anonymní výměně souborů po internetu (více v kap. 3.1.1.2).

underground[10] - napadání cizích systémů nebude tolerováno a bude velmi tvrdě postihováno.

V témže roce dochází k historické události známé pod jménem **„Operace Sundevil"**. Šlo o celostátní policejní razii v USA, která měla za cíl zadržet elektronické podvodníky, odpovědné za krádeže kreditních karet a zneužívání telefonních kódů. Operace měla především odstrašující charakter a vyvolala tak otázky ochrany svobody projevu a občanských práv v kyberprostoru. Došlo k založení *Electronic Frontier Foundation*[11], neziskové společnosti zabývající se právy uživatelů digitálních technologií.

Roku 1991 se **Kevin Poulen** s dvěma dalšími hackery nabourал do telefonních linek kalifornské rozhlasové stanice a tak zmanipuloval reklamní soutěž. Později byli všichni tři chyceni.

V roce 1994 pronikli dva hackeři „Data Stream" a „Kuji" do několika stovek počítačových sítí, včetně *NASA* a *Korejského jaderného výzkumného institutu*.

V roce 1995 ruský počítačový nadšenec **Vladimir Levin** pronikl do počítačové sítě americké banky *Citibank* a převedl na své bankovní účty poměrně vysoké finanční částky. Ještě tentýž rok byl chycen *Interpolem* a odsouzen. V době zatčení neexistovala smlouva o vydávání pachatelů mezi Ruskou federací a USA, ale Levin se dopustil té chyby, že navštívil Velkou Británii, aby se zúčastnil počítačové výstavy, a ta dohodu s USA měla.

V roce 1996 se proslavil americký hacker, **Timothy Lloyd**, který pomocí šestiřádkového kódu způsobil škodu více než 10 miliónů dolarů společnosti *Omega Engineering*. Tento kód smazal veškerý důležitý software a Llyodův případ se stal jedním z nejslavnějších napadení společnosti vlastním zaměstnancem.

Roku 1999 **David Smith** vytvořil ***virus Melissa***, který způsobil globální ohrožení počítačů. Nakazil a zlikvidoval po celém světě přes 300 počítačových firemních sítí. Celková škoda byla vyčíslena na 400 milionů dolarů.

Roku 1999 byla podána žaloba společností *RIAA* na systém pro sdílení hudby **Napster**. Výsledkem bylo zablokování skladeb chráněných autorským právem (dále AP) a tím pádem odliv uživatelů na jiné sítě P2P. Napster byl nakonec zrušen a odkoupen firmou *Bertelsmann* (součástí je nahrávací studio BMG). Nyní nabízí legální prodej hudby přes internet (více o této problematice v kapitole 3.1.1.2).

---

10 Volné sdružení osob, které se angažují v aktivitách hackování, phreakování, softwarového pirátství a udržují neformální síťové kontakty. Vrcholu dosahoval zejména v 80. letech, v letech 90. díky ohromnému nárůstu uživatelů sítí došlo k vyčlenění jednotlivých subkultur. Nejznámější organizací digitálního podzemí byla zřejmě Legion of Doom.

11 Zakladatelé Michael Karpor a John Barlow.

V tomto výčtu nemůže opomenout členy skupiny **Masters of Deception**, která se zaměřovala zejména na telefonní systémy, ale dostali se například i do *NSA*[12] nebo *Bank of America* či skupinu **Masters of Downloading**, která pronikla do počítačové sítě Pentagonu a odcizila SW a tajné informace.

Na počátku 90. let v České republice stály v popředí burzy s nelegálními hudebními či filmovými nahrávkami a pochopitelně nelegálním SW. Podle BSA[13] dosahovala míra používání nelegálního SW až 80 %. Situace se začala pozvolna měnit s nárůstem kupní síly obyvatelstva a šířenou osvětou o nelegálním SW (v roce 2003 míra softwarového pirátství klesla na 40%). Dále u nás dochází zejména ke zneužívání osobních dat, šíření pornografie a internetovým podvodům typu letadla[14] či bankovním podvodům (v letech 1992-2000 došlo k 13-ti zveřejněným bankovním počítačovým zločinům, všechny případy se týkaly neoprávněné manipulace s bankovními záznamy). V roce 1996 se na českém a slovenském internetu objevuje hackerská skupina *CzERT* a *Binary Division*, které se specializovala na pozměňování webů. V příloze č. 2 je možno vidět ukázku jejich tvořivosti (více na www.hysteria.sk/hacked).

1.2.5 Období po roce 2000

Společnost je stále více závislá na počítačích a počítačových sítí. Počet uživatelů internetu neustále roste, v České republice je zmapován **nárůst uživatelů** během let 2000-2005 o celých 170 %.[15] Rozvoj internetu změnil chápání autorského díla (vznik sítí P2P) a stává se také stále více nástrojem **organizovaného zločinu**. Počítačoví piráti se spojují do skupin, vzniká tzv. **warez**. Nelegální SW se šíří prostřednictvím anonymních FTP serverů či decentralizovaných výměnných systémů typu peer-to-peer. Začínají se také objevovat věrohodné padělky autorských děl hudebních, filmových či software.

Čím dál častěji se objevují typy útoků jako **spamming**, **phishing**, **pharming**, **rozesílání malware**[16] (dle statistik McAfee [87] bylo zaznamenáno téměř každý měsíc 1500 škodlivých virů) či **spyware**[17].

Novým typem útoku se stává zaheslování souborů uložených na počítači na dálku a následné výkupné za SW - tzv. **ransomware**.

---

12 National Security Agency – Národní bezpečnostní úřad v USA.

13 Business Software Aliance [14] (více v kapitole 3.1.1 a 4.1.1).

14 Principem hry je přerozdělování vložených finančních prostředků, částečně ve prospěch hráčů, částečně ve prospěch pořadatele podle daných priorit.

15 Stav k 3. únoru 2005, zdroj: http://www.czech-talkpro.cz/-hps=stats.evropa.htm.

16 Souhrnné označení veškerých nežádoucích programů viry, červi apod. (více v kap. 3.2.1).

17 Program, který monitoruje úkony prováděné na počítači (zadávání hesel, spouštěné programy, psané e-maily apod.).

V roce 2000 hacker **MafiaBoy** (15-ti letý Kanaďan) napadl významné webové servery jako *Yahoo, eBay či Amazon*, získal tak přístup k 75-ti počítačům ve 52 sítích a spouštěl na nich DoS[18] útoky. Byl odhalen FBI (na základě vychloubání se útoky v chatovaní místnosti) a zatčen ještě téhož roku.

V témže roce spatřil světlo světa vir ***„I love you"***, který způsobil škodu asi 10 miliard dolarů, jehož autorem byl filipínský student **Onel DeGuzman** – vzhledem k neexistenci příslušné filipínské legislativy nemohl být odsouzen.

V letech 2000-2001 probíhal soudní spor mezi internetovým portálem ***Yahoo*** a francouzskou ligou proti rasismu ***LICRA***. *LICRA* žalovala *Yahoo* za propagaci nacismu, neboť přes aukční stránky portálu byly přístupné nacistické materiály a relikvie. Ve Francii *Yahoo* soud prohrál, v USA však soud rozhodl ve prospěch *Yahoo*, neboť rozhodnutí cizího soudu bylo v rozporu s Ústavou USA. V roce 2005 byl případ znovu otevřen u odvolacího soudu.

V roce 2001 došlo k zatčení ruského softwarového inženýra **Dmitryho Sklyarova** z firmy *ElcomSoft*, který porušil AP. Podařilo se mu prolomit ochranu elektronických knih Adobe ve formátu PDF. *ElcomSoft* nabízí utilitu *Advanced eBook Processor*, která převádí elektronické knihy z chráněného formátu *Adobe eBook* na nechráněný formát PDF. Podle ruské legislativy jde o legální činnost, ale vzhledem k tomu, že byl SW nabízen na internetu a mohli se tak k němu dostat občané USA - kde platí jiné zákony, byla distribuce považována za trestný čin. Firma *Adobe* nakonec od žaloby opustila. Kauza má ovšem precedenční význam, trestnost činu na internetu bude posuzována podle toho, odkud se uživatelé na obsah dívají.

Roku 2002 byl zatčen **Gary McKinnon** z Velké Británie, který pronikl do více než 90 počítačů americké armády ve Velké Británii. McKinnon se odhodlal veřejně promluvit o špatné úrovni zabezpečení sítí, které prolomil. Úřady Velké Británie ho chtěly propustit bez trestu, ale vložily se do toho Spojené státy, jejichž počítače byly napadeny. Ty požadují vydání McKinnona, kterému hrozí 45 let trestu ve federálním vězení v USA.

V roce 2005 došlo k největšímu útoku na bezpečnost dat. Bylo ohroženo až 40 miliónů kreditních karet, díky nedostatečným směrnicím a nařízením společnosti *MasterCard*.

Tentýž rok se na internetu objevily nové verze virů. V modifikované variantě zaútočil několik let starý ***vir Sober***, který je součástí e-mailu tvářící se, že jeho

18 Denial of Service, česky odepření služby - na rozdíl od počítačové viru nejde o infekci počítače, ale o jeho zahlcení či případné vyřazení z provozu (více v kap. 3.2.5).

odesílatelem je FBI. ***Červ Mytob*** se snaží příjemce přesvědčit, že e-mail pochází od poskytovatele internetového připojení.

V **České republice** roku 2000 dochází asi k nejznámějšímu případu porušování AP. Počítačová firma *Mironet* byla obviněna z instalace nelegálního software. Po neúspěšné policejní prohlídce případ utichl, *Mironet* však nakonec žaloval firmu *Microsoft*, která několik let vyvíjela tlak na instalace OS Windows, a tak padla v podezření z policejního udání. Mezi další případy můžeme zařadit umístění pirátských kopií českých filmů na internet, bankovní podvody, krádeže citlivých údajů a jejich následný prodej či e-mailové hrozby. Ani naše republika není ušetřena phishingových útoků – dokladem je březnový případ *Citibank*.

1.3 Trestné činy

Na úvod této kapitoly je vhodné uvést definici „trestného činu" dle Trestního zákona (dále TrZ) [32]:

*Trestný čin je pro společnost **nebezpečný** čin, jehož znaky jsou uvedeny v tomto zákoně. Čin, jehož stupeň nebezpečnosti pro společnost je **nepatrný**, není trestným činem, i když jinak vykazuje znaky trestného činu. K trestnosti činu je třeba **úmyslného zavinění**, nestanoví-li tento zákon výslovně, že postačí k zavinění **z nedbalosti**. Stupeň nebezpečnosti činu pro společnost je určován zejména významem chráněného zájmu, který byl činem dotčen, způsobem provedení činu a jeho následky, okolnostmi, za kterých byl čin spáchán, osobou pachatele, mírou jeho zavinění a pohnutkou.*

Pro určení deliktu se vymezují tyto formální znaky:

- **objekt trestného činu** – za objekt trestného činu jsou považovány předměty ochrany trestním zákonem,
- **předmět útoku** – tím může být člověk, věc, ale i nehmotný majetek (právo, informace apod.),
- **objektivní stránka trestného činu** – zahrnuje především tzv. obligatorní znaky, kterými jsou: jednání, následek a příčinný vztah mezi nimi (kauzální průběh),
- **subjektivní stránka trestného činu** – zahrnuje znaky týkající se psychiky pachatele (zavinění, pohnutka apod.).

Vzhledem k šíři EIK jsou zde uvedeny klasifikace možných trestných jednání vztahujících se k počítači, které lze podle SMEJKALA [122] rozdělit do následujících subkategorií, podle kterých rozeznáváme tři typy kriminality:

- trestné činy ve vztahu k **počítači**, jeho příslušenstvím a jiným nosičům informací – zde hovoříme o majetkové kriminalitě v klasickém významu, na kterou se vztahuje zejména **§250** TrZ,

- trestné činy ve vztahu k **software**, k datům, resp. uloženým informacím - jde o informační kriminalitu, která je předmětem této práce a na kterou se vztahují zejména **§152**, **§178** a **§257a** TrZ a **§65-66** Autorského zákona (dále AutZ),
- trestné činy, při nichž je **počítač prostředkem** k jejich páchání – hovoříme o hospodářské kriminalitě, na kterou se vztahuje zejména **§125** TrZ.

Definovat jednotlivé trestné činy a zejména seskupit je do určitých logických kategorií je pro tento druh kriminality poměrně obtížné, existuje několik pojetí od různých autorů. Převážně se operuje s termínem kriminalita počítačová, jak již bylo naznačeno v úvodní kapitole. Dále jsou pro názornost uvedeny publikované klasifikace, např. LÁTAL [73] rozeznává:

- úmyslné útoky **proti vlastnímu nosiči informace**, případně i datům v něm uložených s úmyslem je zničit,
- počítač slouží jako **prostředek obohacení**, přičemž se dále rozlišuje:
  - krádež dat a programů,
  - krádež strojového času počítače,
  - nezákonné manipulace s počítačem, daty nebo programy.

SMEJKAL [123] trestné činy rozděluje při určitém zjednodušení do dvou základních skupin na:

- delikty, kde počítač, program, data, informační systém apod. jsou **nástrojem** trestné činnosti pachatele,
- delikty, kde počítač, program, data, informační systém atd. jsou **cílem** zločinného útoku, přičemž se může jednat o tyto trestné činy:
  - fyzický nebo logický útok na počítač nebo komunikační zařízení,
  - neoprávněné užívání počítače nebo komunikačního zařízení,
  - neoprávněné užívání nebo distribuci počítačových programů,
  - změnu v programech a datech, okrajově i v technickém zapojení počítače nebo komunikačního zařízení,
  - neoprávněný přístup k datům, získávání utajovaných informací (tzv. počítačová špionáž) nebo jiných informací o osobách (osobní údaje),
  - trestné činy, jejichž předmětem útoku je počítač jako věc movitá.

Obdobně NOVÁK [96] rozděluje počítačovou kriminalitu na:

- útok směřující ke **zničení počítače**,
- útok směřující ke **zneužití dat** formou neoprávněného získání nebo změnou dat, přičemž tento útok může být motivován zištně s cílem získat hmotný prospěch, nebo s cílem dosáhnout zprostředkovaného hmotného prospěchu, např. zneužitím citlivé informace),
- **porušení AP**, a to formou využití softwaru pro svou potřebu nebo nezákonnou distribucí softwaru,
- **zneužití strojového času**.

Výčet trestných činů (skutkových podstat) podle české legislativy, které by patřily pod výše uvedené podtypy, je poměrně bohatý. Mezi **historické** trestné činy v České republice řadíme sabotáže, dokladové delikty a neoprávněné užívání počítačů. Současný **Trestní zákon (140/1961 Sb.)**, ve znění pozdějších předpisů, rozeznává v oblasti EIK níže jmenované trestné činy, resp. skutkové podstaty. Tento přehled pravděpodobně nevyčerpává všechny varianty zneužití ICT, neboť ty mohou být aplikovány na mnoho klasických trestných činů. Obecně můžeme říci, že pomocí ICT lze spáchat jakýkoli trestný čin, který nevyžaduje pachatelovu přítomnost na místě činu. ICT mohou být také využívány v **přípravné fázi**, resp. komunikaci mezi pachateli. V závorce jsou jmenovány paragrafy Trestního zákona, které se k danému deliktu vztahují:

- **poškození a zneužití záznamu na nosiči** (§257a) – zde máme na mysli zejména infikování počítačovým virem a průnik do cizího počítače (zásahy do cizích programů a databází) – tzv. **počítačová defraudace**;
- **porušování autorského práva, práv souvisejících s právem autorským a práv k databázi** (§152) – v tomto případě hovoříme především o pirátství týkající se SW, audio či video souborů (nelegální kopírování, distribuce, plagiátorství), osobování si autorství cizího díla, neuvedení autora, změně či užití díla bez svolení autora, nezaplacení autorské odměny za užití díla atd.;
- **porušení práv k ochranné známce, obchodnímu jménu a chráněnému označení původu** (§150) - zde máme na mysli především doménové pirátství;
- **porušování průmyslových práv** (§151);
- **neoprávněné zacházení s osobními údaji** (§178);
- **zkreslování údajů o stavu hospodaření a jmění** (§125) – jde zejména o uvádění nepravdivých nebo zkreslených informací v podnikových informačních systémech;
- **porušování tajemství dopravovaných zpráv** (§239-240) – tento případ se týká zasílání mailů či sledování síťové komunikace, neboť internet dle §239 považujeme za veřejné zařízení, §240 týkající se způsobení úmyslné škody či osobního obohacení můžeme aplikovat i na obsah doručeného e-mailu či síťový provoz;
- **poškozování a ohrožování provozu obecně prospěšného zařízení** (§182) – v případě zneužívání telekomunikačních služeb;
- **podvody** (§250) - podstata tohoto jevu spočívá ve využití něčího omylu ve svůj prospěch, k těmto deliktům dochází zejména ve finančních sektoru (např. neoprávněné manipulace s bankovním záznamy, aukční podvody nebo finanční hry typu letadla či pyramidy - §250c), k podvodům může docházet i v souvislosti s neoprávněným nakládáním s osobními údaji, s nekalou soutěží či porušováním AP - padělky digitálních dokumentů či padělky nosičů informací v podobě telefonních, kreditních, platební a jiných karet;
- **zpronevěra** (§248) - v souvislosti s trestným činem podvodu, zejména ve finanční oblasti;

- **neoprávněné užívání cizí věci** (§249) – sem můžeme zahrnout neoprávněné užívání počítače či komunikačního zařízení pod identifikací jiného oprávněného uživatele,
- **nekalá soutěž** (§149) – souvisí s porušováním AP, neboť plagiáty parazitují na dobré pověsti oficiálního výrobce SW.

Dále jsou uvedeny trestné činy, ke kterým může dojít při zpřístupňování, shromažďování a šíření informací v prostředí internetu, tedy prostřednictvím e-mailu, IRC[19], WWW, blogů či různorodých diskusních skupin:

- **pomluva** (§206),
- **ohrožování mravnosti** (§205),
- **podpora a propagace hnutí směřující k potlačení práv a svobod člověka** (§260-261),
- **hanobení národa, rasy a přesvědčení** (§198, §198a),
- **šíření poplašné zprávy** (§199-200),
- **neoprávněné nakládání s osobními údaji** (§178),
- **ohrožení státního tajemství** (§106),
- **vydírání** (§235).

Jmenované skutkové podstaty rozlišují varianty trestního postihu podle **výše způsobené škody** nebo dosaženého prospěchu. České právo, na rozdíl od anglosaského, nezná sčítání trestů. V případě, že je pachatel odsouzen za více trestných činů, je mu vyměřen trest podle nejvyšší - nejpřísnější trestní sazby. Podle zákona lze za každý trestný čin uložit odnětí svobody, za některé činy lze uložit i jiné tresty současně, nebo i alternativní tresty v podobě zákazu činnosti, peněžitého trestu, propadnutí věci, veřejně prospěšné práce atd. Při stanovení trestu musí soud vycházet ze **zásady úměrnosti** a brát ohled na **intenzitu porušení společenského zájmu**. [85]

Na závěr této je zmíněno členění, které přijala **Rada Evropy**, jehož smyslem je mj. sjednotit legislativu evropských zemí, neboť tato trestná činnost má díky internetu neomezené hranice v celosvětovém měřítku.

Do minimálního seznamu trestných činů jsou zahrnovány:

- počítačové podvody,
- počítačové falzifikace,
- poškozování počítačových dat a programů,
- počítačová sabotáž,
- neoprávněný přístup,
- neoprávněný průnik,

19 Internet Relay Chat – označení protokolu či také chatovaní sítě, kde spolu jednotliví účastníci komunikací mluví v reálném čase.

- neoprávněné kopírování autorsky chráněného programu,
- neoprávněné kopírování fotografií.

Do volitelného seznamu trestných činů je zahrnuto:

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

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

Autoři SMEJKAL a SOKOL [124] se domnívají, že toto členění není ideální, protože v některých případech jde o překrývající se nebo těžko odlišitelné úkony, některé nejsou jasně definovány, chybí zde diskuse, zda se jedná výlučně o úmyslné trestné činy nebo zda jsou sem zahrnuty i delikty nedbalostní.

1.4 Pachatelé

Klasifikace pachatelů EIK může vycházet jednak z **psychologických** hledisek, jednak z hledisek **kriminologických**. Z tohoto pohledu podle LÁTALA [73] pak rozlišujeme:

- cílevědomé kriminogenní osobnosti
- příležitostné typy

Obecně můžeme říci, že pachateli trestných činů v oblasti EIK bývají obvykle osoby:

- se středoškolským, jiným vyšším nebo vysokoškolským vzděláním - zejména v technických oborech, speciálně v oboru IT,
- často nadprůměrně inteligentní, vynalézavé - zejména ve specifické programátorské oblasti,
- zneužívající svého vyššího výsadního postavení v zaměstnání s tomu odpovídající pravomocí,
- ve svém pracovním zařazení nebo ohodnocení neuspokojení,
- jejichž protiprávní jednání je vzdáleno tradičním hrubým formám delikvence - neobsahuje prvky násilí.

Pachatele můžeme dělit také z hlediska jejich **vztahu k informacím**, a to na:

- **Amatéry,** kam bychom zařadili hackery, crackery, neúspěšné kritiky a mstitele. Jde o osoby pronikající náhodně nebo cílevědomě do informačních

systémů tak, že vyhledávají zranitelná místa. Jejich cíle nebo motivace jsou různé.

- **Profesionály,** kam by patřili pracovníci speciálních tajných služeb, detektivové, žurnalisté, podnikatelé, specialisté informatici, softwaroví piráti či teroristé (zvláštní skupina organizovaného zločinu). [73]

Někteří pachatelé provádí trestnou činnost samostatně, ale ve většině případů jde o sdružování a spolupráci více osob, které se formují do určitých skupin. Jednotliví členové se většinou ani osobně neznají, neboť veškerá komunikace probíhá elektronicky.

Vztahy mezi undergroundovými skupinami, zabývající se touto trestnou činností, jsou poměrně spletité. Je pochopitelné, že mezi „laiky", ale i médii panuje značný chaos v terminologii a chápání problematiky vůbec, proto je vhodné tyto nejasnosti v následujících subkapitolách objasnit.

1.4.1 Hackeři a jejich subkultury

Význam označení hacker[20] prodělal v průběhu let pozoruhodný vývoj. Zatímco dříve bylo synonymem pro člověka, ke kterému se vzhlíží s úctou, dnes jej většina lidí považuje za označení počítačového kriminálníka. Termín se objevil mezi radioamatéry již v 50. letech, o desetiletí později byl použit komunitou z *Massachusets Institute of Technology*. Obecně můžeme říci, že hacker je člověk nadšený programováním, baví ho zkoumat detaily a způsoby využití systémů, překonávání překážek tvořivým způsobem je pro něj výzvou. Musíme tedy zdůraznit, že činnost pravého hackera spočívá v **pronikání do ochraňovaných systémů** s cílem **prokázat své schopnosti** a **kvality bez zájmu získat informace** či **narušit systém**. Podstatné je překonávání ochranných bariér, což je považováno za zábavu, dobrodružství. Nutno podotknout, že svět hackerů je založen na reputaci.

Pro opravdové hackery je typické jejich sociální chování, používaný jazyk, uznávání morálních hodnot a samozřejmě provádění samotného hackingu. Pojem **hacking** označuje činnosti, které pravý hacker provádí a kterými získává uznání a respekt - získání a zpřístupnění zdrojového kódu programů, odhalení slabin informačního systému a zpřístupnění příslušných informací, publikování užitečných informací na internetu, pomoc při administrativě a provozu diskuzních skupin, seznamů, archivů atd., pomoc při testování nových programů – tzv. beta verze či propagace hackerské kultury. [133] Pro zajímavost můžeme zmínit, že hacking, který **není** páchán tak, aby způsobil někomu jinému škodu či jinou újmu nebo sobě či

[20] Slovní základ hack lze přeložit mnoha způsoby - rozsekat, rozřezat, otesávat, opracovávat, zaseknout, udělat zářez.

jinému neoprávněný prospěch, není kvalifikován jako trestný čin, a tudíž **není postižitelný** (více v kap. 3.2.2).

Pro doplnění je ještě nutné uvést pojem **hactivismus**, který představuje politicky motivované napadání internetových stránek.

Mezi hackery můžeme rozeznávat následující subkultury, které zmiňuje MAXFIELD (1985)[21], i když jde spíše o historickou záležitost:

- **průkopníci** (pioneers) – ti, kteří jsou fascinovaní vývojem technologií, zkoumají prostředí bez určitého cíle,
- **uličníci** (scamps) – hackeři se smyslem pro humor, neplánují žádnou destrukci,
- **průzkumníci** (explorers) – hackeři motivovaní potěšením z pronikání do systémů, čím obtížnější překážka, tím větší požitek,
- **hráči** (game players) – ti, kteří překonávají softwarovou nebo systémovou ochranu, vše berou jako určitou hru,
- **vandalové** (vandals) – ti, kteří působí škody, aniž by jim z toho plynuly zisky,
- **nadšenci** (addicts) – počítačoví hlupáci, kteří jsou doslova závislí na hackingu a počítačových technologií.

V důsledku různých medializovaných kauz průniků do sítí se výraz „hacker" vžil jako nálepka pro vandalství, poškozování informačních a komunikačních systémů. Označení „hacker" je tak velmi často zaměňováno s níže popisovaným pojmem „cracker", a to na úkor první zmiňované skupiny.

1.4.2 Crackeři a jejich subkultury

Toto označení se objevilo v souvislosti s pojmem **crack**, který představuje narušení zabezpečení ochrany a integrity programu nebo systému. Podle jednoho pohledu jde o osoby schopné **prolomit kód** určitého SW a umožnit tak jeho nelegální kopírování, z jiného hlediska jde o osoby, které **pronikají do počítačových systému s úmyslem jejich poškození**.

Cracking[22] je činnost, kdy dojde k narušení informačního systému zvenčí (prolomení ochrany). Cracker zpravidla nepracuje sám, ale ve skupinách. Členové bývají ve skupině děleni na hierarchicky odlišené pozice a každý má na starosti konkrétní činnost. Skupiny bývají tematicky specializované na herní oblasti, weby a na aplikace. Mezi skupinami panuje poměrně vysoká soutěživost, své úspěchy pečlivě dokumentují a zpravidla i zpřístupňují na internetu. [133]

21 Zdroj: http://faculty.ncwc.edu/TOConnor/315/315lect12.htm.

22 Slovní základ crack znamená rozbít, rozlousknout.

Crackeři se sami často považují za hackery. Avšak jejich znalosti informačních systémů, internetových protokolů a programování nejsou na tak vysoké úrovni jako u hackerů. Crackeři používají k průniku do informačních systémů především zveřejněné slabiny, na které ještě administrátoři nezareagovali. K úpravě komerčních programů crackeři používají a testují známé triky. Cracknuté programy dále šíří nelegální cestou - **warez** (více v kap. 3.1.1.1). Zásadní rozdíl, odlišující tyto patogenní osobnosti od hackerů, spočívá v pronikání do systémů s cílem data získat a následně zneužít ve vlastní prospěch. K těmto charakteristikám můžeme ještě přiřadit potěšení z destrukce systému.

Pro získání celkového přehledu osob pohybujících se v digitálním undergroundu jsou uvedeny další pojmy:

- **samuraj** – útočník, který pronikne do systému, avšak následně správci oznámí bezpečnostní nedostatky a poskytne mu konkrétní rady,
- **script-kiddies** – začínající útočníci s průměrnými znalostmi, kteří dokáží na internetu najít kód a mírně ho upravit, např. pro spuštění nové varianty viru (převážně využívají nástroje vytvořené jinými útočníky- skripty),
- **packet monkeys** – nezkušení uživatelé, kteří provádí DoS útoky či jiné útoky nevyžadující prolomení ochrany, opět za použití utilit vytvořených jinými,
- **phreaker/phracker** – útočník, který proniká a zneužívá telefonních sítí (více v kap. 3.2.3),
- **phisher** – útočník, který vytváří identické webové stránky většinou různých finančních institucí a poté ukradne a zneužije citlivé údaje uživatelů, kteří je zadají v domnění, že jde o oficiální stránky instituce (více v kap. 3.2.4),
- **knacker** – útočníci, který odstraňují ochranný kód programů za účelem jeho volného používání,
- **looser/lamer** – uživatelé neznalí prostředí IT.

V literatuře zahraničních autorů [135] se můžeme také setkat s pojmy:

- **white hats** – tzv. „hodní" hackeři, kteří nezpůsobují žádné škody a upozorňují administrátory systémů na objevené bezpečnostní chyby, někdy jsou také označování jako „ethical hackers" – jde tedy o hackery v pravém slova smyslu,
- **black hats** – hackeři s kriminálními motivy, účelem je vlastní obohacení – jde tedy o tzv. crackery,
- **grey hats** – šedá zóna hackerů stojící na pomezí mezi předchozími typy, typické je pro ně zveřejňování bezpečnostních děr, tzv. exploitů v internetu za účelem růstu úrovně bezpečnosti systémů (výše uvedený samuraj),
- **elite** – hackeři proslavení nejlegendárnějšími kousky (viz zmiňované osobnosti v kapitole 1.2).

Uvedené členění hackerů na white, black a grey hats se nabízí jako vhodné řešení terminologických nejasností. Nicméně můžeme konstatovat, že zaměňování termínů hacker - cracker v posuzování trestnosti či beztrestnosti nehraje žádnou roli.

Záleží na povaze trestné činnosti, kterou pachatelé provádí, ať už je označíme tak, či onak. A toto pojetí se pravděpodobně nezmění ze dne na den.

1.4.3 Motivace a cíle

Jak již bylo výše naznačeno, motivace a cíle pachatelů jsou různé. Hackeři v pravém slova smyslu (white hats) věří ve **svobodu jedince** a jsou ochotni pomoci jiným, **elektronický svět je pro ně výzva** a je zaplněn problémy, které čekají na jejich pokoření – vyřešení. Hacker žádný problém neřeší dvakrát – jednou vyřešený problém již pro něj není zajímavou výzvou. Svět hackerů je založen zejména na **reputaci**. Nový člen komunity získá svoji pozici v této komunitě až poté, co projeví své schopnosti, ale také svoji ochotu podílet se na ideálech komunity hackerů. Hacker nebere, ale dává. Věnuje svůj čas, svoji kreativitu a výsledek svých znalostí ve prospěch řešení problémů. [133]

K osvětlení hackerských motivací je žádoucí zmínit dva základní **morální principy** této komunity:

- víra, že sdílení informací je správné a dobré, a že je etickou povinností hackerů dělit se o své poznatky psaním open-source[23] a usnadňováním přístupu k informacím a počítačovým zdrojům v maximální možné míře,
- víra, že pronikání do systémů pro pobavení a získání zkušeností je eticky v pořádku, dokud však nedojde k vandalismu, zcizení informací či porušení jejich utajení.

Oba tyto základní principy jsou mezi hackery přijímány. Většina hackerů se hlásí k hackerské etice v prvním zde uvedeném významu a naplňuje její význam psaním a zveřejňováním open-source SW. Někteří jdou v tomto trendu ještě dále a prosazují myšlenku, že všechny informace by měli být **volně dostupné** a jakákoli **patentová kontrola je špatná**; toto je filosofie, která stojí za **GNU**[24] projektem. Nejlepší ukázkou obou smyslů hackerské etiky je skutečnost, že téměř všichni hackeři se aktivně podílejí na šíření a sdílení technických triků, softwaru a počítačových zdrojů s ostatními hackery. Internet, jakožto síť bez jakékoli centrální kontroly či cenzury funguje právě díky tomuto fenoménu - spoléhá a zdůrazňuje smysl komunity, která je snad největším přínosem hackerství. [64]

U crackerů (black hats) je převažujícím motivem **zisk** či **osobní obohacení**. Tento druh kriminality je vysoce výnosný, a to mnohonásobně než u tzv. klasické kriminality. Crackeři převážně napadají webové stránky a informační systémy s cílem získat, pozměnit či poškodit některá uložená data. [133] Nejproblematičtější a zároveň

23 Software obsahující volně dostupný zdrojový kód – možná úprava a distribuce. Otevřenost znamená jak technickou dostupnost kódu, tak legální dostupnost.

24 GNU's Not Unix - Projekt Free Software Foundation, který si klade za cíl vytvořit volně šiřitelnou náhradu operačního systému UNIX.

pro pachatele nejvýnosnější oblastí je **finanční sektor**. Existují i další motivy, případně jejich kombinace, jako např.:

- pocit převahy nad zaměstnavatelem (pachatelé – zaměstnanci znají dobře firemní systém, zabezpečení systému, disponují určitou úrovní oprávnění k přístupům do IS), policií či veřejností,
- názor, že firmě nemohou uškodit malé ztráty,
- pocit beztrestnosti a neodhalitelnosti,
- snaha kompenzovat svoji nespokojenost s prací, osobním životem,
- touha po dobrodružství a riziku.

Cíle, které souvisí s informacemi, mohou představovat získání informace, znemožnění získání informace, udržení získané informace, ztracení či zničení získané informace, šíření informace nebo znemožnění šíření informace. [104] U pachatele a oběti vlastně dochází k protikladným cílům. Možné varianty informačního boje jsou naznačeny v následující tabulce č. 1.

	POTENCIONÁLNÍ OBĚŤ / obránce	**PACHATEL / útočník**
1	chce získat informaci	chce znemožnit obránci získat informaci
2	chce udržet získanou informaci	chce, aby obránce získanou informaci ztratil
3	chce znemožnit útočníkovi získat informaci	chce získat informaci
4	chce, aby útočník získanou informaci ztratil	chce udržet získanou informaci
5	chce, aby útočník získal informaci	chce, aby nemohl získat informaci
6	chce, aby útočník udržel získanou informaci	chce ztratit získanou informaci
7	chce, aby nemohl získat informaci	chce, aby obránce získal informaci
8	chce ztratit získanou informaci	chce, aby obránce udržel získanou informaci
9	chce šířit informaci	chce zabránit šíření informaci
10	chce zabránit šíření informaci	chce šířit informaci

Tabulka č. 1 - Typy informačního boje, převzato z [104]

Konkrétně může jít např. o prodání získaných dat či jejich využití k další trestné činnosti (např. šíření poplašných zpráv, vydírání, bankovní podvody apod.), poškození dat či SW atd. Extrémní případy vedou k informační/kybernetické válce (více v kap. 3.2.6).

2 Zásady informační bezpečnosti

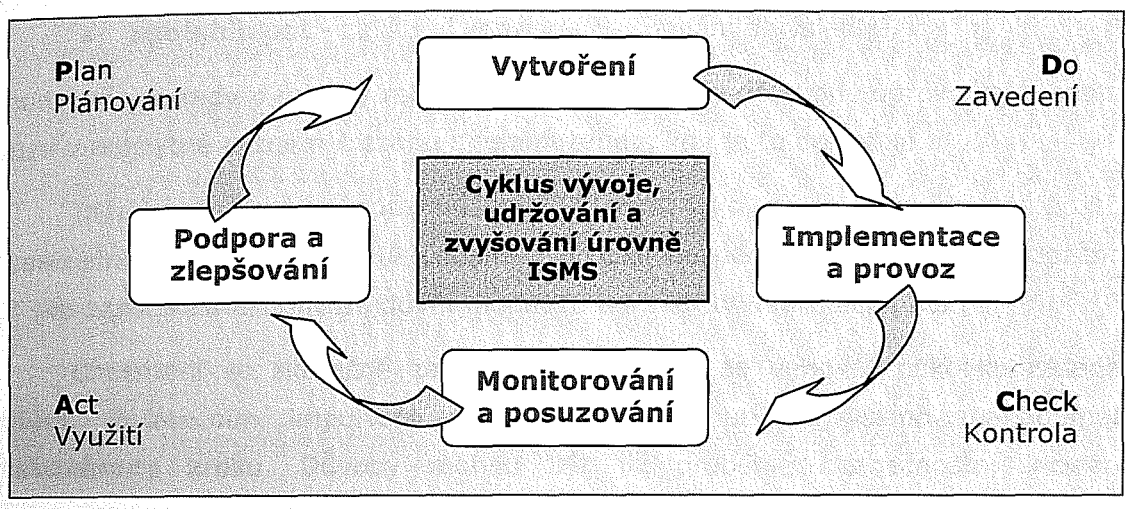
Pojem informační bezpečnost (dále IB) se dostává do popředí díky prudkém rozmachu IT, potažmo informačních a komunikačních systémů. Jejich rozrůstající se implementace do všech oblastí lidského života ovšem zvyšuje také riziko napadení, ať už záměrné nebo způsobené chybou či neznalostí. To nás přivádí - nebo by alespoň mělo – ke zvyšování zabezpečení proti napadení a zneužití těchto systémů. IB se stává samostatným multidisciplinárním oborem, proto v následujících kapitolách naznačuji jen nejdůležitější body této problematiky. IB by měla být chápána jako komplexní a dynamická záležitost a vzhledem k neustálému technologickému vývoji by mělo být její budování trvalým procesem. Bezpečnost se nedá zúžit pouze na IS nebo ICT, musí se řešit všechny aspekty včetně organizačních procedur a chování jednotlivců.

Informace, které jsou nejčastěji v ohrožení jsou buďto osobní data občanů či hospodářsky využitelné údaje. Ochrana soukromí je dána Ústavou ČR a Listinou základních práv a svobod. **Ochrana osobních údajů** v prostředí informačních systémů byla původně ustanovena zákonem č. 256/1992 Sb., který se však ukázal nevyhovujícím a stal se terčem kritiky. Nedostatky měl odstranit Zákon č. **101/2000 Sb.**, o ochraně osobních údajů. Ten upravuje ochranu osobních údajů, práva a povinnosti vznikající při jejich zpracování, sankce za porušení. Vztahuje se na osobní údaje zpracovávané státními orgány, orgány veřejné správy, fyzickými či právnickými osobami. Elektronické zpracování občanských osobních údajů je dnes zcela běžnou činností a proto je jejich právní úprava nezbytná. S postupující globalizací informační společnosti a vývojem ICT jsou osobní údaje čím dál cennější, ale zároveň také zranitelnější. Získané soubory dat lze velmi dobře prodat, ale také propojit s kteroukoli jinou databází. Což může způsobit vytvoření celistvého obrázku o uživateli, o jeho zájmech, majetku atd. Spousta citlivých údajů - jako čísla kreditních karet, mobilních telefonů - umožňuje najít také oblíbený vyhledávač **Google,** který je sbírá. Je bránou k celým databázím přístupových jmen a hesel.

Neoprávněné nakládání s těmito údaji upravuje **§178** TrZ. Další právní úpravou týkající se ochrany soukromí v kyberprostoru je dlouho očekávaný Zákon č. **480/2004 Sb.,** o některých službách informační společnosti (více v kap. 3.3).

Hospodářsky využitelné informace, např. utajované obchodní informace, které v případě jejich zneužití mohou vést např. až ke konkurzu firmy, jsou nehmotným bohatstvím firmy. Neoprávněné získávání takovýchto informací je označováno jako počítačová špionáž, na kterou se mohou vztahovat trestné činy **§105** – vyzvědačství, **§106-107** ohrožování utajované skutečnosti, **§125** – zkreslování údajů o stavu hospodaření a jmění, **§149** – nekalá soutěž apod.

Cílem řešení IB je s minimálními náklady vytvoření maximální ochrany před možnými útoky. [44] Za tímto účelem čím dál více specializovaných firem nabízí podnikům systémy řízení informační bezpečnosti, tzv. *ISMS (Information Security Management System).* Zavádění ISMS je prováděno podle modelu *PDCA* (Plan – Do – Check – Act), který rozděluje celý proces do čtyř kroků zobrazených na obrázku č. 1:



Obr. č. 1 - Model PDCA

Příklady **českých firem**, které se specializují na jednotlivé fáze budování informační bezpečnosti:

- F.S.C. bezpečnostní poradenství, a. s.
- NeXA
- DNV
- DCIT
- DAMOVO aj.

2.1 Důvěrnost – integrita – dostupnost

Zajištění adekvátní úrovně IB je nezbytné pro všechny firmy a instituce, které pracují s IS připojenými k internetu (na velikosti subjektu nezáleží), neboť nedostatečné zabezpečení informací, resp. IS, může těmto subjektům způsobit nedozírné škody. V každé takové firmě či instituci jsou systémy, které zpracovávají informace různé důležitosti a stupně utajení, a záleží na managementu, zda zorganizuje budování IB. Otázkou by však nemělo být zda, ale „kdo – co a proč – jak".

Teorie bezpečnosti informací popisuje tři základní atributy nezbytné k zabezpečení informací, a to [127]:

- **důvěryhodnost** – zajištění toho, že informace je dostupná pouze osobám s autorizovaným přístupem,

- **integrita** – zabezpečení přesnosti a kompletnosti informací a metod zpracování,
- **dostupnost** - zajištění toho, že informace a s nimi spjatá aktiva jsou dostupné autorizovaným uživatelům podle jejich potřeby.

K těmto třem základním požadavkům bychom mohli ještě doplnit:

- **zodpovědnost** – privilegování individuální zodpovědnosti,
- **spolehlivost** - zajištění konzistence chování a výsledků.

V podstatě jde tedy o to, aby relevantní informace byly dostupné oprávněným osobám pouze v nezbytně nutném rozsahu a jenom tehdy, kdy je to potřebné.

Informační bezpečnost můžeme definovat jako vzájemně provázaná opatření organizační, administrativní, personální a fyzické bezpečnosti a opatření bezpečnosti ICT pro zajištění dostupnosti, důvěryhodnosti a integrity informací. [127]

Chceme-li se skutečně zabývat IB, musíme se věnovat několika zásadním bodům. Počátečním impulsem musí být rozhodnutí nejvyššího managementu k takovémuto kroku. Důvody mohou být již proběhlé bezpečnostní incidenty, implementace nového IS, negativní závěry auditu, rozhodnutí majitelů, snaha získat konkurenční výhodu apod. **Budování IB** obnáší zajištění interních i externích lidských zdrojů, vyhrazení finančních prostředků, zodpovědnost a v neposlední řadě smíření se s faktem, že řešení bezpečnosti je nikdy nekončící proces.

Podporu managementu lze považovat za nultý krok, na který navazují další fáze popisující IB, a to:

- **strategie informační bezpečnosti** – spočívá v definování hlavních cílů (co a jak chránit), v návrhu a následném schválení dalších kroků, výstupem bývá projektová dokumentace, popř. celková bezpečnostní politika,
- **analýza rizik** – odpovídá na otázku, která opatření je vhodné použít i cílenému a zároveň efektivnímu zajištění bezpečnosti informací,
- **informační bezpečnostní politika (IBP)** – definuje hlavní pravidla a zásady bezpečnosti (více v kapitole 2.2),
- **bezpečnostní směrnice a standardy** – konkrétní závazná pravidla a postupy bezpečnostní politiky, jsou součástí interní legislativy (více v kapitole 2.3),
- **implementace bezpečnosti** – zahájení jednotlivých koordinovaných bezpečnostních projektů (např. bezpečnostní vzdělávání, havarijní plánování, zabezpečení připojení na internet, implementace infrastruktury veřejných klíčů),
- **monitorování a kontrola** – podstatná část procesu umožňující zpětnou vazbu (korekce celkové bezpečnostní politiky).

Podnětem k budování IB jsou **bezpečnostní rizika** (ohrožující data a informace), která mohou pocházet z různých zdrojů. Dle určitého zjednodušení

rozeznáváme rizika personální, administrativní a technická. V první řadě zde selhává **personální faktor**, ke kterému se přidávají faktory obvykle též spočívající v personální rovině, kdy zaměstnanci zodpovědní za bezpečnost a výpočetní techniku nesplnili své povinnosti nebo podcenili hrozící nebezpečí. Člověk, ať strůjce informací, je nejslabším článkem v celém informačním procesu, co se možnosti zneužití týče. Personální rizika jsou ovlivněna životními postoji, psychikou člověka, zainteresováním na pracovním úkolu a v podstatě přístupem k celé problematice. V případě úmyslného promyšleného útoku, pachatel vychází ze znalosti vnitřního systému, disponuje určitou úrovní oprávnění přístupu a nic mu, snad kromě svědomí, nebrání k provedení útoku. Proto je třeba implementovat dle konkrétní situace účinná **technologická** (šifrování síťové komunikace, používání antivirových a antispywarových programů, pravidelné provádění aktualizací, implementace firewallu apod.) a **organizační** opatření (vypracování bezpečnostních pravidel, směrnice, oddělení intranetu od internetu, časově rozlišené přístupy, certifikace systémů, sofistikovaná a silná autentizace - např. pomocí biometrie, používání silných hesel atd.).

Podle průzkumu společnosti *Ernst & Young*, časopisu *DSM* – data security management a *Národního bezpečnostního úřadu* považují české firmy za největší hrozbu bezpečnosti informačních systémů **internet** a **e-mail**. Pro bližší představu o stavu bezpečnostní politiky v České republice v roce 2005 uveďme zjištěná data [29]:

- přes 60% společností využívá outsourcing v alespoň jedné oblasti IS/IT (nejčastěji banky a finanční společnosti, dále potravinářské nebo zemědělské firmy),
- 48% společností má v podobě dokumentu formálně definovanou bezpečnostní politiku,
- 86% společností uvádí výskyt spamu,
- 72% společností zaznamenalo zavirování PC nebo sítě e-mailovým virem,
- 44% společností se setkalo s fingovanými či podvodnými e-maily,
- 93% společností využívá firewall,
- 86% společností provádí kontrolu přítomnosti počítačových virů pomocí antivirových programů,
- 52% společností používá elektronický podpis, 37% využití plánuje,
- téměř 60% oslovených firem se domnívá, že situace v ČR je stejná nebo lepší ve srovnání se západoevropskými státy,
- 32% společností považuje za největšího překážku flexibilnějšího prosazování informační bezpečnosti nízké bezpečnostní povědomí, 17% finanční náročnost a 16% nedostatečnou podporu ze strany managementu.

Z průzkumu vyplývá, že IB je stále ještě podceňovanou oblastí - organizace, které jsou na svých datech a informacích závislé, by si měly uvědomovat potencionální

rizika a věnovat se cílené a efektivní ochraně svých nehmotných statků. Zavádění IB v organizacích je **dlouhodobý a poměrně nákladný proces**, avšak tato investice by měla být brána jako náklad na pojištění.

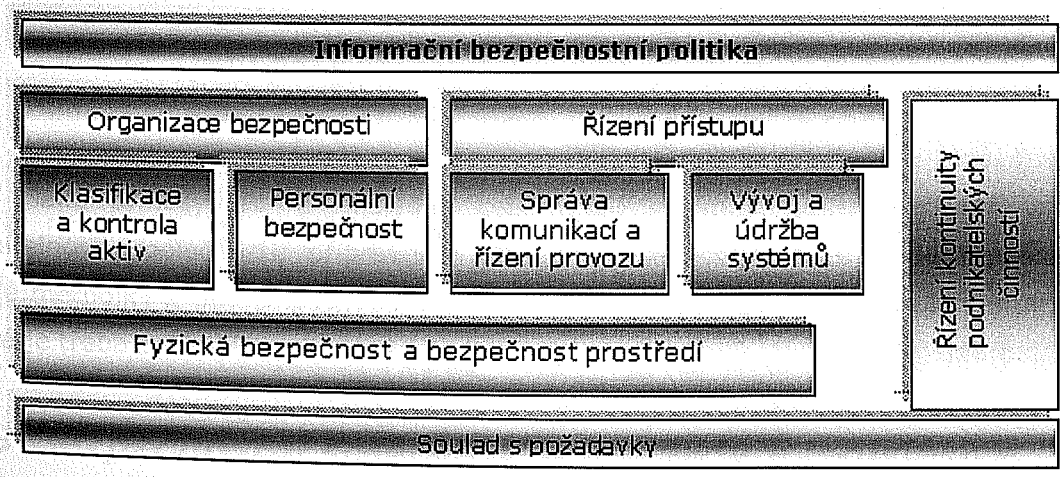
2.2 Informační bezpečnostní politika

Informace, jakožto majetek s určitou hodnotou (aktiva) musí být chráněny před neoprávněným přístupem, zcizením, zfalšování, zneužitím, vyzrazením či jinými hrozbami, a to v rámci informační bezpečnostní politiky (dále IBP). Vytvoření IBP následuje po analýze rizik, která vede k detailnímu poznání problémů (HW, SW, provozní prostředí či lidé) a potřeb organizace. Zpracování bezpečnostní politiky je povinné podle Zákona č. **412/2005 Sb.**, o ochraně utajovaných informací a Zákona č. **353/1999 Sb.**, o prevenci závažných havárií.

IBP chápeme jako **programový dokument** (většinou součástí dokumentace ISO 900x či jiných systémů řízení kvality), který:

- definuje hlavní cíle při ochraně informací,
- stanoví způsob řešení bezpečnosti (budování ISMS) a
- určuje pravomoci a odpovědnosti za budovaný ISMS.

Tento klíčový dokument je po přijetí managementu závazný pro celou společnost. Na následujícím obrázku č. 2 jsou zobrazeny jednotlivé oblasti IB, které pokrývá bezpečnostní politika podle doporučení **ISO/IEC 17799** (více v následující kapitole).



Obr. č. 2 – Komponenty bezpečnostní politiky, převzato z [127]

- **organizace bezpečnosti** – definování vhodných organizačních a řídících struktur, rolí a odpovědnosti pracovníků a organizace,
- **klasifikace a kontrola aktiv** – provedení přehledu a klasifikace toho, co bude předmětem ochrany,

- **personální bezpečnost** – definování cílů v oblasti zajištění a zvyšování bezpečnostního povědomí pracovníků,
- **fyzická bezpečnost** – definování cílů v oblasti předcházení neautorizovanému přístupu k citlivým informacím,
- **řízení provozu** – zajištění správného a bezpečného provozu prostředků IT/IS,
- **řízení přístupu** – zajištění adekvátního přístupu k informacím organizace,
- **vývoj a údržba systému** – stanovení bezpečnostních pravidel pro údržbu a rozvoj systému,
- **řízení kontinuity** – minimalizace výpadků a škod stanovených bezpečnostními incidenty,
- **soulad s požadavky** – zajištění dodržování právních norem, smluvních a bezpečnostních požadavků. [127]

Žádná ze jmenovaných složek by neměla být podceněna, ponechána náhodě. Útočníci se na akce připravují velmi pečlivě a mají zjištěny spousty informací o prostředí systému, na který chystají útok. Využívají metod sociálního inženýrství (více v kap. 3.2.2) a počítačová a fyzická bezpečnost opravdu nejsou jediným způsobem, jak citlivá data ochránit.

IBP a sada navazující dokumentace je jádrem řešení bezpečnosti informací, které je nutno vždy navrhnout individuálně podle konkrétních firemních podmínek. Organizace by se proto podle společnosti NeXA (www.nexa.cz) měly vyvarovat:

- přebírání IBP jiné firmy,
- nereálné IBP (chtít nemusí znamenat možnost či schopnost realizace dané BP),
- IBP plné kompromisů,
- neúčinné propagaci (podcenění významu a způsobu prezentace IBP v organizaci).

Jako přínosy IBP a následně celého ISMS můžeme uvést např. snížení zranitelnosti společnosti, připravené náhradní řešení v případě incidentu, postupy podle metodiky a jiné případy. Po schválení IBP nastává etapa její implementace, ke které je třeba znalostí a schopností – „know-how" v podobě standardů a směrnic.

2.3 Bezpečnostní směrnice, standardy a legislativa

Bezpečnostní standardy, směrnice a legislativa jsou důležitou součástí IB, která sjednocuje formu příslušných bezpečnostních opatření a přístupů, a tak usnadňuje komunikaci mezi odborníky na celém světě. Vysoká míra současné standardizační aktivity a následná harmonizace přispívá k prohlubování informační bezpečnosti a promítá se i do českého prostředí.

Standardy (normy) jsou publikované dokumenty vytvořené na základě dohod, zahrnují technické specifikace nebo jiná přesná kritéria uplatňovaná jako pravidla. Zatímco **směrnice** jsou jisté definice, které zaručují, že materiály, produkty, procesy a služby splní svá poslání.

Na Českou republiku, jakožto člena EU, se vztahují legislativní předpisy Evropské unie, které mají podobu tzv. směrnic a nařízení. Mezi nejdůležitější předpisy pro oblast informační bezpečnosti patří:

- **Směrnice rady 1991/250/EHS,** o právní ochraně počítačových programů
- **Směrnice 1995/46/ES,** o ochraně osobních dat
- **Směrnice 1997/66/ES,** o ochraně dat v telekomunikacích
- **Směrnice 1999/93/ES,** o zásadách Společenství pro elektronické podpisy
- **Směrnice rady 2001/264/EC,** o ochraně utajovaných informacích
- **Nařízení 2001/45/ES,** o ochraně fyzických osob při zpracování osobních údajů orgány a institucemi
- **Směrnice 2002/58/ES,** o soukromí v elektronické komunikaci
- **Směrnice 2002/58/ES,** o zpracování osobních údajů a ochraně soukromí
- **Směrnice OECD pro bezpečnost informačních systémů a sítí: směrem ke kultuře bezpečnosti** (OECD Guidelines for the Security of Information Systems and Network: Towards a Culture of Security), která stanovuje devět zásad v oblasti bezpečnosti informačních systémů a sítí

Dále jsou zde uváděny nejdůležitější české právní předpisy vztahující k IB, které jsou na rozdíl od standardů a směrnic závazné. Východiskem pro zavedení ISMS je následující **národní legislativa**:

- Ústavní zákon č. **23/1991 Sb.**, kterým se uvozuje Listina základních práv a svobod - stanovuje základní pravidla pro nakládání s informacemi
- Zákon č. **148/1998 Sb.,** o ochraně utajovaných skutečností a o změně některých zákonů
- Zákon č. **106/1999 Sb.,** o svobodném přístupu k informacím
- Zákon č. **101/2000 Sb.,** o ochraně osobních údajů
- Zákon č. **227/2000 Sb.,** o elektronickém podpisu
- Zákon č. **365/2000 Sb.,** o IS veřejné správy
- Zákon č. **412/2005 Sb.,** o ochraně utajovaných informací a o bezpečnostní způsobilosti

Mezi nejdůležitější standardy patří:

- **BS 7799** – nejznámější britský bezpečnostní standard s celosvětovým rozšířením. Původně publikován v r. 1995, několikrát revidován:
    - **BS7799-1:1999** – Information Technology Code of Practice for Information Security Management (**ČSN ISO/IEC 17799:2000** - Katalog bezpečnostních funkcí a bezpečnostních opatření):

standard shrnuje praktické zkušenost s řešením IB, definuje 127 bezpečnostních funkcí rozložených do 10 oblastí - bezpečnostních zón

- **BS7799-2:2002** – Information Security Management Systems – Specification with guidance for use (**ČSN BS 7799-2:2004) -** Plán pro návrh celoživotního cyklu systému Outsourcing

Standardy plně pokrývají všechny bezpečnostní oblasti, popisují velký počet bezpečnostních opatření a jsou podporou pro výstavbu efektivní bezpečnostní politiky pro různé typy organizací. BS 7799-1 byl přijat jako mezinárodní standard **ISO/IEC 17799:2000** v prosinci 2000. Nejnovější verzí je **ISO/IEC 17799:2005 -** Soubor postupů pro management bezpečnosti informací. Národní bezpečnostní úřad považuje tuto normu za základní pro hodnocení a certifikaci informačních systémů, které zpracovávají informace podléhající zákonu o ochraně utajovaných skutečností. V komerční sféře je standard využíván jako základ pro hodnocení IB podnikových IS.

- **ISO/IEC TR 13335** (Information technology – Guidelines for the management of IT Security) - Informační technologie - Směrnice pro řízení bezpečnosti IT
- **ČSN ISO/IEC 15408 -** Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT
- **ČSN ISO/IEC 15816 -** Informační technologie - Bezpečnostní techniky - Bezpečnostní informační objekty pro řízení přístupu
- **ČSN ISO/IEC TR 14 516 -** Informační technologie - Bezpečnostní techniky - Směrnice pro používání a řízení služeb důvěryhodných třetích stran
- **ČSN ISO/IEC 9798 -** Informační technologie - Bezpečnostní techniky
- **ISO/IEC TR 19791** (Information Technology - Security Techniques - Security Assessment for Operational Systems) - Standard doplňuje rozsah normy ČSN ISO/IEC 15408 o další aspekty, které jsou převážně netechnologického charakteru jako např. personální bezpečnost, řízení konfigurací včetně řízení konfigurace bezpečnosti, bezpečnostní povědomí, testování, vedení dokumentace či podpora životního cyklu
- **ISO/IEC 18044** (Information technology - Security techniques - Information security incident management) - Řízení bezpečnostních incidentů. Cílem standardu je vymezit nejdůležitější kategorie bezpečnostních incidentů, stanovit typové postupy jejich řešení, vymezit role v procesu řešení incidentů a s nimi stanovit jejich pravomoci a odpovědnosti. Součástí standardu je i vzorová dokumentace pro vedení evidence bezpečnostních incidentů; aj. [38]

Dále je zde zmíněn dokument, který se týká naší republiky, která má svou strategii IB zakotvenu v *Národní strategii informační bezpečnosti* – ***NSIB*** z roku 2005. Vznik tohoto dokumentu byl iniciován novelou *„Státní informační a komunikační politiky: eČesko 2006"* a navazuje na dokument *„Bezpečnostní strategie ČR"*. Strategie je zpracována v rámci právní ochrany informací, na úrovni požadavků na IB stanovenou předpisy EU a doporučeními OECD s návazností na klíčové normy.

„NSIB ČR tvoří platformu pro budování důvěryhodné demokratické informační společnosti na právních základech, která dbá na zabezpečení informací ve všech oblastech lidské činnosti a umožňuje svobodně a bezpečně využívat a sdílet informace. Účelem NSIB ČR je ovlivnit zavádění nejlepší praxe a spolupráce všech subjektů společnosti při správě a budování důvěryhodných informačních a komunikačních systémů. Současně stanoví role a zodpovědnosti centrálních orgánů veřejné správy k podpoře ochrany informací". [47]

Tato strategie, jejíž základní prioritou je ochrana informačních a komunikačních aktiv před hrozbami prostřednictvím minimalizace rizik, bude brána jako podklad při tvorbě politik, směrnic, metodik, pravidel jiných dokumentů týkající se informační bezpečnosti.

Na závěr této kapitoly musíme dodat, že vytvořením IBP proces budování bezpečnosti nekončí, to nejdůležitější, a sice **implementace** a **následná kontrola**, je na privilegovaných zodpovědných osobách. Zaměstnanci by měli být řádně proškolováni (praktické ukázky, ne jen nudná teorie), popř. by měly být prověřovány jejich znalosti. Proces „učení" by neměl být jednorázovou akcí, ale měl by být prováděn průběžně, ruku v ruce s vývojem ICT a dle aktuálnosti problémů. Další významnou aktivitou je provádění **monitoringu** a získání zpětných vazeb, podle kterých se situace může efektivně vyvíjet dál. Vrcholem zavádění IB by měla být **certifikace celého ISMS**. Konkrétní zásady bezpečnosti „domácího" uživatele jsou uvedeny na konci následující kapitoly.

3 Elektronická informační kriminalita

EIK, jak již bylo naznačeno v úvodní kapitole, spočívá ve zneužití ICT k páchání trestných činů. Jedním z nejrychleji se vyvíjejícím typem informačního zločinu v kyberprostoru je krádež identity, zvaná phishing. Mezi další „top-ten" kybernetické zločiny řadíme internetové podvody, hacking, porušování AP, e-mailové hrozby, obtěžování a šíření dětské pornografie. Tyto delikty jsou nejčastěji páchány pomocí dvou běžných metod – **sociálního inženýrství** a **malware**, které ve své kombinaci mohou dosáhnout katastrofálních výsledků.

U EIK vyvstává **několik problémů**, které znemožňují její odhalení. Zaprvé, je to **prostředí**, ve kterém se odehrává. Kyberprostor je místem, kde neplatí žádná vynutitelná pravidla a kde jednotliví uživatelé mohou vystupovat pod různými identitami (nicky, čísla ICQ, e-maily, domény atd.) – které podle definice osobních údajů dle Zákona č. **101/2000 Sb.**, o ochraně osobních údajů [34], mohou být chráněnými údaji. Zadruhé, jde o samotnou **právní postižitelnost** prostředí. Jak uvádí SMEJKAL [122], tzv. **„počítačové právo"** (computer law) či **„informatické právo"** je průřezovou právní disciplínou, která se zabývá nejrůznějšími právními obory a odvětvími, spojenými jedním společným prvkem - počítačem, jeho obsahem (daty a programy) a jeho příslušenstvím. Toto odvětví se vytváří napříč klasickými právními disciplínami, protože zasahuje do veřejnoprávní i soukromoprávní sféry, do procesních norem, do teritoriálních i mezinárodních úprav, do občanského, obchodního, správního, trestního i dalších oblastí práva. V zahraničí se používá termín **„cyber law"** (kybernetické právo), a to zejména ve spojení s právem na internetu.

Internet jako takový, podle SMEJKALA [122], není subjektem práva – nemá právní subjektivitu, není ani ryze hmotným předmětem, ani čistě nehmotným statkem a dokonce není ani objektivní právní skutečností, nezávislou na lidském chování. Jde o informační a komunikační systém, který jako celek nemá svého majitele. **Subjekty** právních vztahů jsou v tomto případě uživatelé internetu, poskytovatelé služeb, vlastníci serverů a sítí apod. Právní vztahy při přenosu dat v internetu vznikají mezi jednotlivými provozovateli sítí, ale především mezi koncovými uživateli a providerem. V každé geografické oblasti existuje propojovací uzel, tzv. NIX – Neutral Internet eXchange, který toto propojení zabezpečuje. V naší republice je jím zájmové sdružení právnických osob *NIX.CZ*, jehož členy jsou významní čeští poskytovatelé připojení, tzv. Internet Service Providers (dále ISP). **Objekty** práva jsou hmotné i nehmotné objekty, chování, resp. výsledky určitého chování apod.

Z naznačených charakteristik internetu vyplývá jakási bezmocnost uchopit ho v rámci právního řádu. Proto se na internet pohlíží jako na přenosové médium - umožňující využívání poskytovaných služeb. Právní režim se řídí dvěma principy:

- prioritní **princip teritoriality**, který uplatňuje právo země, kde je služba poskytována (sídlo poskytovatele služeb, příp. umístění serveru),
- sekundární **princip práva upravující druh činnosti**, která je takto realizována, bez ohledu na médium (obchodní, občanský zákoník, autorský zákon apod.). Charakter internetového prostředí (globální, bez časových a prostorových hranic, anonymní aj.) však tuto situaci velmi komplikuje.

Vcelku zásadní problém, který nastává při **odhalovaní EIK**, představuje shánění důkazních prostředků, které by mohly sloužit k usvědčení pachatele. Digitální důkazy jsou totiž nehmotné a přechodné povahy. Situace je komplikována snahou pachatelů zahlazovat po sobě veškeré stopy, zejména v případě hackingu, využíváním anonymizérů[25] atd. Jako zdroje důkazních informací[26] v kyberprostoru můžeme využít:

- **e-mailové adresy** a další informace umístěné v hlavičce zprávy - received (server umístí do hlavičky název a IP adresu počítače, od kterého zprávu přijal),
- **WWW stránek** (obsah, doménové jméno),
- **serveru** (IP adresa) – záznamů providera (též lze zjistit uživatelské jméno, heslo aj. osobní údaje),
- **log soubory –** např. u služby přístupu k síti, u FTP,
- **diskusních skupin**, které využívají protokol NNTP[27]
- **přístupových čísel** – ze záznamů providera, ten je schopen podle IP adresy zjistit, na jaké telefonní číslo bylo voláno.

Některé země přijaly právní úpravu, která ukládá povinnost ISP uchovávat provozní data. Spolupráce ISP při vyšetřování a stíhání EIK může být pro policii apod. orgány neocenitelná. Další komplikace vzniká, když je EIK páchána přes více zemí (většina případů), tedy ISP, kteří nespadají do územní působnosti vyšetřovatele. Pak nastává nutnost mezinárodní spolupráce (více v kap. 4.3).

V případě, že pachatel využívá freemailových či freewebhostingových služeb (bez pevného připojení), je pátrání komplikováno. K tomu musíme ještě dodat, že i

25 Speciální programy pro anonymní přijímání a odesílání zpráv (remailery) či prohlížení webových stránek. Remailery tak mohou být zneužívány pro šíření pornografie, extremismu, porušování AP.

26 Zejména tzv. provozních údajů, v angl. traffic data.

27 Network News Transfer Protokol – protokol pro přenos síťových zpráv.

když se podaří zjistit identitu pachatele, není proces dokazování u konce. Je nezbytné prokázat, že daná osoba skutečně vytvořila a odeslala e-mail, příspěvek atd.

Tato kapitola, která je rozdělena do tří tematických celků (porušování AP, útoky na data a internetové obtěžování a podvody), popisuje jednotlivé formy páchání trestných činů, které byly popsány v kapitole o trestných činech (1.3). K nejpalčivějším analyzovaným problémům, které ohrožují uživatele, resp. jejich data uložená v IS, jsou připojena možná **preventivní opatření** a příslušné **skutkové podstaty** (tzv. subsumpce) podle české trestněprávní úpravy, pokud existuje. Stane-li se, že v českém právním řádu není daný jev uveden, nezbývá než konstatovat, že není považován za trestný čin (podle zásady nullum crimen nulla poena sine lege – není zločinu ani trestu bez zákona). [85] V případě, že se k určitému jevu vztahuje činnost konkrétní instituce, jsou zjištěné skutečnosti zmíněny.

3.1 Porušování autorských práv

Předmětem práva autorského jsou díla literární, vědecká a umělecká, která jsou výsledkem tvůrčí činnosti autora, zejména díla slovesná, divadelní, hudební, výtvarná včetně děl umění architektonického a děl umění užitého, díla filmová, fotografická a kartografická a to v jakékoli vnímatelné podobě včetně podoby elektronické. Za předmět ochrany se považují i programy počítačů, pokud splňují pojmové znaky děl podle tohoto zákona; nestanoví-li tento zákon jinak, jsou chráněny jako díla literární.

§2 odst. 1 AutZ

Porušování AP a práv souvisejících s právem autorským je především **občanskoprávní delikt**, podle okolností však může naplnit znaky skutkové podstaty trestného činu porušování AP, práv souvisejících s právem autorským a práv k databázi podle **§152 TrZ** nebo přestupku na úseku kultury podle **§32 Zák. č. 200/1990 Sb. o přestupcích**. [28]

Z výše uvedené definice AutZ vyplývá, že ochrana a potažmo pirátství se může týkat jak **SW** (rozmnoženiny nebo kopie bez souhlasu autorů jsou porušením AP, platí výluka volného užití), tak děl **hudebních** a **filmových** (zhotovování rozmnoženin těchto děl a záznamů lze jen s výslovným souhlasem nositelů práv uděleným licenční či smlouvou, pokud nejde o zhotovení jediné kopie pro osobní potřebu), **databází** (chráněny od 1.12.2000 a obdobně jako u SW nelze pořizovat rozmnoženiny bez souhlasu pořizovatele databáze, s ohledem na **§88** a **§30** odst. 1 AutZ není možné zhotovit záložní kopii podstatné části databáze bez souhlasu jejího pořizovatele) i **WWW stránek**. Stimulem pro **masové porušování AP** se stal bezesporu internet a jeho služby, díky němuž padají veškeré bariéry. Zároveň je prostředím, které poskytuje nepřeberné množství různých pomůcek k překonání ochrany proti

kopírování (generátory sériových čísel, nebo tzv. cracky), návody pro hacking (zkušenosti nasdílené v rámci hackerské etiky) atd.

Problematika se týká zejména **majetkových práv** AutZ, a to práva dílo **užít** (§12), které rozeznává dále právo dílo **šířit** (§13) a **rozmnožovat** (§14), dále právo **volného užití** (§30), **ochrany** díla (§43-44), a počítačových programů (§65-66).

3.1.1 Softwarové, hudební a filmové pirátství

Pod pojmem **pirátství** chápeme neoprávněné nakládání s dílem, které je předmětem ochrany podle AP, či práv souvisejících s právem autorským. Základní trestní odpovědnost za tuto činnost je dána **§152** TrZ - porušování autorských práv. LÁTAL [73] k tomu dodává, že při realizaci pirátství přichází v úvahu uplatnění i dalších ustanovení trestního zákona a to: **§150** TrZ - porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu a **§149** TrZ - nekalá soutěž (vyrobený a distribuovaný plagiát parazituje na dobré pověsti oficiálního výrobce).

Softwarové pirátství je pravděpodobně nejproblematičtější oblastí neoprávněných zásahů do autorského díla. Každý uživatel počítače si shání SW dle svého zájmu, upotřebení a pochopitelně též finančních možností. Ač jsou k některým typům SW dostupné bezplatné alternativy v podobě shareware, freeware apod., existují kromě vysokých finančních nákladů určité pohnutky (naznačeny v kapitole o motivaci pachatelů), které přesto vedou k softwarovému pirátství. Počítačovým programem nemáme na mysli jen různé kancelářské aplikace, rozmanité utility pro práci s grafikou, ale také hry, které jsou častou obětí softwarového pirátství u dětí. Dalším oblíbeným artiklem, který se ocitá ve spárech pirátství jsou **hudební** (nejčastěji v komprimovaném formátu MP3) a **filmová** díla (formát AVI, DivX apod.).

Vyrobit, resp. zkopírovat nelegálně kopii SW, hudby či filmu není v dnešní době žádný problém. Běžnému uživateli stačí pouze vypalovací mechanika a paměťové médium, což je v současnosti cenově dostupné vybavení. Jde o zcela běžné praktiky mezi studenty či zaměstnanci, kdy jsou mezi kamarády získávány a šířeny nelegální kopie různých aplikací, her, filmů, souborů MP3 apod. Dále dochází k závažnější trestné činností, a to k **průmyslově výrobě**, kdy pachatelé potřebují speciální vybavení k padělání daného SW či hudebních a filmových nosičů a následně ho různými způsoby prodávají. Snahou takového výrobce je vydávat svůj produkt za originál (tzv. padělky) a zmást tak uživatele (hologramy, balení, registrační karty). Těm ale musí být jasné, že nízká cena jinak drahého produktu a neautorizovaný prodejce v sobě skrývá nějakou nekalou činnost. Řešením jednoznačné identifikace výrobce je jeho povinnost označovat své produkty unikátními kódy.

Počítačový program je jako ostatní díla chráněn autorským zákonem, podle kterého lze SW **užívat** (až na některé výjimky) pouze se svolením autora na základě licenční smlouvy. **U neoprávněného užívání softwaru** je možno rozlišovat, zda program používá nějaký jedinec doma pro svou **soukromou potřebu** (nejrozšířenější forma), či jde o užívání softwaru **za účelem zisku** v rámci své komerční činnosti. Výsledkem ale vždy je, že tato nelegální aktivita uživateli přináší zisk, a to částku, kterou by za daný software zaplatil, kdyby si ho řádně koupil. Porušení AP nevýdělečným používáním nelegálního SW pro osobní potřebu je typově nejméně společensky nebezpečnou formou. Podle studie Ministerstva vnitra [31] může být v některých případech **paradoxně** docíleno jak zisku výrobce dotyčného SW, tak uživatele nelegálního SW. Např. nelegálně nainstalovaný SW v učebnách vzdělávacích zařízení může být pro jeho výrobce úspěšnou reklamou. Jeho uživatelé se s ním naučí pracovat, oblíbí si ho a budou ho dále propagovat.

Konkrétními případy neoprávněného používání SW mohou být situace, kdy si uživatel pořídí nelegální kopie SW a ty pak používá, příp. legálně získaný SW (originál) používá ve více instalacích - než je ustanoveno v licenčním ujednání - či využívání nabídek na upgrade bez legální kopie. V následujícím odstavci je uvedeno sdružení specializující se na problematikou nelegálního SW, které zastupuje zájmy světových výrobců SW (např. Adobe, Microsoft, Software 602, Autodesk, Novell aj.). A tím je nechvalně známá ***BSA (Business Software Aliance)***

BSA
BUSINESS SOFTWARE ALLIANCE

Zabývá se, dle popisu na svých webových stránkách (www.bsa.org), prosazováním bezpečného a legálního prostředí v digitálním světě. Je mluvčím světového komerčního softwarového průmyslu směrem k vládním organizacím a na mezinárodních trzích. BSA vzdělává spotřebitele v oblasti řízení SW a ochrany AP, kybernetické bezpečnosti, obchodování, e-commerce, a v ostatních záležitostech souvisejících s internetem. BSA rovněž vede vzdělávací projekty pro mládež zaměřené na ochranu duševního vlastnictví. Patří k nim iniciativa na posílení zodpovědného přístupu k práci s internetem na www.netrespect.ie v Irsku, společný program škol a průmyslových subjektů v Itálii přístupný na www.controlapirateria.org a nedávno představený projekt oceňování výzkumných prací zaměřený na univerzitní studenty v Německu.

Ani samotní výrobci SW boj proti pirátství nevzdávají. Jmenujme např. aktuální osvětový program *„Výhody legálních Windows"* (*Windows Genuine Advantage Notification*). Jde o nástroj dostupný pomocí automatických aktualizací, který informuje uživatele o možnostech legalizace OS Windows XP. Windows Update nabízí nástroj jako volitelný doplněk, z kterého se však stane povinná komponenta. V případě, že utilita rozezná pirátskou nelegální kopii, bude uživateli nabízet legalizaci

OS (přesměrování na www.microsoft.com) v podobě OEM licence[28] či přímo zakoupení licence on-line. Pirátský systém bude do doby koupi licence upozorňovat uživatele o užívání nelegálního systému hláškou v přihlašovacím okně (příloha č. 2) a v systémové liště ikonkou  . Jde však spíše o psychologický nátlak na uživatele, neboť těchto alarmujících apelů se dá lehce zbavit (odinstalování zmíněného nástroje v podobě poslední aktualizace či stažení cracku, který se na internetu objevil velmi rychle). V loňském roce byl tento program ve zkušebním provozu přístupný na WWW stránkách MS. Během jednoho roku si v České republice více než 400 000 návštěvníků *MS Download* své OS Windows dobrovolně ověřili. Z ověřovaných Windows tvořily nelegální kopie přibližně 40%[29].

S pirátstvím je neodmyslitelně spjata problematika výroby a užívání tzv. **cracků** (§43 TrZ). Tímto pojmem rozumíme program, který umožňuje plně funkční užívání časově omezeného nebo jinak chráněné aplikačního programu nebo hry. **Cracking** je tedy zásah do programu, který umožní obejít jeho ochranu proti kopírování či neoprávněnému užití. Tato činnost, která úzce souvisí s problematikou warezu a hackingu, je zpravidla páchána z důvodu umožnění distribuce nelegálních kopií či neoprávněné užívání SW. Kromě cracků je na internetu také zveřejňováno velké množství sériových čísel (např. www.serials.com, www.serials.ws, www.t1000.net aj.) k nezměrnému počtu programů, po jejichž zadání se program stává plně funkční. [31] Někteří právní experti jsou toho názoru, že jakákoli modifikace SW je vždy nezákonná, a to i tehdy, kdy byl daný SW řádně zakoupen a crack byl použit pouze z důvodu ztráty licenčního čísla či instalačního CD s plnou verzí. Což je poměrně diskutabilní.

3.1.1.1 Warez

Fenomén **warezu** je výsledkem nástupu moderních ICT, a to především internetu. Zatímco do nástupu warezu se jednalo i izolované obory pirátství v oblasti SW, hudby a videa, díky rychlé přenosové kapacitě internetu a stále se zdokonalujícím kompresním formátům dat spolu se zařízením pro jejich uchovávání se dnes spojují všechny tyto tři činnosti do jedné. Před nástupem internetu vycházely releasy[30] na disketách, s rozvojem CD technologie na CD-ROMech (formát CD-Image, který je znám jako ISO). Začaly se dělat „očesané" verze ISO her, které nyní známe pod názvem **RIP.** Představitelé všech tehdejších významných skupin, které ovládaly warez scénu, přistoupili k rozhodnému kroku a dohodli se na jednotných pravidlech, tzv.

28 Original Equipment Manufacture - plnohodnotné produkty přeinstalovanými výrobci počítačů na nových počítačích a dodávanými za cenově velmi zajímavých podmínek.

29 Zdroj: http://zive.cz/h/Viryabezpecnost/AR.asp?ARI=128498.

30 Výsledný produkt – hra, video, mp3 či aplikace - warez scény.

releasing rules, určujících, v jakém formátu a jakým způsobem se bude oficiálně warez vydávat – releasovat, čímž došlo ke sjednocení warez scény.

Princip warez scény je postaven na bázi **„non-profit"**. Drtivá většina lidí toto pravidlo respektuje a chová se podle něj. Jediné co jednotlivec nebo skupina získají, je **respekt konkurenčních skupin** v případě kvalitních výsledků. Warez bývá doménou skupin, které se vyznačují poměrně vysokou mírou specializace a dělby práce. V každé takové skupině většinou bývá jeden či několik crackerů, kteří se zabývají obcházením ochrany proti kopírování zabudované v programech. Další se věnují propagaci, tvorbě WWW stránek s upoutávkami na své „produkty", tvorbou katalogů, které jsou rozesílány, reklamních letáků atp. [85] Šíření warezu probíhá většinou následujícím způsobem. V momentě, kdy se na trhu objeví nějaká očekávaná verze komerčního SW či filmu, využije warezová skupina svých kontaktů u nahrávacích, filmových či softwarových studií. Následně produkt předá zkušenému programátorovi k odstranění ochrany proti kopírování a takto upravený warez je předán tzv. kurýrovi, který ho rozšíří. Výsledkem je objevení se kopie produktu na trhu ve stejný den jako originál, či ještě dříve.

Pro zajímavost jsou zde uvedeny příklady možností[31], jak zhotovit kopii filmových děl v digitálnímu formátu, který je vhodný pro vypálení a následnou distribuci prostřednictvím internetu. Jde o následující formy, resp. zdroje vytvoření:

- CAM – rip vytvořený digitální kamerou přímo v kině, zvuk je nasnímán pomocí mikrofonu umístěného přímo v kameře (kvalita zvuku i obrazu většinou na špatné úrovni),
- TELESYNC (TS) – stejné jako u CAM kromě zvuku, ten je použit z externího zdroje,
- TELECINE (TC) - přístroj, který nasnímá film přímo z filmových kotoučů - obraz i zvuk velmi kvalitní,
- SCREENER (SCR) – propagační materiál na VHS kazetě, film obsahuje tzv. tricker, což je nápis upozorňující diváka na zákaz kopírování, objevuje se v určitých intervalech, obraz bývá místy černobílý,
- DVD SCREENER (DVDscr) – stejný princip jako u SCR, s tím rozdílem, že zdrojem je DVD,
- DVDRip – kopie klasicky prodávaného DVD, excelentní kvalita (podobné u VHSRip a TVRip, ale se sníženou kvalitou),
- DivX – film vzniklý překódováním VideoCD do malého Divx filmu, vhodného k šíření po P2P,
- WORKPRINT (kopie nedokončeného filmu) aj.

Technicky zdatní piráti jsou schopni opatřit originální film titulkami požadované jazykové verze (různorodá kvalita).

31 Zdroj: http://www.shareforum.net/modules.php?name=News&file=article&sid=21.

Na scéně existuje několik desítek skupin, které mezi sebou bojují. Každý release se boduje a body se rozdělují do žebříčku. **Hodnocení** probíhá tak, že se počítá prvních dvacet míst, konkrétně za 1. místo se dává 20 bodů, za 2. místo 19 bodů atd. Počet bodů se dále vynásobí rankingem severů. Nakonec se sečtou výsledky jednotlivých serverů a statistiky jsou hotové. Protože každá skupina chce být co nejlepší, probíhá týden co týden těžký souboj o dosažení co nejlepšího místa. [134]

V dřívějších dobách se warez **šířil** prostřednictvím klasické poštovní služby, tajných FTP serverů, sítí IRC či WWW stránek. Po nástupu sítí P2P a vzniku příslušných programů ztrácí WWW stránky - jako způsob šíření warezu – na významu, uživateli nabízí „pouze" cracky či ho zahltí nepřeberným množství reklam, falešných odkazů a pop-up oken, které návštěvníka přesměrují většinou na pornostránky s placeným přístupem. Tímto způsobem je často generován zisk, v případě, že se uživatel zaregistruje a zaplatí registrační poplatek. [85]

3.1.1.2 P2P

Nejrozšířenějším distribučním kanálem nelegálního SW, hudebních a filmových děl je pochopitelně v současné době internet. Programy a hudební či filmové soubory jsou buďto umisťovány na zahraniční anonymní FTP servery (mimo dosah české legislativy) a uživatelům je za poplatek poskytováno heslo pro přístup a následné stáhnutí SW. Mnohem populárnější formou pro sdílení nelegálního obsahu jsou tzv. **peer-to-peer sítě - P2P** (opak architektury klient-server). Oblíbenost výměnných sítí spočívá v tom, že s rostoucím množstvím uživatelů celková dostupná přenosová kapacita roste, zatímco u modelu client-server, kdy se uživatelé musí dělit o konstantní kapacitu serveru, průměrná přenosová rychlost při nárůstu uživatelů klesá.

Tyto výměnné sítě vyhledávají a užívají osoby, které zde shromažďují nelegální obsah s cílem umožnit jeho volné kopírování. Cílem tohoto jednání není zisk ani jiný osobní prospěch, ale například snaha o **volnou dostupnost** jinak drahých programů, hudebních skladeb či filmů jako projev svérázné životní filozofie. Uživatel, který se chce stát součástí takové sítě, si musí nainstalovat program, díky němuž se jeho počítač změní v server, který sdílí svůj adresář s hudebními skladbami ve formátu MP3, filmy či SW s ostatními uživateli. Tyto programy pro sdílení souborů jako např. *Direct Connect (DC, DC++), BitTorrent, WarezP2P* aj. umožňují vyhledávání podle jména, žánru či klíčového slova týkající se AVD či SW. Odhaduje se, že na internetu se nachází téměř miliarda nelegálně nasdílených hudebních skladeb.

Dnešní anonymní výměnné sítě umožňují (legální i nelegální) výměnu souborů s prakticky nulovou mírou odpovědnosti jednotlivých uživatelů. Dochází však k žalobám (zejména v USA) na provozovatele takovýchto sítí, které podávají zástupci

autorů a organizace jako je *RIAA* či *MPAA* (více v kap. 4.2.1). Jako příklad můžeme uvést rozhodnutí amerického Nejvyššího soudu z června loňského roku, podle kterého byli provozovatelé sítí P2P služby *Grokster* a *StreamCast* zodpovědní za porušování AP jejich uživateli. RIAA ihned reagovala rozesláním dopisů sedmi dalším provozovatelům P2P sítí, ve kterých je nabádá k ukončení své činnosti. [126] Prezident RIAA *Cary Herman* přišel s novým označením pro ty, kteří si nelegálně stahují hudbu, a sice „songlifter" (odvozeno z „shoplifter", označení pro zloděje v obchodě).

Problémem jsou omezené možnosti provozovatelů výměnných sítí kontrolovat, co se na nich děje. Studia si mohou zjistit pouze IP adresu piráta, ne jeho totožnost. Tu zná pouze provozovatel sítě, který je ale vázán mlčením dle telekomunikačního tajemství, sdělit ji smí až na příkaz soudu. Pochopitelně by bylo možné obvinit samotné tvůrce těchto programů, což by vyhovovalo filmovým a nahrávacím studiím, kterým by se zjednodušil postih viníka a vymáhání škody. Programátoři se ovšem případnému postihu brání tím, že ve stanovách k programům uvádí, že program je určen výhradně pro použití s legálně zakoupenými daty, a že tedy jen uživatel je odpovědný za porušení zákona. Tato situace vyžaduje změny v uplatňování a vynucování autorského práva. [72]

Výměnné sítě však mohou sloužit i k jiným účelům než jen ke stahování nelegální hudby, SW či filmů. Mohou být využívány jako úložiště velkých souborů, které by např. nebylo možno poslat jako přílohu e-mailu, či k distribuci shareware, různých dokumentů apod. Jako příklad z našeho prostředí můžeme uvést zpřístupnění alba Jaromíra Nohavici *„Pražská pálená"* přes výměnnou síť **BitTorrent**. Jedná se o maximálně decentralizovanou síť, vytvořenou původně pro zcela legální účely, což se velmi rychle změnilo. K vyhledávání souborů slouží internetové stránky a samotné stahování se realizuje v okně internetového prohlížeče. Specifikem této sítě je, že její autor *Bram Cohen* uzavřel dohodu s filmovou organizací MPAA, že nebude přes svůj server (tracker) šířit tzv. torrenty (seznamy toho, co uživatelé sítě nabízejí ke stažení) na díla autorů, které tato organizace zastupuje.

Paradoxně výměnné sítě čelí nejen právním ale i **přímým útokům.** Mezi slabiny P2P sítí a metody útoků patří např. DoS útoky, počítačové viry, spam (více v kap 3.2). P2P sítě pravděpodobně úplně nezaniknou, ale je pravděpodobné, že budou - tak jako již v úvodu zmíněný *Napster* - transformovány na univerzálnější, průhlednější a autorům vydělávající služby. Některé hudební a filmové společnosti si uvědomily, že jejich boj proti pirátství je marný a mění proto svou obchodní strategii. Produkty zlevňují a nabízí je ke stažení legální cestou - za poplatek přes internet (např. *iMesh, Altnet, Napster2, iTunes* či český server *Starzone.cz*). Některá

hollywoodská filmová studia zpřístupní vybrané filmy pro online stahování. Existují dva provozovatelé, kteří takové stahování filmů umožňují – *Cinema Now* a *Movielink*.

Trestněprávní úprava

Většina západních zemí posuzuje tvorbu a distribuci warez za nelegální činnost, země třetího světa ji naopak považují buď za zcela legální, nebo přinejmenším volně trpěnou až zcela ignorovanou. V naší republice je kopírování a šíření autorských děl bez povolení autora trestný čin podle **§152** TrZ - porušování autorského práva, práv souvisejících s právem autorským a práv k databázi. **Použití** (konzumace, zhotovení záznamu, rozmnoženiny – stažení z internetu[32]) jiného autorského díla než programu či elektronické databáze pro **vlastní potřebu** (podle §30 AutZ) je však v ČR legální i bez svolení autora. Tedy např. stažením filmu a jeho užitím pro vlastní potřebu není český zákon porušen, třebaže film či hudba jsou šířeny v rozporu se zákonem. Kompenzace autorům za užití pro osobní potřebu spočívá v paušálních platbách. Ty je povinen platit každý výrobce či dovozce strojů a přístrojů pro rozmnožování zvukových či filmových nahrávek, nahrávacích nosičů apod. tzv. kolektivnímu správci – organizaci, která vybrané poplatky spravuje a rozděluje autorům. V praxi je proto součástí ceny každého prázdného CD, DVD, vypalovacího zařízení drobná platba kolektivnímu správci práv. Ovšem v případě **zpřístupňování** hudebních či filmových děl prostřednictvím internetu (vystavování, sdílení) se jedná o porušení AutZ. **Kopii SW** si uživatel může vyrobit pouze v případě, že bude sloužit jako záložní zdroj. Legálnost kopie je dána tím, že spolu s ní uživatel vlastní i originální instalační CD.

Porušování AP na internetu je díky rychlému a zároveň levnému připojení a cenovým politikám vydavatelství audia, videa a SW opravdu velkým problémem, a to na celém světě. Můžeme se domnívat, že zabránit užívání nelegálních kopií autorských děl je zatím zcela nemožné. Dá se předpokládat, že i kdyby cena veškerého SW, hudebních a filmových děl klesla na přijatelnou míru a originální nosiče byly „zabezpečeny" ochranou proti kopírování, vždy se najdou uživatelé, kteří budou o krok napřed a pirátství bude žít dál. I v případě, že by jednoho dne došlo k uzavření všech klientů P2P sítí (což už je jenom pro možnost šíření legálních aktivit zcela nelogické), stále existuje možnost distribuovat ilegální obsah prostřednictvím e-mailů, ICQ či umístění na FTP server. Jde o určitý druh adrenalinového sportu, který je navíc natolik ekonomicky zajímavý (téměř nulové investice), že prosté potrestání jedinců, kterým je prokázáno úmyslné porušení zákona, stěží odradí další pachatele od této činnosti.

32 Na konkrétní službě nezáleží, může jít o WWW stránku, FTP server, P2P sítě.

3.1.2 Neoprávněné zásahy do autorského díla

Jako neoprávněný zásah do autorské díla řadíme dle AutZ **§43** již zmíněné **cracky,** které slouží k překonání ochrany. Poměrně velké množství crackerů pochází ze zemí bývalého východního bloku, neboť zde se v minulosti ani originální SW sehnat nedal. O nelegálnosti crackingu není pochyb, ale do jisté míry jde o činnost, díky níž je daný výrobce SW propagován (uvažujeme-li, že jinak by si uživatel SW nezakoupil). K prolamování ochran SW se využívá vhodných nástrojů typů debugger nebo disassembler (např. *Turbo Debugger, SofIce* atd.).

Dalším typem překonávání důkladnější ochrany, a to tzv. hardwarového klíče, který je implementován u dražších programů jako např. *AutoCAD*, se využívá tzv. **reverse ingeneering** (zpětná dekompilace systému).

Jako mediálně známé příklady překonání ochrany můžeme jmenovat kauzu z roku 2000, kdy byla vyvinuta utilita *DeCSS* na dekódování DVD, která umožnila přehrávat filmy i na počítači OS Linux. Další případ je z roku 2005, kdy jistý programátor, pod přezdívkou *tj21*, dokázal zlomit ochranu DRM[33] (Digital Rights Management), kterou jsou zabezpečeny videonahrávky ve formátu WMV. Podobné typy ochran jsou v oblasti kopírování informací prioritním tématem. Na zahraničním i našem trhu jsou dostupné speciální časopisy, které se této problematice věnují. Princip ochrany spočívá v přehrání obsahu média bez možnosti vytvoření jeho kopie. Dle BEDNÁŘE [6] jde o dopředu prohraný boj. Technologie jako *Cactus Data Shield* či *Key2Audio* sice zabrání do jisté míry vytvoření identické kopie CD, ale na druhé straně je ignorován zásadní fakt. Zvukové či obrazové informace jsou analogové rázu a i kdyby se podařilo zabránit digitálnímu kopírování, s finálním zobrazením nelze dělat nic.

Další oblastí, kterou bychom mohli zahrnout do této kategorie jsou **WWW stránky**, neboť jde o díla, která jsou výsledkem jedinečné tvůrčí činnosti autora a mohou být chráněna AutZ. Webové stránky mají dvě podoby, jednak samotný **zdrojový kód** (HTML, PHP atd.), jednak **cílovou podobu**, kterou uživatel vidí v prohlížeči (design i obsah). V mnoha lidech přetrvává chybné povědomí, že to co je „na internetu" je zadarmo a neplatí zde žádné legislativní omezení. Zcela suverénně kopírují jednotlivé části WWW stránek (grafiky, texty atd.) či celý design.

Podle **§44** AutZ sem dále můžeme zahrnout **zásahy do WWW stránek** hackery, kdy dojde k pozměnění zdrojového kódu původní stránky (tzv. defacement). Tomu předchází trestný čin neoprávněného průniku (více v kap. 3.2.2). Mezi typické

[33] Systémy, které mají za úkol ověřovat platnost licencí pro digitální informaci. Jsou založeny na šifrování, ověřování e-podpisů, časových a HW omezeních. Mají umožnit bezpečné šíření hudebních a filmových děl a SW.

zásahy, které jsou podle **§257a** TrZ klasifikovány jako trestný čin poškození a zneužití záznamu na nosiči informací, patří vymazání částí textu, grafiky či nahrání celé nové stránky apod. Druhy napadených subjektů jsou různorodé, od vzdělávacích a bankovních institucí až po ministerstva. Způsobená škoda závisí na frekvenci a účelu využívání webových stránek.

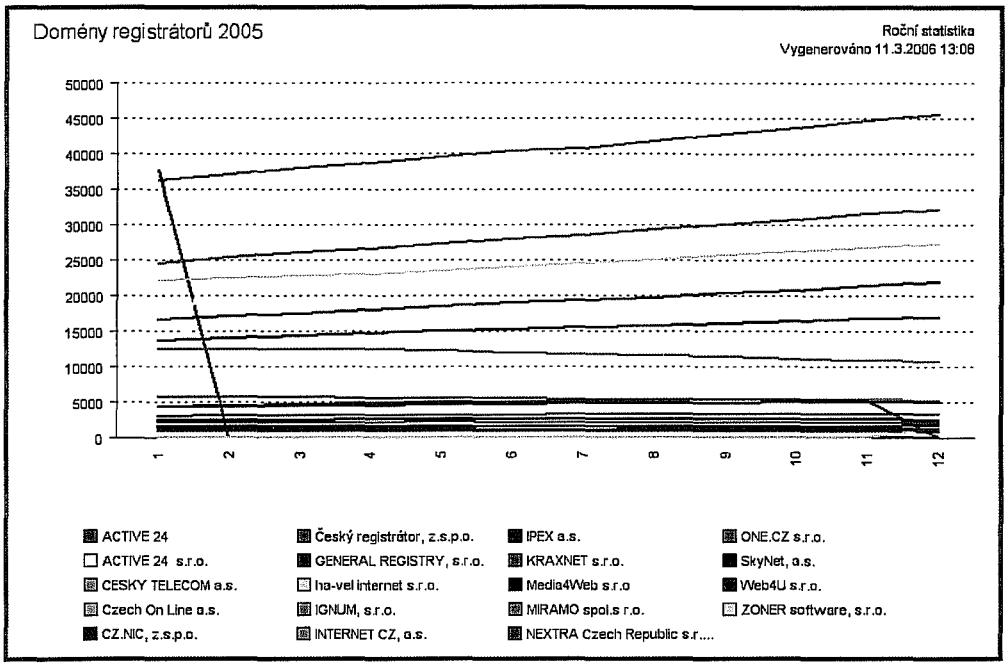
3.1.3 Cybersquatting

Další oblastí porušování AP, kde může být páchána informační kriminalita jsou **jména domén v internetu**. Aby bylo možné jednoznačně identifikovat a adresovat každý z mnoha miliónů počítačů připojených k internetu, bylo třeba přidělit jednotlivým serverům určité adresy a tyto adresy hierarchicky uspořádat do tzv. domén[34]. **Domény nejvyšší úrovně** (top-level domain) jsou tzv. generické - označeny známými koncovkami:

- .com (komerční),
- .org (organizace),
- .gov (vládní),
- .mil (vojenské),
- .edu (vzdělávací),
- .aero (letečtí dopravci),
- .pro (právníci, lékaři, architekti a jiné profese),
- .museum (muzea a galerie) aj.

nebo národní domény, které jsou přiděleny na základě názvu státu. Pro jednotlivé generické domény platí různá registrační pravidla a procedury, které má na starosti centrální doménová autorita *ICANN*[35]. [101] Národní doménu .cz a tedy i její registraci u nás spravuje zájmové sdružení právnických osob *CZ.NIC* (*Network Information Center*). V následujícím grafu (obr. č. 3) je zobrazen počet zaregistrovaných domén v loňském roce a nejvýznamnější poskytovatelé jejich provozu.

[34] Základní adresní jednotka, která reprezentuje konkrétní IP adresu – převod via DNS (více v kap. 3.2.2).
[35] Internet Corporation for Assigned Names and Numbers.



Obr. č. 3– Domény registrátorů 2005, převzato z http://www.czechia.cz

Domény druhé úrovně (např. mvcr.cz nebo seznam.cz) určují rozdělení serverů na daném území. Způsob, jakým jsou na území každého státu přidělována jména právě těchto domén druhé úrovně, má velkou důležitost pro využívání internetu v dané zemi. **Domény třetí** a další úrovně umožňují další specifikace využití (např. reality.centrum.cz).

Česká legislativa nestanovuje žádná pravidla pro registraci doménového jména, přidělování funguje na základě systému "kdo dřív přijde". Doménové jméno je přiděleno prvnímu žadateli. Na existenci jiných práv se nebere ohled. Rozhodující je okamžik přijetí žádosti. Subjekt, který podá žádost o doménu a je mu přidělena, k ní má vlastnická práva a povinnosti. Registrace probíhá podle podmínek zveřejněných na webových stranách www.nic.cz pomocí smlouvy o registraci doménového jména. Tato situace s sebou přináší řadu konfliktních situací - není totiž stanoven právní režim domény. [85] Existují sice dokumenty společné politiky *„Request for Comments"* *(RFC)*[36], nezbytné pro fungování internetu, nutno ovšem říci, že takováto doporučení nejsou obecně závazná a jejich dodržování není vynutitelné. [122]

Jednoduchá a zejména snadno zapamatovatelná doména se při dnešní nezbytnosti registrace firem na internetu stává cenným artiklem. Stále se zvyšující počet subjektů prezentujících se na internetu vyvolává spory mezi zájemci o atraktivní domény. Může jít o dvě rozdílné firmy s rozdílnou oblastí služeb, dokonce i

36 Vydavatelem je Internet Engineerig Task Force, navrhovatelem může být kdokoliv. Obsahem RFC specifikací jsou nejen standardy, ale i návody, doporučení atd. týkající se internetu.

z jiného regionu, ale se stejným nebo podobným jménem. Nebo i o dvě obce se stejným jménem, třeba z opačného konce republiky. Vznikající spory o domény lze rozdělit na spory se **spekulanty** (doménu zaregistruje subjekt, který k ní nemá žádný vztah v úmyslu ji později se ziskem prodat) a spory s **konkurenty** (spor se seriozním zájemcem o doménu, který má zájem registrovanou adresu využívat).

V **České republice** je v Obchodním rejstříku zapsáno přes 200 000 právnických osob, ale domén byla registrován doposud čtvrtina[37]. Pravidlem bývá, že jedna firma má zaregistrováno více domén (pro firemní stránky, produkty nebo budoucí aktivity). Vhodné také bývá zaregistrovat jméno lehce zaměnitelné s konkrétní doménou, či doménové jméno s překlepy. Těchto „doporučení" využívají ve svůj prospěch tzv. squatteři (doménoví piráti, spekulanti).

Pod pojmem **Cybersquatting** či také **Domain Name Grabbing** rozumíme zaregistrování doménového jména shodného nebo zaměnitelného se známými ochrannými známkami či významnými firmami. Majitel nově získaných domén potom spekuluje s tím, že doménu s nemalým ziskem prodá majitelům ochranných známek či firem. Dnes již tato činnosti ustupuje do pozadí, neboť svůj „boom" zažila v době, kdy firmy na internet teprve vstupovaly. Ale stále najde své opodstatnění např. při uvádění nového produktu na trh, kdy jsou **squatteři** rychlejší než výrobci produktu, kteří jsou pak nuceni od nich doménu odkoupit za nepřiměřeně vysoké částky. Dalšími formami doménového pirátství jsou podle MATĚJKY [85] různá nekalosoutěžní jednání, kdy dochází např. k parazitování na pověsti, pokud si někdo založí stránku se jménem věhlasného produktu a provozuje na ní svůj internetový obchod apod.

Trestněprávní úprava

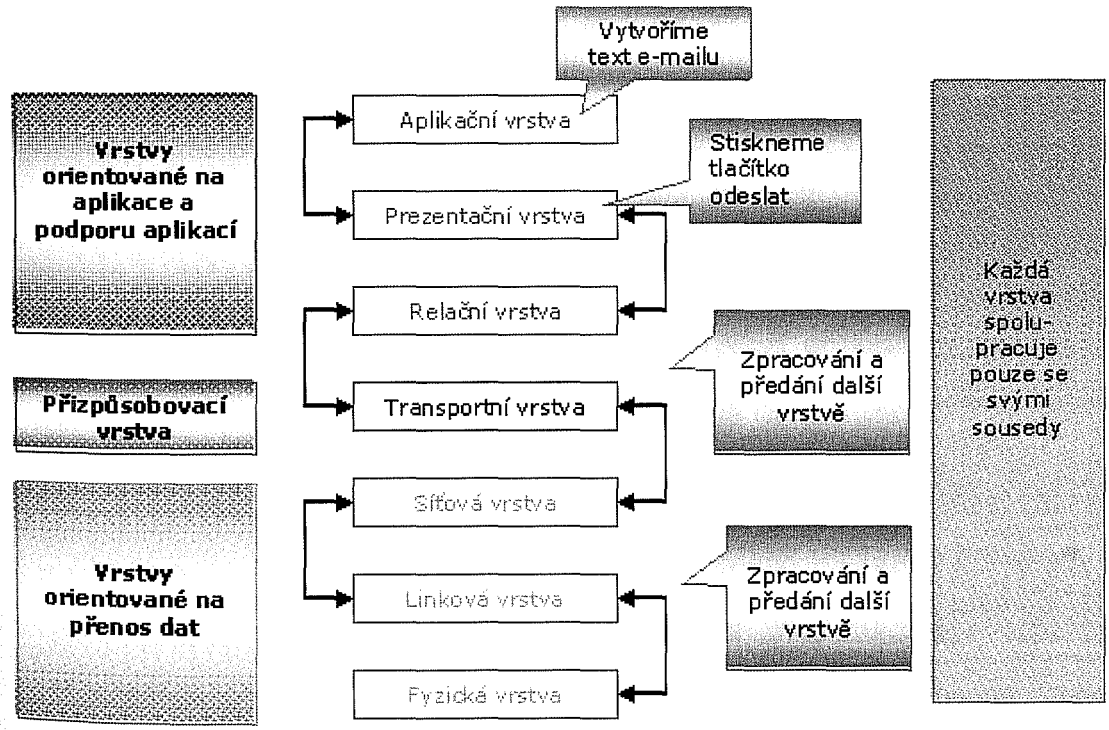
Problematika registrace domén spadá do oblasti soukromého práva, především do oblasti práva známkového a soutěžního. Z trestněprávního hlediska můžeme cybersquatting posuzovat na základě **§149** TrZ – nekalá soutěž, popř. **§150** TrZ – porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu. Otázkou by možná mělo být, zda není protiprávní už pouhé zaregistrování domény, zaměnitelné s ochrannými známkami, bez následného spuštění na WWW? Ze strany ICANN lze očekávat doplnění dosavadní zásady registrace *„first come, first served"* o jednoduchý princip *„use it or lose it"*.

37 Zdroj: http://www.czechia.com/info_about_domain_asp.

3.2 Útoky na data

Většinou jde o útoky využívající protokolu **TCP/IP**[38], který je starý přes 30 let a ne vše bylo tudíž navrženo optimálně. V době jeho vývoje se nepředpokládalo, že bude počítačová síť celosvětově rozšířená. TCP/IP protokoly jsou používané v internetu i v podnikových sítí – kde se nachází spousta informací a dat, které lákají ke zneužití. Pomocí těchto protokolů dochází k připojení k WWW serveru, přenosu souborů, odesílání nebo přijímání e-mailu. Pro uvedení do problematiky, resp. různých metod, které vedou ke zneužití dat, jsou přiblíženy základy síťové komunikace.

Aby komunikace mezi dvěma stranami byla možná, je nezbytná existence nějakých standardů a protokolů, které stanoví určitá komunikační pravidla. Síťová komunikace se řídí sadou protokolů definovaných v referenčním modelu ISO/**OSI** (Open System Interconnection). Ten poskytuje sadu mezinárodních pravidel a standardů, které umožňují všem systémům respektující tyto protokoly komunikovat s ostatními systémy. Tyto protokoly jsou obsaženy v sedmi oddělených, avšak navzájem propojených vrstvách, viz obr. č. 4. Na tomto obrázku je též znázorněn průběh odeslání e-mailu. [119]



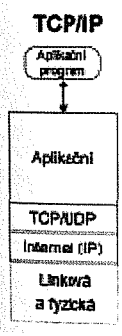
Obr. č. 4 - Vrstvená architektura ISO/OSI model

38 TCP (Transmission Control Protocol) – složitější nadstavbou nad protokolem IP a mění jeho způsob fungování – na spojitý a spolehlivý). Protokol TCP je spojovanou službou (connection oriented), tj. službou která mezi dvěma aplikacemi naváže spojení – vytvoří na dobu spojení virtuální okruh.

- **Fyzická vrstva** – obsluhuje fyzické spojení mezi dvěma body. Jedná se o nejnižší vrstvu a její hlavní úkol je posílání bitů po síti a aktivace, správa a deaktivace této komunikace na bitové úrovni.
- **Linková vrstva** – pracuje s posíláním dat mezi dvěma body (Ethernet). Poskytuje vysoce úrovňové funkce (např. korekce chyb, řízení toku), procedury pro aktivaci, správu a deaktivaci datových připojení. Vrstva poskytuje standardní adresovací systém pro všechna zařízení Ehternetu. Tyto adresy jsou známy pod pojmem MAC (Media Access Control) adresy. MAC adresu změnit nemůžeme, ale IP adresu ano. Protokol IP pracuje o vrstvu výš, takže se nestará o hardwarové adresy, ale používá mechanismus pro převod mezi dvěma adresovacími schématy – ARP (Address Resolution Protocol). Existují čtyři různé typy zpráv ARP, dvě nejdůležitější jsou ARP request (požadavek) - a ARP reply (odpověď).
- **Síťová vrstva** – hlavní úkol spočívá v zasílání informací mezi nižšími a vyššími vrstvami a také poskytování funkce adresování a směrování. Síťová vrstva využívá **IP** (Internet Protocol), pracuje s IP pakety a pakety ICMP (Internet Control Message Protocol – využíván často k testu konektivity). **IP pakety** se používají k zasílání samotných dat, zatímco **ICMP pakety** slouží pro zasílání diagnostických zpráv. IP je méně spolehlivý, tzn. neexistuje záruka, že IP paket opravdu dorazí do svého cíle. V případě problému dojde k zaslání ICMP paketu a upozornění odesílatele. V případě, že paket je větší velikosti a systém neumožní jeho přenos, IP rozdělí data na fragmenty, které už je možno odeslat. IP hlavičky se vloží do každého fragmentu a všechna data se poté odešlou. Když cílový počítač přijme tyto fragmenty, použije se hodnota offset v hlavičce ke zpětnému sestavení paketu.
- **Transportní vrstva** – poskytuje transparentní a spolehlivý přenos dat mezi systémy. Využívá dva protokoly TCP a UDP (User Datagram Protocol). TCP se nejvíce používá pro internetové služby – HTTP (webový provoz), SMTP (poštovní provoz) a FTP (přenos souborů). Výhodou a oblíbeností tohoto protokolu je obousměrné spojení mezi dvěma IP adresami, transparentnost a spolehlivost (zaslaná data dorazí do cíle ve správném pořadí). Funkčnost TCP spočívá v nastavení příznaků (např. URG – důležitá data, ACK – potvrzení spojení, RST – resetuje spojení, SYN – synchronizuje sekvenční čísla během počátku spojení apod.). Protokol UDP má menší nároky na funkčnost, je nespojovaný a nespolehlivý.

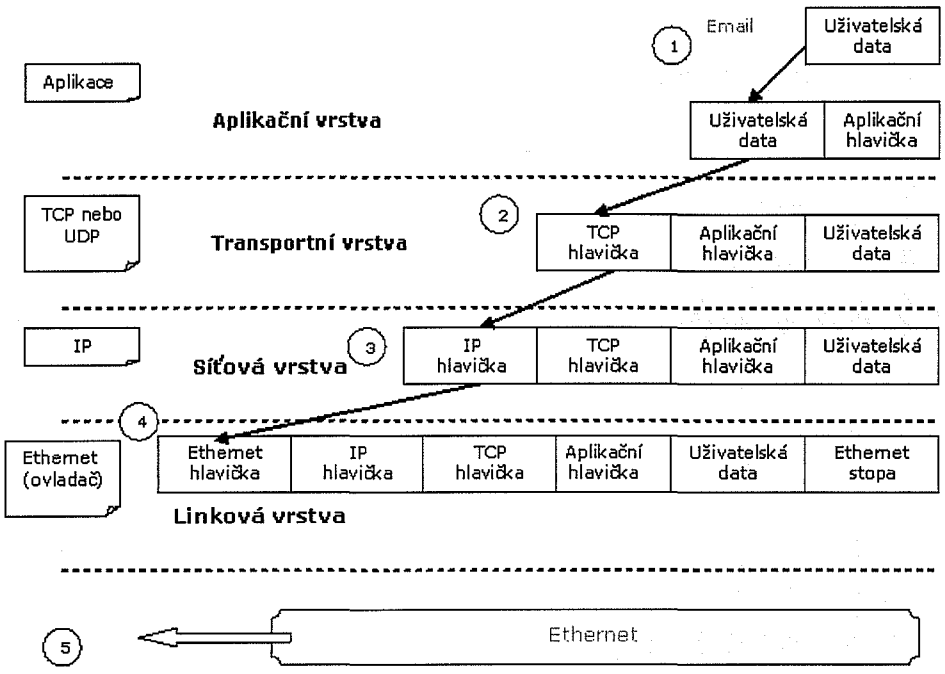
- **Relační vrstva** – zodpovědná za sestavní a správu připojení mezi síťovými aplikacemi.
- **Prezentační vrstva** – zodpovídá za prezentaci dat aplikacím v syntaxi nebo jazyce, kterému aplikace rozumí (umožňuje např. šifrování či kompresi dat).
- **Aplikační vrstva** – stará se o udržování požadavků aplikace.

Všechna data, bez ohledu na to, komu nebo od koho jsou určena, procházejí přenosovým médiem (kabelem) v seskupení zvaném rámec. Každý **rámec** je určen konkrétní **MAC adrese**, což je adresa každé konkrétní síťové karty, která je u většiny karet neměnná a byla kartě přidělena výrobcem. Každá karta na stejném segmentu sítě přijme každý rámec, který přenosovým médiem prochází a zjistí, zda je určen pro ni. Pokud ano, předá tento rámec ke zpracování vyšší vrstvě. Pokud ne, rámec je ignorován. Datová komunikace probíhá v tzv. **paketech**, které obsahují implementaci těchto protokolů ve vrstvách. Paket, který projde aplikační vrstvou, je obalen daty z prezentační vrstvy, které zase daty obaluje relační vrstva atd. Jednotlivé vrstvy síťových protokolů jsou tedy implementovány pomocí tzv. **enkapsulace**, čili zapouzdření. Každá ze síťových vrstev má přesně definovanou činnost, proto musí k datům, která přenáší, přidat specifickou informaci (hlavičku).



Zatímco referenční model ISO/OSI má sedm vrstev, síťový model TCP/IP má vrstvy pouze čtyři a také s nimi vystačí. Modely se také liší v představě o fungování síťové vrstvy. **Model ISO/OSI** má blíže k „telekomunikačnímu paradigmatu", kdy vítězí představa inteligentní, na funkce bohaté sítě a třeba i jednoduchých „hloupých" koncových uzlů. Přenosy dat na všech vrstvách by měly probíhat stejným způsobem a měly by být řešeny spolehlivě – v případě defektu, by se měly starat o nápravu. Oproti tomu **model TCP/IP** uplatňuje „počítačové paradigma" spočívající v „hloupé" síti a „chytrých" uzlech. Což znamená maximální zefektivnění přenosové části sítě, která bude nabízet minimum funkcí v co nejjednodušším provedením, ale velmi rychle. O ostatní by se měly starat až koncové uzly na úrovní transportní nebo aplikační vrstvy (spolehlivost přenosu, kompenzace ztrát). [97]

Na následujícím obrázku č. 5 je znázorněna implementace TCP/IP a enkapspulace dat v případě odeslání e-mailiu. Každá zapouzdřená vrstva obsahuje hlavičku (informace o protokolu vyžadované vrstvou) a tělo (data pro vrstvu). Internetová komunikace probíhá tak, že datové pakety jsou zapouzdřovány směrem dolů k fyzické vrstvě, kde jsou dále předány směrovači.



Obr. č. 5 – Protokol TCP/IP zapouzdřuje data odesílaná do sítě, převzato z [105]

Popis kroků, které se stanou po odeslání e-mailu prostřednictvím TCP/IP sítě [105]:

1) po dokončení dopisu – odeslání,
2) aplikační protokol vytvoří vlastní hlavičku, kterou předá i s daty transportní vrstvě,
3) po vytvoření TCP-hlavičky je tato spolu s daty obdrženými z aplikační vrstvy předána do síťové vrstvy implementací IP-protokolu,
4) zde je k datům připojena IP hlavička a vše je předáno do linkové vrstvy (síťová vrstva s ovladačem), která přidá vlastní hlavičku a data zkonvertuje do elektrických signálů, které jsou přeneseny médiem k cílovému zařízení,
5) systém, který tento paket přijme, odřízne ethernetovou hlavičku a předá získaná data vyšší vrstvě. Podobnou činnost provede každá z vrstev a uživatel nakonec obdrží zprávu.

Vrstvy, které jsou **náchylné k útokům** jsou síťová, transportní a linková vrstva. Pachatel, který se snaží získat přístup k nějakým internetovým serverům, se snaží postupovat tak, aby nemohl být zpětně identifikován. Při každém pokusu o přístup k jinému počítači se tento počítač dozví minimálně **IP adresu**[39] pachatelova počítače. Ta se vkládá při síťové komunikaci do každého paketu, aby WWW server a router (směrovač) na internetu věděl, kam má vyřízený požadavek zaslat. Pokud uživatel nemá trvalé připojení k internetu, zpravidla dostává při každém připojení jinou IP adresu. **Pouze poskytovatel připojení** může na základě souborů se záznamovými

[39] Jednoznačný identifikátor počítače v síti internet.

protokoly zjistit, který uživatel, kdy a pod jakou IP adresou se připojil na internet. Z důvodu ochrany dat však tyto informace nesmí nikomu poskytnout, kromě orgánů činných v trestním řízení. Záleží jen správci severu, jestli si dá práci s porovnáváním hledané IP adresy se seznamem neznámých, popř. anonymních vlastníků a jim přidělených IP adres. Pro větší zabezpečení anonymity používají hackeři jednu nebo více „přestupních stanic". Jde o tzv. **aktivní proxy server** nebo VPN[40]. Odesílaná a přijímaná data se tak nejprve umístí do této přestupní stanice, která se následně postará o jejich správné přesměrování. Server, na nějž se posílají požadavky, se tedy prakticky dozví pouze IP adresu přestupní stanice. [105]

V následujících kapitolách jsou popsány jednotlivé typy útoků na data a možné způsoby jejich provedení.

3.2.1 Distribuce malware

Podle studie provedené specialisty z Washingtonské univerzity[41] obsahuje každá 67. WWW stránka (reprezentativní statistický vzorek tvořil 18 miliónů WWW stránek) nějaký malware, což je opravdu neradostná statistika. Pod pojmem malware[42] rozumíme **škodlivý SW**, který je dále zneužíván k průnikům do systému a následnému zneužití či destrukci dat, případně celého systému. V současnosti jsou uživatelé internetu rozděleni na dva tábory: ti, kteří používají pokročilé zabezpečovací programy a ti, kteří prostřednictvím svých nechráněných počítačů dál škodlivý SW šíří. Konkrétně jde o tyto typy malwaru:

Počítačový virus – program, který má schopnost vlastní reprodukce, může být připojen k jiným programům, tvořit vlastní kopie nebo další modifikované viry:
Logical bombs (logické bomby) – programy, které se tajně vkládají do aplikací nebo OS, kde provádí naprogramované destruktivní aktivity.
Trojský kůň – program, který počítač zpřístupní tak, aby se do něj po síti mohl kdokoliv dostat. Neposílá jen nakažené e-maily, ale spolupracuje např. i s keyloggery. Počítačům, které napadne trojský virus se říká **zombie**; několik zombie vytváří tzv. **botnet**. Botnety lze řídit z jednoho vzdáleného počítače tak, aby prováděli stejné příkazy.
E-mailový červ - škodlivý kód, který se šíří prostřednictvím elektronické pošty v infikované e-mailové zprávě. K tomu, aby dokázal počítač infikovat, potřebuje zpravidla aktivní spolupráci samotného uživatele.

---

40 Virtuální privátní síť.
41 Zdroj: http://www.ucdc.edu/aboutus/livingindc.cfm?dir=Faculty&id=15.
42 Původ slova z malicious software.

Síťový červ – naprosto samostatný škodlivý kód, který se většinou šíří pomocí určité bezpečnostní díry v cílovém systému a nepotřebuje žádnou spolupráci ze strany uživatele.

Rootkity - skryté soubory programů umožňující napadení a následné ovládnutí počítače útočníkem (*„nepředstavují přímé nebezpečí, ale bránu k tomuto nebezpečí doširoka otevřenou"*)[43]. Tento škodlivý kód pracuje na nízké úrovni OS (kernel), který se dokáže ukrýt před uživatelem i před různými bezpečnostními programy. Původní rootkity pocházejí z unixových OS, kde sloužily k získání administrátorských (root) práv. Jde o utility, které dovolí hackerům pronikajícím do systému skrýt na napadeném počítači po sobě všechny stopy a soubory, takže uživatel vůbec nepozná, že se na jeho systému nějaký malware vyskytuje.

V roce 2005 proběhla **aféra** s rootkitem od firmy *Sony BMG*, který obsahovala protikopírovací ochrana *XCP (eXtended Copy Protection)* na vydávaných CD. Tento rootkit umožňoval hackerům skrýt na počítači viry a učinil ho imunní proti antivirovým programům. SW se do počítače instaloval bez vědomí uživatelů, bez možnosti odinstalování - trvale zatěžoval systém a odesílal data o uživateli. Po vložení CD do počítače se totiž zobrazily licenční podmínky EULA[44] s nimiž musel uživatel souhlasit (jinak by se dál nedostal). *XCP* postihla především platící zákazníky, vyvolala bojkot k produktům Sony a mnoho žalob. Firma, která danou ochranu pro *Sony BMG* vyvíjela, se k problému stavěla velmi laxně. Výsledkem pátrání bylo zjištění, že firma *Sony*[45] o závažnosti problému věděla již od začátku, ale s přiznáním chyby veřejnosti nijak nespěchala. Kauza vyvolává zamyšlení, zda takovýto způsob ochrany proti hudebním pirátům je efektivním řešením. [74]

Keylogger – škodlivý kód, který monitoruje a zaznamenává stisknuté klávesy. Může být zneužit třeba ke kompromitaci přihlašovacích údajů, hesel apod.

Bot – škodlivý kód, který se soustředí zejména na ovládnutí infikovaného systému a jeho další využití. Může také např. vytvářet šifrovaný kanál pro komunikaci mezi útočníkem a infikovaným počítačem.

Spyware – program, který bez vědomí uživatele sleduje navštívené stránky, používané služby používá a vůbec vše, co uživatel na počítači provádí (IP adresu, záznam DNS adresy, seznam všech nainstalovaných programů, údaje o souborech uložených na počítači, záznamy o aktivitách na síti, informace o telefonickém připojení, hesla atd). Skrývá se často v SW, který je distribuován zdarma, v podobě dodatkových reklamních aplikací – **adware**, špatně se odinstalovává a narušuje tak

43 PŘIBYL, Tomáš. Causa rootkit. *PC World*. 2006, č. 3, s. 52-55.

44 End User Licence Agreement.

45 Podle vyjádření zástupců tuzemské pobočky Sony BMG - nejsou a nikdy nebyla hudební CD s problematickou ochranou XCP v Čechách prodávána.

průběh aplikací. Na vině jsou sami uživatelé, kteří si instalují spoustu programů distribuovaných na internetu zdarma. Mnoho výrobců sharewarových aplikací přešlo ke „spywarovému" modelu, který nabízí zdarma a peníze dostanou od pochybných reklamních společností za informace o uživateli tohoto SW. MS se také podílel na těchto aktivitách, např. *Media Player* umožňuje jednoznačně identifikovat daného surfujícího uživatele nebo při zatuhnutí systému nabízí odeslání informací o výpisu z operační paměti na jeho server. Až doposud se jednalo o převážně „neškodné" programy, jejichž cílem bylo sledovat, na jakých internetových stránkách se uživatel pohybuje (marketingové a reklamní cíle). Internetoví zločinci se však stále častěji zaměřují na finanční zisk - a spyware se tak bude využívat ke zločinným účelům, například k ukradení identity či monitorování klávesnice za účelem zachycení osobních údajů. Adwarové a spywarové produkty se vyskytují i ve výměnných sítích. Osvětě ohledně spyware se věnuje sdružení *Anti-Spyware Coalition* (www.antispywarecoalition.org).

Hijacker – program, který přesměruje internetový prohlížeč na nechtěné WWW stránky, využívá trhliny v zabezpečení IE. Nejčastěji nainstaluje do WWW stránek nebo tzv. *Browser Helper Objects* funkce, které lákají k využívání různých internetových služeb a snaží se tak vysledovat uživatelovy zájmy.

Backdoor *(zadní vrátka)* - škodlivý kód, který do infikovaného počítače otevírá nežádoucí komunikační kanál, který obchází aktuální způsoby autentizace uživatele. Zadní vrátka jsou především nástrojem pro vzdálený přístup hackera do infikovaného systému. Obvykle jsou reprezentovány jedním souborem, který nakopíruje svá data do počítače, modifikuje systémové soubory a odposlouchává datový provoz na síti.

Dialer - program, který mění telefonní číslo vytáčeného připojení k internetu na číslo s vysokým tarifem nebo na číslo zahraničního poskytovatele. Některé antidialery jsou tak důmyslné, že zeslabí reproduktor modemu, aby nebylo možné postřehnout okamžik přepojení. Dialery se často zapisují do registrů počítače a schovávají se.

Podle statistik z roku 2004 - počet škodlivých kódů přesáhl hranici 100 000, ale jde jen o orientační číslo (různé verze virů, jejich modifikace atd.). Viry se šíří především elektronickou poštou, např. v roce 2003 byl celosvětový poměr e-mailů a virů v nich 33:1, o rok později se počet zdvojnásobil na 16:1. [110] Škodlivé kódy se už nepíší jen pro zábavu nebo reputaci jejich autorů, ale hlavně k odcizení dat z napadených počítačů či k instalaci jiných zákeřných programů. Uvedený malware **využívá bezpečnostních nedostatků** systémů a umožňuje zneužívání počítačů k provádění dalších ilegálních činností (šíření dětské pornografie, rozesílání spamu, DDoS útoky, krádež identity atd.), které jsou popisovány v následujících kapitolách. Utěšující zprávou je, že se neustále **zkracuje doba** mezi zranitelností SW a objevením příčiny, která příslušnou chybu využívá. Podle statistik společnosti *X-Force* [65], která

analyzuje nejnovější trendy v bezpečnosti a aktuálním ohrožení, dochází k časové kompresi, např. v roce 2002 odhalení viru *Slammer* trvalo 6 měsíců, v roce 2003 byl vir *Blaster* odhalen již za 26 dnů a v loňském roce stačily k odhalení viru *Zotob* pouhé 2 dny.

Opatření proti škodlivému SW jsou instalace a pravidelné aktuliazace antivirových programů (např. *AVG, Avast!, Norton Antivirus* atd.), antispywarových programů (např. *SpywareBlaster, SpyBlocker, Spybot Search&destroy* atd.), programů na odstraňování rootkitu (např. *RootkitRevealer, BlackLight* atd.), používání osobního firewallu (např. *Zone Alarm*) a antidialerů (např. *MrSoft Antidialer*). K tomu můžeme dodat radu - nestahovat z internetu vše, co je k dispozici „zadarmo" a brát v potaz důvěryhodnost serverů.

Trestněprávní úprava

Úmyslné rozesílání virů může být kvalifikováno jako řada trestných činů. Jedním z nich je **§257a** TrZ - poškození a zneužití záznamu na nosiči informací, dále může jít o **§105** TrZ – vyzvědačství, **§178** TrZ - neoprávněné nakládání s osobními údaji aj. Záleží na motivu pachatele a vlastnosti malware.

3.2.2 Hacking

Tímto pojmem rozumíme neoprávněné získání přístupu k datům, tzv. průnik do systému jinou, než-li standardní cestou. Po trestných činech vztahujících se k porušování AP, jde o druhou nejčastější oblast EIK. Mezi těmito typy kriminality existuje ovšem, podle MATĚJKY [85], propastný rozdíl. Zatímco u hackingu je patrná tendence ke zpřísňování postihu, masovost porušování AP vede spíše k úvahám na téma udržitelnosti současné právní úpravy, neboť se jedná o čin, který v menší či větší míře páchá značná část počítačově gramotného obyvatelstva.

Tyto trestné činy jsou páchány nepřímo, přes více internetových serverů, aby bylo dosaženo snížení možnosti identifikace skutečného umístění pachatelova počítače. Jak již bylo naznačeno - k průniku se využívá tzv. **backdoors**. Na internetu se nachází celá řada podpůrných programů i s popsanými postupy, jak průnik nejefektivněji spáchat. Hacking je lákavou činností počítačových nadšenců bez destruktivních záměrů, ale zároveň i vykalkulovanou aktivitou s cílem obohacení a poškození. Amatérské průniky do systémů lze většinou snadno odhalit, zatímco v závažných případech mnohdy zůstává pachatel neodhalen. [31]

Technika, která je při počítačovém útoku hojně aplikována, se nazývá **sociální inženýrství** (social engineering), tzv. sociotechnika. Sociální inženýrství využívá nátlakové metody v podobě časového limitu či hrozícího nebezpečí. Další záminkou

k získání důvěry uživatelů je fakt, že např. u e-mailu je odesílatelem subjekt s vyšší autoritou, obsah slibuje nevídané slevy či nabízí něco zdarma atd. Průkopníkem této metody je **Kevin Mitnick**, který se touto tematikou zabývá ve dvou vydaných publikacích (*Umění klamu* a *Umění průniku*). Jde o velmi nebezpečnou techniku, a to nejen počítačového útoku, neboť je zaměřena na **nejslabší článek** celého systému, kterým bývá člověk. Jakmile selže lidský faktor, jsou veškerá implementovaná bezpečnostní opatření zbytečná. [108] Sociální inženýrství vychází z filozofie „proč dělat věci složitě, když to jde jednoduše". Nač se zbytečně snažit prolamovat heslo, když ho můžeme získat úplně primitivním způsobem? Zní to neuvěřitelně, ale je to tak. Umění spočívá ve snížení pozornosti člověka, aby vykonal úkon, který by za normálních okolností neprovedl, nebo by dokonce pojal podezření a přijal by odpovídající opatření.

Podmínkou průniku je síťová komunikace a též využívání různých bezpečnostních děr v systémech. Hacking je páchán především z těchto důvodů [73], [31]:

- **Neoprávněné získání a užití informací** – jeden z nejnebezpečnějších útoků na jakákoliv data. Nebezpečí spočívá v neodhalitelnosti pachatele, což přináší zásadní bezpečnostní riziko pro rozsáhlé databáze různých subjektů. Podle studie Ministerstva vnitra [31] mohou tuto formu trestné činnosti využívat i cizí zpravodajské služby, protože přináší nejmenší riziko odhalení jejich činnosti. V současnosti dochází k zvyšování počtu útoků tohoto druhu.
- **Zničení, poškození nebo učinění informací neupotřebitelnými** – jde o nepřátelskou manipulaci s daty, považovanou za primitivní formu trestného činu, protože jeho následky lze snadno zjistit. Příkladem jsou změny webových stránek. Pohnutkou pachatele je nejčastěji ukázka vlastních schopností, případně záměrné poškozování firmy či osoby, které webové stránky vlastní, vytvářejí nebo spravují.
- **Zásah do technického nebo programového vybavení počítače** – jako příklad můžeme uvést tvorbu tzv. backdoors[46], či cracků apod. Dále může docházet k zneužívání možností konkrétního počítače, který má přímé a bezplatné napojení na jinak placenou službu.

Úspěšnost útoků je dána „kvalitou" bezpečnostních opatření na počítačích připojených internetu, které jsou závislé jednak na schopnostech správce počítače nebo připojení, jednak na výběru použitého softwaru.

Trestněprávní úprava

Co se týče **právní úpravy** hackingu, samotný průnik do systému je trestný podle **§257a** TrZ, tj. poškození a zneužití záznamu na nosiči informací, ovšem **jen**

46 Backdoors (zadní vrátka) – SW pro hledání bezpečnostní díry která byla záměrně vytvořena pro rychlý přístup do systému v problematických či kolizních situacích. V případě jejího odhalení či prozrazení je však ideálním místem průniku pro neoprávněné osoby.

tehdy, pokud hacker touto aktivitou způsobí jinému škodu či jinou újmu, nebo sobě či jinému neoprávněný prospěch. Prostřednictvím hackingu jsou páchány další nelegální aktivity, jako např. zkreslování údajů o stavu hospodaření a jmění (**§125** TrZ), nekalá soutěž (**§149** TrZ), porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu (**§150** TrZ), porušování průmyslových práv (**§151** TrZ), neoprávněné nakládání s osobními údaji (**§178** TrZ) atd.

Některé veřejně publikované úspěšné průniky mohou znít jako neuvěřitelné detektivní příběhy. Realita je však úplně jiná. Existují metody útoků, které lze páchat i bez náročného vybavení. V následujících odstavcích jsou popsány vybrané metody, postupy vyhledávání stop, s jejichž pomocí může být dosaženo jmenovaných trestných činů.

Sniffing

Sniffing („čmuchání"), jehož principem je zachytávání a analýza síťového provozu (převážně sítí typu LAN), je stejně jako např. cracking využíván především k **usnadnění** další nelegální činnosti. Existuje celá řada (i volně šiřitelných) programů - tzv. snifferů, které umožňují **monitorovat veškerou komunikaci**, která prochází přes dotyčný uzel sítě (např. *Tcpdump, Hunt* či *Ethereal*). Stačí takový program pouze nainstalovat a spustit, zbytek již program provede sám. Program přepne síťovou kartu do tzv. „promiskuitního" modu a poté sleduje a analyzuje veškerý provoz v daném segmentu sítě. Takto lze získat veškerý obsah nešifrované komunikace, přístupová jména a hesla, znění e-mailů na freemailových službách či soubory posílané po síti.

Opatření proti tomuto druhu činnosti spočívá především v důsledném šifrování internetové komunikace a zabezpečení sítě proti neoprávněným přístupům. Sniffery neslouží pouze útočníkům k průnikům do systémů apod. činnostem, ale i administrátorům např. k diagnostikování chyb sítě.

Trestněprávní kvalifikace sniffování spadá pod **§239** TrZ – týkající se porušování tajemství doručovaných zpráv, příp. **§240** TrZ v případě, že dojde k vyzrazení či zneužití dopravovaných zpráv.

DNS spoofing[47]

DNS (Domain Name Service) je službou, která se stará o převod doménových jmen na IP adresy a naopak. Podmínkou zfalšování DNS je sledování síťového provozu a spuštění programu, který odchytí všechny DNS dotazy a snaží se ně odpovídat podle útočníkova záměru. Cílem je tedy podvrhnout DNS odpověď a

[47] Základ slova to spoof – švindlovat.

přesměrovat hosta na jiný server. [54] Princip podvodu spočívá v hlavičce HTTP protokolu, ve které se upraví informace o WWW stránce (parametr Refferer). Tento „trik" je využíván u phishingu a pharmingu (kap. 3.2.4).

Skenování portů

Jde o proces, při kterém jsou sledovány všechny služby a jejich reakce na cílovém počítači. Standardní skenování portů TCP probíhá formou *three-way handshake* (třícestného spojení). I pro tuto činnost existuje spousta podpůrných nástrojů, např. *SuperScan*, či *fscan* atd. Každé skenování snižuje kapacitu, popř. výkonnost systému, v řadě případů může přispět k pádu či přetížení celého systému. **Trestněprávní kvalifikace** skenování portů není výslovně ustanovena, avšak může zde být uplatněn **§257a** TrZ. **Opatření** spočívá v blokaci na úrovni celé sítě pomocí směrovače nebo firewallu. [88]

In the Middle Man

Tento typ útoku patří mezi méně sofistikované metody. Spoléhá na netečnost a nedůslednost uživatele. Počítač se v síťové komunikaci chová jako mezistanice, např. pomocí proxy severů. Pokud je počítač správně nakonfigurován, nenapojuje se přímo na požadovanou webovou stránku, ale posílá požadavky přes proxy. Tím zjistí pouze IP identifikaci, která umožňuje zpětně sledovat připojení k internetu. [54]

Prolamování hesel

Hesla slouží k zabezpečení počítače, jednotlivých programů či konkrétních dokumentů před neoprávněným přístupem. Můžeme sem také zařadit již zmíněná sériová čísla, která se dají stáhnout zdarma z internetu (např. www.serials.ws, www.freeserials.com, http://www.serials.com, http://www. t1000.net aj.), a tak celkem snadným způsobem prolomit ochranu. Systémová a jiná hesla je možno získat několika způsoby. Jednak za pomocí **utilit** pro zobrazení uložených hesel v systému, např. *Asterisk Logger*, dalším využívaným způsobem je **slovníková metoda**, která vychází z toho, že heslo je pravděpodobně nějaké obvyklé slovo, neobsahující číslice ani speciální znaky. Na internetu je možno stáhnout velké množství takovýchto slovníků. Poněkud drastičtější metoda, jak už vyplývá z názvu, je použití **hrubé síly**, která spočívá v kombinování všech možných znaků, což je velmi zdlouhavé, a proto ne příliš oblíbené. K překonání ochrany textových či tabulkových dokumentů je na trhu dostupný **komerční SW**, např. *Office Password* od firmy *Lastbit Software* či *Advanced Office Password Recovery* od firmy *Elcomsoft*.

Dalšími možnostmi získání hesla je již popsaná sociotechnika. Pro zajímavost můžeme uvést, že spousta citlivých údajů se nachází v odpadkových koších, kde útočníci jednoduchým způsobem většinou najdou, co potřebují k průniku (tzv.

trashing). Nejúčinnějším **opatřením** je nenechat útočníka získat přístup do cílového počítače (zabezpečení síťové komunikace) a užívat velmi silná hesla (alespoň osm znaků, kombinace velkých, malých písmen a ostatních znaků, žádné osobní údaje apod.).

Metody obcházení ochrany přístupu na placené stránky

Kromě již zmíněného spoofingu lze ilegálně získat přístup na stránky s placeným obsahem a nedostatečnou ochranou pomocí tzv. **Deep Links**, tedy prostřednictvím URL adresy. Deep Links, např. www.hlavnistranka.cz/placene/obsah1.htm, jsou odkazy, které vedou přímo k placenému obsahu. Pokud se tedy útočník jednou dozví jméno složky s placeným obsahem, pak si může při dalších návštěvách zadávání jména a hesla ušetřit a dostat se na stránky s placeným obsahem přímo. Dalším způsobem, jak obejít placený přístup je pomocí tzv. **cookies**. Po zaplacení registrační poplatku uživatel obdrží soubor cookie s potřebnými informacemi, který se uloží na pevný disk. Poté je možno prohlížet placený obsah bez dalšího přihlašování. Trik spočívá v tom, že si uživatel soubor cookie zazálohuje a službu odhlásí. Poté si cookie nahraje na stejné místo na disku a má možnost bezplatně surfovat. Proto dnes již převažují zabezpečené cookie. [19]

Všechny naznačené metody jsou pouhou ukázkou hackerských dovedností. Čím dál důmyslnější a průbojnější techniky - sloužící ke sledování síťové komunikace, odchytávání hesel či obcházení všelijakých zabezpečení - jsou dostupné běžným uživatelům v knižních publikacích, např. [105], [119] či jsou sdíleny samotnými hackery v rámci jejich etiky (blogy, diskusní fóra atd.).

3.2.3 Phreaking (telefandovství)

Pod pojmem phreaking[48] rozumíme činnost, která vede k bezplatnému využívání telefonních linek (napichování služby, hovory na účet někoho jiného nebo telekomunikační firmy). Phreaking se pyšní bohatou čtyřicetiletou historií. Původní telefandové pokládali phreaking za jistou formu zábavy. Bavili se na úkor telefonní společnosti s ostatními, podobně motivovanými jedinci, třeba na druhém konci světa. Postupně přestala být tato forma zábavy módou a **phreakeři** (používají ukradené telekomunikační informace pro přístup k dalším počítačům) či **phrackeři**[49] (snaží se napadat programy a zneužívat databáze telefonních společností za účelem získaní

[48] Původ slova z phone a freaks (podivíni).

[49] Původ slova z phone a crackers.

telefonních služeb zdarma) se začali učit pronikat do počítačových systémů. Hackeři (white hats) se od této skupiny distancují.

Dnes jde především o studenty elektrotechnických oborů, kteří své znalosti zúročují výrobou tzv. věčných čipových telefonních karet, výjimkou ovšem nejsou ani případy „napíchnutých" telefonních ústředen či pouličních automatů. [85] Díky digitalizaci telefonů je phreaking na značném ústupu – na rozdíl od rozmáhajícího se phishingu.

Trestněprávní úprava

Na tyto aktivity se vztahuje **§182** TrZ – poškozování a ohrožování provozu obecně prospěšného zařízení, v případě, že dojde i k poškození či zneužití záznamu na nosiči informací, je možno uplatnit **§257** TrZ. Dojde-li také k porušení telekomunikačního tajemství, bude použit **§239** TrZ.

3.2.4 Phishing a Pharming

Phishing[50] a pharming[51] jsou zřejmě nejnebezpečnější formou využití spamu či jiných útoků, která dnes existuje. Phishing (také znám pod pojmy „brand spoofing" a „carding") historicky navazuje na aktivity phrackerů, těžiště jejich zájmu nejsou čísla telefonních karet, ale krádež obecnějších **privátních citlivých informací** patřících jedinci. Těmito údaji mohou být především údaje o platební kartě nebo krádež přístupového jména a hesla k různým internetovým službám, s jejichž pomocí lze na dálku manipulovat s bankovním kontem. [50] Tyto nelegálně získané údaje jsou pak zneužity např. při převodu peněz, internetových nákupech, aukcích a jiných internetových podvodech. Phishing je běžnou metodou **krádeže identity**. Nejčastěji je prováděn pomocí naprosto legitimně a oficiálně vypadajících e-mailů, které obsahují formulář čekající na uživatelovo vyplnění a odeslání. Na phishing navazuje sofistikovanější metoda - **pharming**, která je sice známa už několik let, ale svůj rozvoj zažívá až v poslední době.

Hlavní metodou phishingu a pharmingu je **sociální inženýrství**[52], které je doplněno dalšími prvky zvyšující důvěryhodnost, např. zfalšovaná e-mailová adresa, napodobená grafika, znalost terminologie atd. **Principem phishingu** je vyplnění formuláře, který žádá o potvrzení nebo doplnění např. bankovních údajů jako jsou - čísla kreditních karet, PIN apod., přímo v e-mailu. **Pharming** je mnohem větším

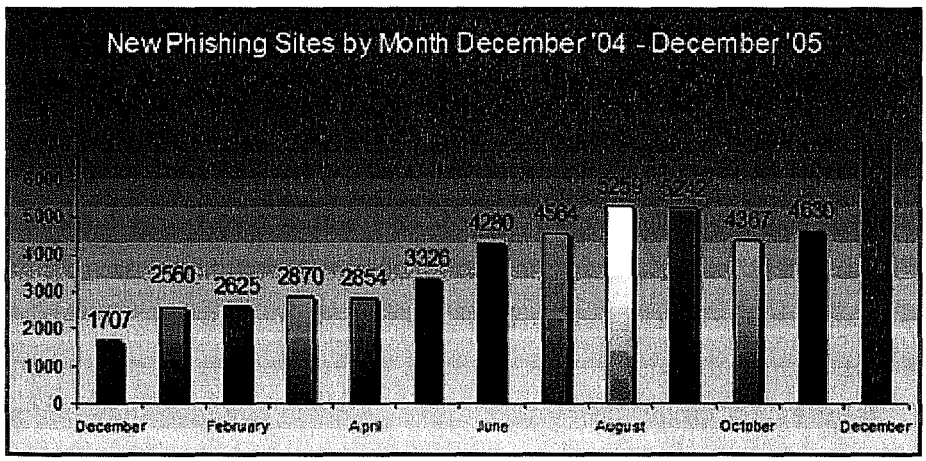
50 Původ slova z password a fishing.

51 Původ slova z password a farming.

52 Manipulace, ovlivňování a klamání toho druhého, kdy je cílem od něj získat informace, které potřebujete, a nebo ho přemluvit a zmanipulovat k tomu, aby třeba konkrétně do počítače zadal kód, který chcete, aby tam zadal.

nebezpečím, které je obtížně rozpoznatelné. Tajemství spočívá v překládání URL adresy do formátu IP adresy prostřednictvím DNS serverů. Útočníci se pokouší najít špatně zabezpečený server, v němž následně přepíší IP adresu určenou např. pro URL banky, IP adresou falešné stránky, např. www.landofbank.com nahradí www.1andofbank.com. Po **odeslání** požadovaných dat nastává „chycení do sítě". Obětí phishingu a pharmingu jsou jednak důvěřiví uživatelé, kteří se stanou cílem a jednak instituce, u kterých měli uživatelé účet. Ty musí investovat značné prostředky a zdroje do různých reklamací a šetření. Dalším dopadem je pokles důvěryhodnosti takových institucí a možný odliv zákazníků ke konkurenci či obava zákazníků využívat služby elektronického bankovnictví.

Aby byl **phishing** úspěšný, musí phisheři - internetoví podvodníci (phishing scams) odeslat obrovské množství falešných e-mailů, což už dnes není příliš snadné, protože velké přijímací (SMTP) servery dokáží mnoho masových mailingů blokovat. Phisheři nejdříve zavirují pomocí e-mailových červů tisíce běžných počítačů **(botnets)** připojených k internetu. Virus, který umí rozesílat e-maily z daného stroje, zatím spí, a je probuzen právě v okamžiku, kdy útočník zavelí k masovému mailingu a odešle si svou dávku e-mailů. Podle statistik firmy *McAfee* [87] dvě třetiny všech webových stránek využívajících phishing se nacházely v roce 2004 na serverech v USA, Jižní Koreji a v Číně. Dle společnosti *Messagelab* bylo od října 2002 do září 2003 zaregistrováno 279 e-mailů, které se pokoušely o phishing. Alarmující jsou údaje z následujícího roku, kdy bylo zaznamenáno již 18,5 miliónů takových e-mailů. Na následujícím obr. č. Obr. č. 6 je možno vysledovat nárůst phishingu v období jednoho roku na území USA.



Obr. č. 6 – Nárůst phishingu během roku 2004 a 2005, převzato z [4]

V **České republice** nejde o příliš častý jev, ač musíme zmínit březnový případ, kdy se pachatel pokoušel vylákat přihlašovací údaje od uživatelů bankovních služeb *CitiBank*.

Podle studie s názvem *Open to Exploitation: American Shoppers Online and Offline*[53] bylo zjištěno, že téměř polovina amerických občanů nedokáže identifikovat phishingový e-mail. V průměru bylo výsledkem 7 správně označených odpovědí ze 17-ti. Podobně na tom jsou obyvatelé Velké Británie, kde 84% respondentů nerozumí pojmu phishing. Je dost pravděpodobné, že v České republice by výzkum dopadl obdobně.

Opatření proti phishingu je věnována značná pozornost (např. prezident Bush zařadil boj proti phishingu do svého volebního programu). V roce 2004 oznámili zástupci řady podniků a donucovacích orgánů založení skupiny *Digital PhishNet*, které se zaměřuje na pomoc a podporu při dopadení a stíhání osob, které jsou zodpovědné za spáchání trestných činů proti zákazníkům prostřednictvím phishingu. Dále byla založena organizace *Anti-Phishing Working Group* (www.antiphishing.rg). Na své webové stránce uvádí informace k tématu, aktuální a předchozí phishingové e-maily v anglickém jazyce atd. Tato skupina doporučuje používání hašování hesla. Proto, abychom nenalétli na phishigový e-mail, můžeme udělat pár maličkostí. První efektivní ochranou je zásada „neklikat" na odkaz, který je e-mailu uveden, ale zadávat adresu instituce přímo do adresového řádku prohlížeče. Případně můžeme e-mail v HTML formátu otevřít přímo v internetovém prohlížeči. Pohybem kurzoru myši nad odkazem se pak ve stavovém řádku objeví odkaz, na který bude stránka přesměrována. S narůstajícím výskytem případů phishingu vytasily své zbraně i softwarové firmy. Zabezpečení slibuje např. nástroj *Netcraft Toolbar,* který kontroluje u příslušného registru domén původ (geografické umístění) a aktuálnost domény, která se vyskytuje v odkazu e-mailu. Po krátké analýze vizuálně zobrazí důvěryhodnost stránky. Další podobně zaměřenou utilitou je *EarthLink Toolbar*.

Na rozdíl od phishingu - **pharming** využívá technologii zvanou **DNS cache-poisoning** – otrávění paměti DNS záznamů. Principem pharmingu je modifikace záznamů v lokální paměti IP adres, tzn. místo korektní IP adresy je záznam změněn na podvrženou adresu. Když se pak uživatel pokusí připojit k nějaké stránce, prohlížeč vezme modifikovaný záznam z paměti a na internetu vyhledá příslušný podvržený server. Uživatel tuto změnu vůbec nezaregistruje, neboť z jeho pohledu došlo ke zcela korektní operaci: zadal správný název instituce a stránka se korektně zobrazila. [113] Takto zmodifikované webové stránky, které z uživatelů lákají citlivé údaje, jsou velmi těžko odhalitelné, neboť neexistují déle než 48 hodin.

Z výše popsaného je zcela jasné, že jde o velmi nebezpečný jev, o kterém pravděpodobně ještě hodně uslyšíme.

---

53 Zdroj: http://www.annenbergpublicpolicycenter.org/04_info_society/Turow_%20APPC_Press_Release_WEB_FINAL.pdf.

3.2.5 DoS a DDoS útoky

DoS útok (Denial of Service), je typem útoku - odmítnutí služby – který je namířen proti serveru, resp. celé síti připojené k internetu s cílem ochromit jejich provoz. Jde o útoky, při nichž je z mnoha míst vysláno velké množství požadavků na jeden server, který se pod jejich náporem zhroutí. Někdy je DoS útok použit jen jako pomocná akce k zahlazení stop, restartování vzdáleného počítače apod. MUKNŠÁBL [90] zmiňuje podtypy těchto útoků, které využívají:

- **chyby v implementaci TCP/IP**
  - *Ping of death* – příkaz ping je využit k vytvoření IP paketu, jehož velkost přesahuje povolená specifikace a ten je pak poslán do cizí sítě
  - *Teardrops attacks* – využívá slabosti při opětovném sestavování fragmentů IP paketu, které mohou být po cestě sítí rozděleny
- **nedokonalosti a nedostatky ve specifikaci TCP/IP**
  - *SYN attack* – využívá spojení „three-way-shaking"
  - *Land attack* – modifikace SYN útoku s využitím zfalšované IP adresy cílového systému
- **hrubé síly**
  - *Surf attack* – útok zaměřený na „všeobecné adresování" (direct broadcast addressing), kdy dojde k zaplavení routeru speciálními pakety, tzv. pingy
  - *UDP Flood* – pomocí falšování je zapnuta služba, jejímž výsledkem je nekonečný tok nesmyslných dat mezi dvěma systémy
- **DNS** – DNS servery jsou zahlceny dotazy se zfalšovanou zdrojovou adresou, která se shoduje s IP adresou systému, na který je zamířen útok.

DDoS útok (Distributed Denial of Service) jsou variantou DoS útoku, který je však prováděn souběžně z velkého množství počítačů. S pomocí tisíců počítačů na celém světě, které se nakazily škodlivým kódem a vytvořily tak **botnet**, je možno zahltit podnikové severy tisíci elektronických zpráv, čímž se zablokují veškeré skutečné transakce a komunikace serveru.

Pachatelé poté zašlou společnosti e-mail, ve kterém požadují finanční obnos pod hrozbou opakovaného útoku. Tento typ vydírání zaznamenal rozkvět zejména v posledních třech letech, kdy roste počet sítí, které zločinci mohou vzdáleně řídit a ovládat. V roce 2004 bylo zaznamenáno, že se denně z 30 000 počítačů stávají aktivní botnety, které jsou dokonce za vysoké finanční obnosy pronajímány. Uvedené technologie, podle studie *McAfee* [87], nejvíce využívají zločinecké gangy z Východní Evropy k poškozování webových severů různých organizací a obchodních společností.

Dochází také k najímání hackerů, kteří tyto útoky provádí na konkurenční firmy zadavatele.

Ač spouštění zmíněných útoků nevyžaduje žádné speciální znalosti – stačí stažení a spuštění speciálního SW - **opatření** proti těmto útokům je poměrně složité (nastavování routerů, firewallů apod.).

3.2.6 Kyberterorismus

Kybernetický terorismus - kyberterorismus je pojem, který zastřešuje kombinaci výše zmíněných útoků, které jsou **nasměrovány proti osobám či majetku** za účelem vyvolání strachu, vydírání nebo vymáhání ústupků. Dle **americké vlády**[54] je kyberterorismus vymezen jako prokalkulovaný, politicky motivovaný útok proti informačním, počítačovým systémům, počítačovým programům a datům, vedený subnárodními skupinami nebo tajnými agenty, jehož výsledkem je násilí proti nezúčastněným a nebojujícím osobám. V literatuře je uváděno mnoho definic kyberterorismu, od velmi širokého pojetí až po úzké vymezení pojmu.

Na tento jev je pohlíženo ze dvou úhlů. Mnoho autorů [43] zastává **užší pojetí**, které kyberterorismus nepovažuje za hrozbu a tvrdí, že se nikdy neobjevil a nemůže nikoho poškodit. Druhé, **širší pojetí** předpokládá, že kyberterorismus je skutečnou bezpečnostní hrozbou vlád a organizací na celém světě. Zdá se, že kyberterorismus se stává realitou - čím dál více jsme závislí na IS a ICT a jejich ohrožení - v podobě narůstajících kybernetických útoků - má za následek nedozírné škody a ztráty.

ICT představují pro vyspělé státy obrovskou **konkurenční výhodu**, zároveň však představují jejich **nejzranitelnější místo**. Často jsou útoky zaměřené proti vládním a jiným institucím pro podporu politických, sociálních a ekonomických cílů. Útoky jsou zaměřené na **IS** oběti - v ohrožení jsou banky, letiště, armádní řídící systémy, nemocnice aj. instituce, které jsou závislé na počítačových sítích a databázích. ICT jsou zde využívány jako **nástroj** útoku pro manipulaci a zneužití cizích informačních systémů, ke krádeži nebo změně dat, příp. k přetížení a zahlcení IS. [104] Ale zároveň jsou ICT také **cílem** útoku, který je zaměřen na zničení vlastního IS a systémů, které jsou na něm závislé. Útoky na IS jsou pro teroristy z hlediska nákladů a potřebného vybavení velmi **efektivní**. S minimálními náklady mohou napáchat nevyčíslitelné škody, způsobit kolaps finančních, dopravních, mocenských či jiných struktur a v nejhorším případě i ztráty životů. Podle POŽÁRA [104] jsou citovány vybrané formy kyberterorismu:

[54] Zdroj: http://fpc.state.gov/documents/organization/45184.pdf.

- kriminální akce s cílem získání peněz z cizích bankovních kont;
- snahy o získání výhody v oblasti competitive inteligence;
- možnost napadení či dokonce likvidace IS;
- zájmy hackerských sdružení;
- snahy vlád některých zemí, které se intenzivně připravují na vedení kybernetické války určitými opatření již nyní. Tyto státy organizují operace, které mají v praxi potvrdit úspěšnost jejich boje proti kyberterorismu, ale přitom svou skutečnou utajují a maskují;
- šíření extremistických názorů,pornografie, návodů na výrobu jaderných zbraní, omamných prostředků, výbušnin apod.

Klasickým **nástrojem** využívaným ke kyberteroristickým útokům jsou všechny zmíněné hrozby jako viry, DoS a DDoS útoky, spyware či backdoors aj., které mohou poškodit, zničit nebo měnit data, případně vyřadit systémy z provozu. Naznačené aktivity jsou pro společnost vždy velkým nebezpečím. Některé státy, bez ohledu na motivaci pachatelů, pokládají **jakýkoliv útok** na IS za kyberterorismus.

V souvislosti s kyberterorismem, je třeba zmínit další jev, a tím je **kybernetická válka** (cyber war) či také **informační válka** (information war). Vzhledem k tomu, že ICT jsou ve vyspělých státech a ekonomikách integrovány do všech oblastí našeho života, ani armáda není výjimkou. Země na celém světě vyvíjejí a zavádějí kybernetické strategie s cílem zasáhnout velitelské a řídící struktury nepřítele, jeho logistiku, dopravu, systémy včasné výstrahy a další rozhodující vojenské funkce. Informační struktury jsou natolik důležité, že útok proti nim je považován za ekvivalent strategického úderu. Podle NATO review[55] budou stále více napadány IS členských států ze strany netradičního nepřítele, jehož cílem je fyzická destrukce a rozvrat. Ten bude využívat všech zranitelných míst, bez ohledu na umístění. Nutno podotknout, že **potencionálními útočníky** na IS vyspělých států světa jsou zpravidla země na nesrovnatelné technologické úrovni. Což představuje velký paradox, tyto státy se nemohou přípravě na informační či kybernetickou válku efektivně věnovat, ale zároveň jsou také těmito prostředky méně zranitelní.

Klíčovým cílem je dosáhnout informační převahy v prostoru kybernetického bojiště. Z literatury je známo několik úrovní kybernetické války (doplněk, omezená, neomezená). Nakonec se ukazuje, že v informační válce je nejzranitelnější ten, kdo je nejlépe připraven ji vést.

Kyberterorismus a kybernetická, popř. informační válka se stávají vážnou hrozbou pro demokratické státy a lze předpokládat, že v blízké budoucnosti bude tento nebezpečný vývoj stále více aktuální. Proto je třeba věnovat značné úsilí otázce bezpečnosti IS, jak bylo naznačeno v kap. 2 a zahrnout „obranné" plánovaní i na virtuální svět.

55 Zdroj: http://www.nato.int/docu/review.

3.3 Internetové obtěžování a podvody

Následující typy útoků v prostředí internetu dostávají zcela nový rozměr. Internet, resp. jeho služby (e-mail, diskusní fóra, blogy, instant messaging a WWW stránky), umožňují anonymní vyjadřování a šíření různých názorů. Uživatelé internetu mohou páchat různé nezákonné aktivity pod falešnou identitou, díky níž padají veškeré zábrany, které by měli v reálném světě. Do této kategorie trestných činů bychom mohli zahrnout činnosti, které u nás zatím nejsou moc známy. Např. **cyberbullying** (kybernetická šikana), která spočívá v zasílání škodlivých či krutých textů, popř. obrázků prostřednictvím internetu. Podmnožinu těchto činů tvoří **cyberstalking** (obtěžování po internetu), u kterého jde o projev násilí – psychického teroru. Jsou rozeznávány dvě formy cyberstalkingu, jednak rozesílání výhružných e-mailů vyjadřující nenávist, obscénnosti a dále v podobě virů a spamu.

V souvislosti s internetem, prostředkem komunikace, je nutno zmínit - dle Listiny základních práv a svobod - **právo člověka na vlastní názor**. Internet je jedinečným nástrojem k získávání potřebných informací a následném vyjádření vlastních názorů. Jednou z podstat demokracie, resp. demokratické svobody projevu je, že máme právo vyjadřovat jakékoliv názory, avšak s respektováním určitých pravidel. Již se objevilo několik snah cenzurovat internet (USA), zejména tedy webových stránek. Např. organizace *ICRA (Internet Content Rating Association)* se specializuje na vyhodnocování obsahu webových stránek z hlediska přítomnosti sexu a násilí. Systém funguje na bázi dobrovolnosti, kdy webmasteři umístí na svůj web kód, ze kterého internetový prohlížeč identifikuje obsah. Uživatelé si pak nastaví svůj prohlížeč tak, aby byl omezen přístup na stránky, které jsou pro ně, resp. nezletilé, nevhodné. Jistou formu cenzury provádí systémy typu *Echelon*, *Carnivore*, které monitorují e-mailovou komunikaci podle slovníku, který obsahuje seznam slov evokující teroristické hrozby apod.

Cenzura internetu, jako jakéhokoliv jiného nosiče informací, je v demokratickém světě nepřípustná. Mělo by záležet na zdravém úsudku uživatele informací, zda se bude na šířené informace dívat jako na pouhé vyjádření názoru a nenechá se závadným obsahem ovlivnit. Tuto myšlenku však nemůžeme uplatňovat u u nezletilých. Komunistické země uplatňují přísnou kontrolu nad přístupem k internetu. Například v čínských internetových kavárnách je na počítačích nainstalován SW, který omezuje přístup na vládou zakázané stránky a je ustanovena „internetová policie", která má sledovat obsah e-mailů a navštívené webové stránky (např. některé informace pomocí Googlu čínský uživatel nenajde. Není výjimkou, že

„podezřelý" blog může být bez vysvětlení najednou zrušen)[56]. Či příklad z Turecka[57] (2002), kde novela mediálního práva stavěla internet na stejnou úroveň jako ostatní informační média. ISP museli denně na státní úřad zasílat tištěné kopie publikovaných materiálů. Občané KLDR nemají k internetu přístup vůbec. Podobně je tomu tak na Kubě, kde k přístupu na internet mají povolení pouze členové vlády vybraní členi komunistické strany.

Zásadním problém spočívá v určení **odpovědnosti** za „závadný obsah". Pochopitelně si v prvním okamžiku řekneme, že odpovědnost nese sám autor problematického příspěvku, vyjádření apod. Situace je ovšem komplikována anonymitou v internetu a dále tím, že odpovědnost může nést také např. provozovatel diskusního fóra, webové stránky apod. Z toho důvodu na mnoha diskusních fórech najdeme upozornění, že příspěvky urážejícího či vulgárního rázu budou automaticky mazány.

V naší republice je odpovědnost poskytovatele služeb (providera) za obsah informací poskytovaných na internetu upravena v Zákoně č. **480/2004 Sb.**, o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). Dle tohoto zákona **není** provider odpovědný za obsah cizích webových stránek, kterým umožňuje umístění na svém serveru a **nemá** tedy povinnost jejich obsah aktivně monitorovat. Pokud se však dozví o protiprávní povaze obsahu stránek (extremistické názory, dětská pornografie atd.), má povinnost dotčené stránky odstranit, respektive znepřístupnit. Provideři mají dále **povinnost** uchovávat údaje o připojení svých uživatelů a to po dobu půl roku.

3.3.1 Pomluvy, útoky na čest, msty

Jak již bylo výše naznačeno, diskusní fóra, osobní WWW stránky či ICQ[58] nám umožňují vyjádřit se o čemkoliv a komkoliv, bez jakéhosi pocitu provinění, či obavy. Internet je zcela **bezprostředním prostředím** pro jakékoliv reakce, je interaktivní. To, že můžeme reagovat na nějaký příspěvek ihned po přečtení a ještě ke všemu třeba pod úplně jinou identitou, může způsobit nemalé problémy. **Trestněprávní odpovědnost** poskytovatele za obsah závadného diskusního příspěvku můžeme považovat při nezměrném počtu příspěvků za ojedinělou, avšak v žádném případě za nerealizovatelnou. Uplatnění bychom našli např. v případě, že poskytovatel obsahu diskusního fóra, ví o tom, že na tomto fóru je vystaven právně závadný obsah (např.

56 Zdroj: http://www.gio.gov.tw/cz/policy/20060309/2006030904.html.

57 Zdroj: http://technet.idnes.cz/sw_internet.asp?r=sw_internet&c=A020529_5070315_sw_internet.

58 Protokol, využívaný pro přenos krátkých textových zpráv po internetu či také označení konkrétního komunikačního programu.

text otevřeně propagující fašismus), avšak zůstává k tomu zcela nečinný. Další problém ovšem nastává, jak dokázat, že provider o závadném obsahu věděl. [83]

Provozovatelům diskusních fór se nabízí několik možností, jak se zachovat v takovýchto případech. Poněkud náročné řešení je monitorovat nové příspěvky a ty závadné mazat. Dále je možno požadovat registraci návštěvníků diskusního fóra, což ovšem nezaručí 100% úspěšnost. Nejjednodušším řešením je diskusi se závadným obsahem zrušit.

Trestněprávní úprava

Podle TrZ se i v prostředí internetu dá uplatnit **§206** – trestný čin pomluvy, který praví, že kvalifikovaná trestní sazba se použije i tam, kde byl trestný čin pomluvy spáchán jiným, obdobně účinným způsobem na úrovni tisku, rozhlasu či televize. V České republice již padl rozsudek za tento trestný čin (soudní spor se vlekl 5 let).

3.3.2 Vydírání, elektronické výpalné

Trestný čin vydírání je velmi často v prostředí internetu spojován s již zmíněnými **DoS útoky** (kap. 3.2.5), či jinými hrozbami **průniku do systému**, které mají za následek krádež či destrukci dat a citlivých informací. Majitelé různých systémů připojených k internetu (často z oblasti finančnictví), jsou zastrašováni podobnými útoky. Jak již bylo naznačeno v kapitole o bezpečnosti, žádný systém si nemůže být nikdy jist svým dokonalým zabezpečením, a proto instituce raději útočníkům-vyděračům vyhoví a zaplatí **e-výpalné**. Uvedené technologie jsou zneužívány zločineckými gangy, dochází k pronajímaní botnetů a vzniká tak **organizovaný zločin**. Online vydírání je závažný problém, který nebere ohledy na geografické hranice. Pochopitelně může jít také o jakékoliv jiné vydírání prostřednictvím elektronické pošty. Novým typem útoku se stává zaheslování souborů uložených na počítači na dálku. Soubory se stávají jakýmsi rukojmím pachatele, který za jejich odblokování požaduje finanční obnos, tzv. **ransomware**, čili výkupné za software.

Trestněprávní úprava

Na tento trestný čin by se podle TrZ vztahoval **§235 -** trestný čin vydírání, v případě útoku též **§257a** - poškození a zneužití záznamu na nosiči.

3.3.3 Šíření pornografie

Šíření pornografie v prostředí internetu je, po warezu a hackingu, **další nejčastěji páchanou** ilegální aktivitou. Provozovatelé pornografických serverů, kteří

vyžadují registraci a poplatek pro přístup k pornografickým materiálům, tak vydělávají velké peníze. Existují pochopitelně i servery zpřístupňující pornografické materiály zdarma, ty ale své peníze vydělávají prostřednictvím zmiňovaného spyware apod. Vedle webových stránek jsou zdrojem, resp. distribučním kanálem, **sítě P2P**. Tyto sítě jsou využívány také k obchodu s fotografiemi či videonahrávkami, k peněžním transakcím a k informacím týkající se dětské sexuální turistiky. Část distribuce dětské pornografie má komerční charakter a je spojena s mezinárodním organizovaným zločinem.

Asi nejznámější **kauzou**, která se týká odpovědnosti poskytovatele za pornografický obsah, je případ německé pobočky *CompuServe Inc.*, která prostřednictvím svých serverů umožňovala přístup k diskusním skupinám (newsgroups), na kterých uživatelé zpřístupňovali pornografii. Ředitel společnosti byl odsouzen ke dvou rokům vězení a zaplacení pokuty, tehdy v hodnotě 100.000 marek. Odvolací soud však nakonec rozsudek zrušil a obžalovaného ředitele žaloby zprostil.

Z českého prostředí (1991) je znám případ umístění dětské pornografie občanem ČR na freehostingový server *XOOM.com*. Na základě zjištěných logů ze zmiňovaného serveru a z českého freemailového serveru byl pachatel usvědčen (policie tehdy spolupracovala s FBI). [85]

Možným **opatřením** před zahlcením nechtěného pornografického obsahu je využití **autocenzurních filtrů**, kdy si uživatelé nastaví vlastní úrovně. Co se týče zpřístupňování pornografického obsahu nezletilým, je na rodičích, aby buď **blokovali** konkrétní servery nebo využili proxy pro **filtrování** tohoto obsahu. Je třeba zadat metadata, podle kterých jsou webové stránky filtrovány, a to vzhledem ke globálnosti internetu i v anglickém jazyce.

Trestněprávní úprava

Podle TrZ je za trestný čin **§205** – ohrožování mravnosti, považováno šíření pornografických materiálů propagujících násilí, dětskou pornografii, nekrofilii apod. deviace. Další podmínkou trestnosti je zpřístupňování pornografie mladistvým, což je značný problém, neboť je velmi obtížné zjistit, kdo takové stránky navštěvuje. MATĚJKA [85] uvádí zveřejněný právní názor, že by pornografické materiály neměly být přes internet nabízeny – protože v případě, že by se prokázalo, že se k takovému obsahu dostala osoba mladší 18-ti let, byla by tím založena právní odpovědnost provozovatele stránky. Ti se však brání tím, že je na stránkách výslovně označeno, že obsah není určen pro osoby této věkové kategorie. Jinak je šíření pornografie v naší republice beztrestné.

3.3.4 Extremismus

Extremismus je chápán především jako **projev nesnášenlivosti** doprovázený agresivním jednáním vůči zjevně odlišným jedincům či skupinám odlišných jedinců. Hnutí a skupiny, které můžeme označit jako extremistické to mají podle DASTYCHA [37] s **medializací svých myšlenek** velmi těžké, a tak využívají internetu, jakožto média „pro všechny". Neexistuje zde regulace ani cenzura obsahu, každý si zde může říkat a šířit, co chce.

Internet je proto pochopitelně ideálním prostředkem pro šíření názorů extremistických skupin. V naší republice jde především o různé militantní náboženské sekty, nacistická, neonacistická, anarchistická, ekoradikální, fašistická aj. seskupení. O stránky s podobnou tematikou není na internetu nouze, jsou využívány také k **získávání** nových příznivců. Podle dokumentů Ministerstva vnitra[59] se v roce 1999 na internetu objevily stránky, které nabízely dětem počítačové hry s rasistickým podtextem, ilustrované knížky se skrytě rasistickou a extremistickou problematikou a dokonce i křížovky uzpůsobené pro dětského řešitele.

Internet je využíván i ke **komunikaci** mezi jednotlivými národními organizacemi těchto skupin a také se jeho prostřednictvím **distribuují** CD s extremistickými hudebními nahrávkami.

Na českém webu můžeme najít zejména weby popisující antisemitské názory a činnosti neonacistických skupin. Postižitelnost takovýchto skupin na internetu je podle KUCHAŘÍKA velkým problémem. *„Celá oblast extremismu těží z toho, že v některých zemích není prezentace těchto názorů trestná a je brána jako svoboda projevu"*. [130] Většina stránek je totiž registrována v USA, kde není extremismus považován za trestný čin. Policie je proto nucena spolupracovat se zahraničím.

Na začátku tohoto roku byl uzavřen případ okolo webu ***Vesjolyje kartinky***, na který bylo podáno trestní oznámení za zneuctění obětí holocaustu. Jde o satirický web, který má podle svých tvůrců přinášet *„vtipné, řemeslně dobře zvládnuté, inovativní i jinak urážlivé fotomontáže"*. Na svých stránkách mají mj. rubriku *„Chcete nás žalovat?"*, kde se po vyplnění formuláře objeví nechvalná hláška. Na podzim loňského roku se na tomto webu objevila montáž loga reality show Vyvolení - na pozadí brány koncentračního tábora bylo použito na logu slovo VyHubení. Na tuto kauzu je nahlíženo jednak jako na drsnější legraci, jednak jako na zneuctění. Výsledek případu je takový, že autoři webu vyváznou bez trestu, neboť jim policie nedokázala snahu o znevažování holocaustu ani propagaci fašismu. Jde o velmi sporný případ, kde se

[59] Zdroj: http://www.mvcr.cz/extremis/1999/zakl_tr.html.

těžko určují hranice „legrace" a vědomého poškození - není zde posuzována subjektivní motivace. [132]

Trestněprávní úprava

Projevy extremismu na internetu je možno posuzovat podle TrZ **§198** – hanobení rasy národy a přesvědčení, dále podle **§198a** – podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod a také je možno uplatnit **§260** – podpora a propagace hnutí směřujících k potlačení práv a svobod člověka. Extremistické weby by měla omezit jednotná **úmluva EU** k potírání extremismu na internetu.

3.3.5 Šíření poplašné zprávy

Dalším způsobem zneužití elektronické pošty je zasílání různých falešných varování **(hoaxes)** či prapodivných historek **(urban legends)**, které mají za úkol vyvolat ve čtenáři **paniku** či **zasáhnout jeho emoce**. Většinou se jedná o neškodná poselství. Mezi nejčastější patří varování o nových, avšak neexistujících, virech **(virus hoaxes)** a srdceryvné příběhy o záchraně lidského života. Dá se říci, že škodí nepřímo. Zahlcují však e-mailové schránky, okrádají uživatele o čas a hlavně ho přivádí do světa lží. Jediné co může uživatel před rozhodnutím, zda e-mail přepošle, či smaže, je **ověřit** si zprávu na speciálních serverech, které shromažďují veškeré hoaxes a urban legends, které obíhají internetem (např. www.hoax.com, www.hoaxbuster.ciac.org, www.hoax.cz, www.snopes.com).

Hoax se šíří vlastně pouze pomocí uživatelů, kteří ho v rámci solidarity rozesílají dalším a dalším uživatelům. *„Zlí jazykové tvrdí, že hoax je vlastně vir, který napadá tu část, která se nachází mezi židlí a klávesnicí"*. Přeposíláním e-mailů dochází ke zveřejňování velkého množství adres, které mohou být **zneužity** spammery. Typická ukázka hoaxe, zesměšňující aktivity BSA, je uvedena v příloze č. 5.

Trestněprávní úprava

Šíření poplašné zprávy není českým právem postihnutelné, ale v případě, že by na základě úmyslně rozeslané zprávy došlo k znepokojení mezi větším počtem lidí, bylo by možné uplatnit **§260** – trestný čin šíření poplašné zprávy. [85] Těžko si však můžeme představit, jakým způsobem by se hledal a usvědčoval přímý autor zprávy, která obíhá mezi tisíci uživateli, kteří se vlastně stali obětí hoax.

3.3.6 Spamming

Spam[60], čili **nevyžádaná pošta** často s komerčním propagačním obsahem, se stává každodenní přítěží uživatele elektronické pošty. Zřejmě první spam napsal zaměstnanec *Digital Equipment Corporation* v roce 1978 na adresy tehdejší sítě ARPANET. Dalším spamem byla zpráva (s předmětem *make.money.fast!!*) rozeslána do diskusních skupin sítě USENET.

Mezi současný typický spam patří různé nabídky podvodného zbohatnutí, produktů typu Viagra atd. Na spamming je pohlíženo **ze dvou stran** – pro subjekty, které využívají internet jako způsob své propagace, jde o cenově výhodný nástroj distribuce. Koncoví uživatelé, tedy adresáti, jsou pochopitelně opačného názoru. Na kolik je tato činnost efektivní je otázkou, podle statistik z roku 2004 [110] 4% uživatelů už někdy zakoupila zboží nabízené ve spamu.

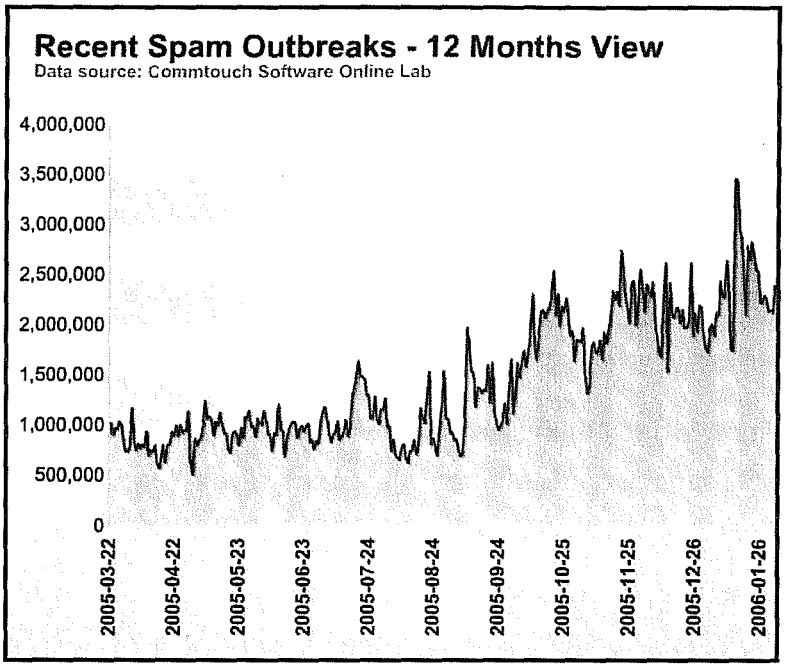
Cílové e-mailové adresy, které zneužívají specializované direct marketingové firmy, jsou získávány většinou **automatickým prohledáváním** různých diskusních fór, konferencí nebo WWW stránek. Mezi další zdroje adres patří **registrace** různorodých služeb, které jsou poskytovány „zdarma" či posbírané adresy z hoaxů. Takto vytvořené databáze e-mailových adres jsou vysoce ceněným obchodním artiklem. Spammeři většinou zneužívají pro rozesílání e-mailů cizí SMTP servery, aby se tak vyhnuli umístění na tzv. black list spammerů a následně nebyli blokováni.

Poměr doručeného spamu a korektních e-mailů rapidně stoupá. V roce 2003 bylo zjištěno, že 30% všech odeslaných e-mailů tvořila nevyžádaná reklama, v roce 2004 již šlo o 60%. Podle studie společnosti *Commtouch*[61] pochází **99% celosvětového objemu spamu** pouze z pěti zemí (USA – 62%, Čína, Jižní Korea, Rusko a Brazílie). V **Evropské Unii** se drží prvenství Rakousko. [89] Následující obrázek č. 7 představuje graf, který zobrazuje průběh spamových útoků během téměř jednoho roku (2005/03 – 2006/01). Musíme připustit, že i přes menší výkyvy jde o stále stoupající trend.

---

60 Používá se též zkratka UBE/UCE (Unsolicited Bulk/Commercial E-mail). Pro opak spamu, tj. žádanou poštu zaslanou konkrétní osobou se specifickým jednorázovým účelem, se řidčeji používá termín *ham* (zdroj: http://cs.wikipedia.org).

61 Commtouch® Software Ltd. byla založena roku 1991 a specializuje na problémy e-mailové komunikace. Vyvíjí speciální detekční antispamový SW, poskytuje antivirovou ochranu uživatelům na celém světě. Monitoruje spamové aktivity, vytváří statistiky, nabízí kalkulátor nákladů, které firmy vynaloží na spam - samozřejmě s porovnáním nákladů vynaložených na nabízené antispamové řešení.



Obr. č. 7 – Spamové útoky během roku 2005, převzato z http://www.commtouch.com

Na webových stránkách zmíněné společnosti (sekce *Research Lab*) můžeme sledovat aktuální spamové hrozby, které momentálně kolují internetem. **Monitoring** zahrnuje lokaci spamu (též grafické znázornění), jeho URL, předmět uvedený v hlavičce e-mailu, počet útočníků a „masivnost" spamu. V příloze č. 4 je zobrazen fragment stavu z 22.3.2006. Z dalších statistických údajů se dozvíme, že v měsíci únoru:

- 2 ze 3 e-mailů tvořily spam (58,2 %),
  - u společností 46,4%
  - u jednotlivců 71,5%
- země s nekontrolovatelným množstvím spamu – USA, Rusko (téměř 75% z celé e-mailové komunikace),
- země s nepatrným množstvím spamu – Francie, Maďarsko (26% z celé e-mailové komunikace),
- nejčastěji využívané domény – hotmail.com (3%), Yahoo.com, msn.com, 0733.com a Gmail.com (0,5%),
- nejčastější kategorie obsahu spamu – farmaceutické výrobky typu Viagra (67%), dárky (14%), finance (8%), porno, SW a ostatní (11%).

Některé freemailové služby poskytují též **statistické údaje** o množství přijatých spamů či zavirovaných e-mailů. Např. *Volný* poskytuje takovýto přehled nevyžádané pošty za poslední tři měsíce (tabulka č. 2):

	Celkem	Virů	Spamů
Březen 2006	550	0 (0.0%)	272 (49.5%)
Únor 2006	723	0 (0.0%)	314 (43.4%)
Leden 2006	1220	3 (0.2%)	793 (65.0%)

Tabulka č. 2 – Poměr doručených e-mailů a spamu (zahrnuje i smazané zprávy)

Na konci roku 2004 *Lycos Europe* odstartovala kontroverzní webovou akci *„Make love not spam"*[62] - kdy si uživatelé mohli stáhnout spořič obrazovky, který spouštěl DDoS útoky na počítače spamerů. Kampaň byla po týdnu ukončena.

Stoprocentně účinné **opatření** proti spamům v současnosti v podstatě neexistuje. Nabízí se však několik přístupů, které mohou problémy v dané oblasti alespoň zmírnit. Uživatel sám může filtrovat poštu, blokovat spamovské zdroje (některá freemailová služba umožňuje blokaci všech podezřelých e-mailů i podle domény), instalace antispamových programů (*Anti-Spam Enterprise Solution, GFI MailEssentials, JunkSweep* pro Outlook atd.), či skrývání adres.

Trestněprávní úprava

V České republice je problematika spamu ošetřena v Zákoně o některých službách informační společnosti č. **480/2004 Sb.** (mezi veřejností mylně označován jako antispamový zákon), který vyžaduje, aby měl odesílatel nevyžádané pošty předem **výslovný souhlas** od příjemce svých zpráv. Kontrolu a dodržování má na starost Úřad pro ochranu osobních údajů. K tomuto úřadu mohou být také podávány žaloby proti spamerským firmám. Za zasílání nevyžádaných obchodních sdělení, spamu, navrhuje zákon **sankci** ve výši až 10.000.000 korun. Podobná legislativní opatření jsou zavedena v řadě zemí. Zatím se však nezdá, že by to vedlo k poklesu spamu. Vysvětlení je nasnadě: 99% spamu pochází ze zahraničí.

3.3.7 Internetové podvody

Kromě již zmíněného phishingu a pharmingu jsou na internetu provozovány různé podvodné aktivity, které nevyžadují příliš sofistikovaných technologií. Většinou jde o **finanční podvody**, kdy se důvěřivé oběti nechají nalákat na slíbené enormní zisky (obchodování s cennými papíry, různými komoditami atd.). Jde o podvody typu **letadla či pyramidy**, které byly zmíněny již v úvodní kapitole. Tito „obchodníci" se

62 Zdroj: http://www.makelovenotspam.com.

prezentují na amatérských WWW stránkách, používají adresy na freemailech, přesto se honosí vysokými ratingy, které mají navodit pocit důvěryhodnosti. Bohužel se i dnes najde velký počet důvěřivých lidí, kteří se na podobné nabídky nechají nalákat. [85] Podle FBI se 46% internetových podvodů odehrává na **aukčních** stránkách (např. *eBay*). Uživatelé si v domnění seriózní koupě objednají zboží, zaplatí, leč z důvodu falešné identity, se produktu už nedočkají. Na vzestupu jsou dle studie *McAfee* [87] **investiční a akciové** podvody. Ty spočívají v nákupu akcií relativně neznámých společností, o kterých jsou následně rozšířeny zfalšované obchodní informace. To má za následek nadhodnocení a navýšení ceny akcií, které následně prodají. Sítě investičních internetových podvodníků mají základny po celém světě a burzy vydávají černé listiny provozovatelů těchto podvodů. K dalším podvodům ve finanční oblasti dochází prostřednictvím falešně získaných identit využívaných k získání **kreditních karet**, které se staly standardem při placení po internetu. Na rozdíl od používání karet při klasickém nakupování, zde stačí zadat číslo kreditní karty a datum expirace, žádné další ověření není nutné. Základním bezpečnostním prvkem při placení po internetu je **zabezpečená komunikace** mezi počítačem zákazníka a počítačem - serverem internetového obchodníka.

Trestněprávní úprava

Mezi skutkové podstaty, které by se zde daly uplatnit patří trestný čin podvodu - **§250** TrZ, zpronevěry - **§248** TrZ a provozování nepoctivých her a sázek - **§250c** TrZ. [85]

Na závěr celé třetí kapitoly je vhodné uvést shrnutí **bezpečnostních a organizačních opatření**, kterých by se uživatelé ICT měli držet, aby nepřišli ani o data a informace, ani o finanční částky. Jde o jakousi obecnou prevenci proti nebezpečím internetu, dle anglické kampaně *Get Safe Online*[63], která spočívá v následujících radách:

- instalace a aktualizace antivirového, antispywarového apod. SW,
- instalace osobního firewallu,
- zálohování,
- instalace oprav (záplat) OS a aplikací,
- používání prostého textu místo HTML e-mailů,
- mazání spustitelných příloh,
- používání důmyslných hesel,

63 Zdroj: http://www.getsafeonline.org.

- šifrování elektronické komunikace (používání elektronického podpisu, PGP[64] atd.)
- ignorace spamu a odkazů typu *„Unscribe"* - ohlášení urážlivých, obtěžujících nebo podvodných e-mailů ISP a společnosti, jejíž jméno bylo zneužito.

Rady pro online transakce:

- neprozrazovat hesla, PINy apod.,
- nevyplňovat e-mailové formuláře,
- neklikat na odkazy v e-mailech,
- hledat na stavovém řádku prohlížeče symbol zámku,
- pravidelně kontrolovat bankovní účty a hlásit cokoliv podezřelého.

Můžeme dodat dubnovou informaci, kdy Ministerstvo informatiky ČR oznámilo spuštění nového portálu *Bezpečně on-line* (www.bezpecneonline.cz), který je inspirován výše uvedeným anglickým projektem (spíše jde tedy o kopii a překlad portálu). Web je zaměřen na počítačovou bezpečnost ve třech oblastech: *Chraňte svůj počítač* (viry, zálohy, antivirové programy atd.), *Chraňte sebe* (e-bankovnictví, e-nakupování, nebezpečný obsah atd.) a *Chraňte svoji firmu* (osobní údaje, šifrování, IBP atd.).

64 Pretty Good Privacy, tzn. „dost dobré soukromí" (Phil Zimmerman, 1991). PGP je určeno pro bezpečný přenos elektronické pošty.

4 Srovnání českého a zahraničního prostředí

Jak již bylo naznačeno v úvodu, stav a vývoj EIK v ČR je - díky zapojení IT do společnosti – zpožděn, nicméně dopad kybernetického zločinu je stejný všude na světě, záleží jen na intenzitě poškození, zneužití IS, resp. dat a informací, ve vztahu k jejich důležitosti. Rozdílná jsou opatření, organizační zajištění a **legislativní řešení**. Zřejmé rozdíly, jak uvádí SMEJKAL [122], jsou zejména mezi systémy „civil law" a „common law". V rámci anglického systému „common law" mohou být potřebná pravidla vytvořena i činností soudců na základě precedenčních rozhodnutí. Ta aktualizují určitý zákon tak, aby bylo zřejmé, že se na nové technologie i pro příště automaticky vztahuje. Internet je sice globálním médiem, ale žádné mezinárodně závazné normy, které by upravovaly jeho činnost, resp. internetové zločiny, zatím neexistují.

Porovnání stavu EIK v České republice a zahraničí je realizováno formou přehledu vybrané aplikované legislativy, zajímavých případů a činností odpovědných institucí. Poměrně podrobná charakteristika je provedena u naší republiky a USA. Statistické údaje týkající se pirátství jsou uvedeny z globálního pohledu pro vytvoření komplexní představy o současném stavu.

4.1 Česká republika

Naše republika se musí vypořádávat se stejnými problémy EIK jako ostatní země světa. Můžeme říci, že patříme k zemím s průměrným stavem kybernetických trestných činů. Rozdílné jsou možnosti represivních a preventivních složek, které se odvíjí od vyspělosti ICT, zkušeností a možné spolupráce. Ve vyspělých zemích vznikají speciální týmy pro boj s kyberzločinem, většinou na centrální úrovni, popř. na vyšší úrovni jednotlivých územích celků. V naší republice se o potírání EIK stará Oddělení informační kriminality, které má ještě hodně před sebou. ČR má, na rozdíl od sledovaných zemí, zřízen vrcholový orgán státní správy – *Ministerstvo informatiky*, které mj. zastřešuje webový portál *Bezpečně online.*

Co se týče legislativního zajištění EIK, jsou zde zmíněny pouze zajímavosti týkající se daných předpisům (legislativa byla uváděna průběžně ke konkrétním případům). **Obecně** můžeme říci, že v naší legislativě neexistuje konkrétní zákon vztahující se k EIK, jednotlivé problémy jsou roztroušeny v různých právních předpisech, a to ne vždy zcela ideálně. V některých případech se s trestnými činy páchanými elektronicky vůbec nepočítá, či nejsou dostatečně definovány jejich skutkové podstaty.

Dle SMEJKALA [121] mezi příčiny **legislativních problémů** patří variabilita možných jednání, převažující distanční charakter činu, existence důkazů pouze v elektronické podobě a jejich snadné zahlazení. Některé jevy EIK lze obtížně přiřadit ke konkrétním skutkovým podstatám, jako např.:

- tzv. **online obtěžování** (politický, náboženský, obscénní aj. charakter), které český právní řád nezná,
- **hromadné útoky** (DoS, DDoS) – spekulace o § 257a či § 257 TrZ,
- **neoprávněného užívání počítače dálkovým způsobem –** podle § 249 TrZ se předpokládá neoprávněné užívání cizí věci,
- **hacking** bez poškození, zničení a využití údajů nelze kvalifikovat podle § 257a.

V loňském roce vyvolal ***Trestní zákon č. 140/1961 Sb., ve znění pozdějších předpisů***, resp. jeho navrhovaná novela (zařazení skutkových podstat podle Úmluvy Rady Evropy o počítačové kriminalitě), bouřlivou diskusi a následnou petici mnoha odborníků zejména z oblasti počítačové bezpečnosti a IS. Projednávaná verze návrhu TrZ by totiž umožnila posílat vědecké pracovníky a administrátory (za kryptoanalýzy, penetrační testy) do vězení - na podkladě stejného ustanovení TrZ jako hackery, páchající skutečnou trestnou činnost. Podle novely by mělo být trestné:

- opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 205),
- poškození záznamu v počítačovém systému na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 206).

Problém spočívá v tom, že u převzatých skutkových podstat není uveden text obsahující podmínku trestnosti, kterou je protiprávní cíl. [125]

Významným legislativním předpisem podporující bezpečnost elektronické komunikace v oblasti elektronického obchodování je ***Zákon č. 227/2000 Sb., o elektronickém podpisu***. Základní princip spočívá ve zrovnoprávnění elektronických zpráv s klasickou, papírovou formou komunikace. Zákon se zabývá základními pojmy používanými v obchodování. Zneužívaní elektronického podpisu je také identifikováno jako jedno z možných nebezpečí, které přinášejí moderní informační technologie. [31]

V loňském roce spatřil světlo světa ***Zákon č. 127/2005 Sb., o elektronických komunikacích***, který nahrazuje Zákon č. 151/2000 Sb. „o telekomunikacích". Zásadní změna spočívá ve stanovení principu, že regulace bude uplatňována jen tam, kde je to skutečně nezbytné. Kvůli tomu, že zde neexistuje dostatečná konkurence, díky které by si trh poradil sám - a i v takovém případě má regulace směřovat k tomu, aby se trh rozvíjel, aby regulace mohla přestat a trh se

mohl rozvíjet sám a bez regulace. Zákon zjednodušuje systém získání oprávnění pro podnikání v oblasti elektronických komunikací.[65]

V letošním roce se projednávala novela ***Zákona č. 365/2000 Sb., o informačních systémech veřejné správy*** (zákon č. 81/2006 Sb.). Ta vychází z předchozích zkušeností, reaguje na rozvoj ICT a dává základ pro další postupné zavádění služeb e-governmentu. Cílem novely je zvýšení efektivity při pořizování a obnově IS veřejné správy, nastavení transparentních a standardizovaných procesů při zavádění a správě IS veřejné správy. Dalším bodem je připravení vhodného prostředí pro rozšiřování a zvyšování kvality služeb, které poskytuje veřejná správa občanům a podnikatelům.[66]

V roce 2005 došlo k podepsání ***Úmluvy o počítačové kriminalitě (ETS 185) Českou republikou***.

Mezi **konkrétní trestné činy**, které jsou **nejvíce** zastoupeny v naší republice patří (řazeno podle četnosti a závažnosti) [1]:

- zakázaná pornografie,
- extrémistické projevy,
- zneužití platebních a obchodních systémů v síti internet,
- porušování autorského práva,
- pomluvy a diskreditace osob,
- zneužívání dat, včetně útoků na data,
- podvodné e-maily, spamy, hoaxy.

Podle zjištěných informací [31] dochází v ČR k oslabení počtu útoků po internetu a k poklesu zájmu pachatelů o medializaci. Nebezpečnost útoků zároveň stoupá a přibývá pachatelů, zneužívajících svých znalostí za úplatu. Co se týče **softwarového pirátství** – dle poslední globální studie[67], kterou pro BSA vypracovala analytická společnost IDC[68] vyplývá:

- 41% pirátského software (rok 2003 - 40%) – svět 35 % ,
- ztráta 132 miliónů amerických dolarů – svět 33 miliard amerických dolarů,
- za posledních deset let se míra nelegálního SW snížila o 20%,
- země s **nejvyšší mírou** softwarového pirátství (okolo 90%): Vietnam, Čína, Ukrajina, Indonésie a Rusko,
- země s **nejnižší mírou** (okolo 20%): Singapur, USA, Nový Zéland, Dánsko, Lucembursko, Finsko a Švédsko,
- míra softwarového pirátství v **EU** zobrazena v příloze č. 6.

65 Zdroj: http://www.micr.cz/scripts/detail.php?id=205.

66 Zdoj: http://www.micr.cz/scripts/detail.php?id=3227.

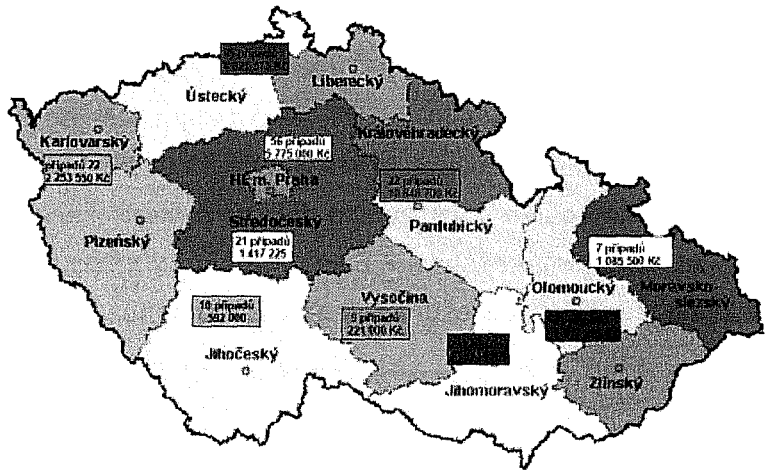
67 BSA zohledňuje pouze případy týkající se přidružených výrobců SW.

68 International Data Corporation (http://www.idc.com) – přední světová společnost v oblasti průzkumu trhu a poradenství pro ICT.

Tímto výsledkem tak ČR neobhájila svůj loňský „úspěch", kdy se jako jediná východoevropská země prosadila mezi dvacet nejlépe hodnocených zemí světa. Její místo zaujalo Portugalsko, poté - co snížilo svou míru softwarového pirátství o jeden procentní bod na 40 %. Podle studie by **snížení** míry softwarového pirátství o 10% do roku 2009 způsobilo:

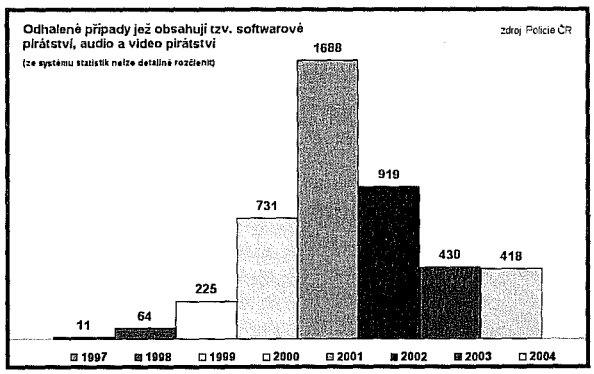
- růst tuzemského IT sektoru z 47 na 58 %,
- vznik 2 900 nových placených pracovních míst v oblasti IT,
- přírůstek k domácímu HDP ve výši 951,9 milionu dolarů,
- dalších 96,2 milionu dolarů ve formě daňových odvodů.

Nejvíce případů BSA eviduje v Praze, severních Čechách a na jižní Moravě. Co se týče výše způsobených škod, na prvním místě se umístily východní Čechy (téměř 11 milionů korun). Konkrétní počet případů a způsobené škody v jednotlivých regionech jsou znázorněny na následujícím obrázku č. 8.



Obr. č. 8 - Statistika počtu případů použití ilegálního softwaru za období 2004-2005, zdroj: http://i.iinfo.cz/urs/bsa-114191486726367.png

Ze statistických údajů Policie ČR, které evidují případy softwarového, hudebního i filmového pirátství dohromady, je patrný klesající trend, viz obrázek č. 9. Jde pochopitelně pouze o odhalené případy, takže skutečný počet případů je mnohonásobně vyšší.



Obr. č. 9 – Přehled odhalených případů pirátství v ČR, zdroj: Policie ČR

4.1.1 BSA

Dříve jsme na stránka BSA mohli najít pobídku k udání uživatele nelegálního SW zavoláním na horkou linku či zasláním údajně „anonymního" e-mailu (server *Zatepla.cz*). Dnes již BSA od těchto praktik upustila a přiklání se spíše k prevenci (možnost otestovat počítač, formulář pro zpětnou vazbu, informace). Zajímavý je případ[69], kdy se BSA lapila do vlastních sítí. Společnost *Digisys* byla nařknuta z instalace nelegálního SW na prodávané počítače a podala žalobu na BSA za nekorektní označení společnosti na jejich stránkách. BSA byla nucena se omluvit a zaplatit pokutu. Zajímavé na celém případu je, že původní BSA CS se zaplacení částky vyhnula vstupem do likvidace.

BSA provozuje osvětové **kampaně** na podporu prevence softwarové kriminality. Ostře kritizovaná kampaň z roku 2002 spočívala v rozeslání černých pytlů s videonahrávkami brutální policejní razie na softwarové piráty. V obálkách byly rozeslány dva dopisy - jeden za Policii ČR, druhý za BSA. Policie garantovala obsah svého dopisu, oproti písemnosti BSA, kterou nikdy neakceptovala. Převažoval v něm represivní aspekt nad preventivním. V rámci současné kampaně BSA informuje 10 000 českých a slovenských firem o rizicích plynoucích z nelegálního užívání SW a možných obranách prostřednictvím bannerů, dopisů a posléze telefonních hovorů. Kampaní chce BSA zdůraznit, že za softwarové pirátství může být uložena pokuta až pět milionů korun či odsouzení až k pěti letům vězení.

4.1.2 IFPI

Institucí, která má za úkol **hájit zájmy** výrobců zvukových záznamů, je národní skupina IFPI ČR (www.ifpicr.cz) - ***Mezinárodní federace fonografického průmyslu***. Je způsobilá vypracovat a pro účely trestněprávního řízení předložit posudky o nelegálnosti nahrávky zaznamenané na nosiči. IFPI má zastoupení téměř ve všech zemích světa.

Přestože počet legálních downloadů roste, hudební internetové pirátství zůstává, podle IFPI, stále velkým problémem. Celkový počet skladeb nelegálně umístěných na internetu ke stažení, oproti minulému roku mírně poklesl, a to i přes masivní rozšíření kvalitního připojení k internetu. Co se týče aktuálních statistických údajů, můžeme dle IFPI [72] shrnout:

- způsobená škoda ve výši 290 milionů korun (2004 – 212 milionů korun , 2003 – 174 milionů korun),
- odhaleno 1455 případů hudebního pirátství,
- vzestupný trend - a to ve všech sledovaných ukazatelích,

[69] Zdroj: http://www.digisys.cz/bsa.htm.

- ilegální stahování prostřednictvím P2P sítí může reprezentovat až 60 % pirátských aktivit,
- ČR zařazena mezi 31 zemí, kde se prodá více padělaných než legálních disků.

V roce 2000 IFPI iniciovala kampaň *Kopírování zabíjí hudbu*, doprovázenou vydáváním tzv. nevypálitelných CD (nejznámější CD Daniela Bárty Illustratosphere). [85] Při takovýchto a podobných kampaních se i umělci staví na dvě protichůdné strany. Na jedné ti, kteří se pustili do soudních sporů (např. Metallica) a na druhé ti, kteří se postavili na stranu P2P (např. Manu Chao).

Pro srovnání zde uveďme globální statistické údaje, které IFPI uveřejnila (www.ifpi.org):

- 7 z 10-ti uživatelů (potencionálních zákazníků hudebních obchodů) si uvědomuje rozdíl mezi legálním a nelegálním opatřováním hudby,
- zahájeno 7000 akcí proti uživatelům, kteří porušují zákon uploadováním souborů ke sdílení v Rakousku, Kanadě, Francii, Německu, Itálii, Velké Británii a USA,
- hodnota pirátské hudby činí 4,6 miliard amerických dolarů,
- stoupl počet legálně stažených hudebních souborů nad 200 miliónů kusů za rok 2004 (2003 pouze 20 miliónů kusů),
- 34% všech hudebních CD, DVD (1,2 miliardy nosičů) je nelegální – každý třetí disk je padělaný,
- CD-R pirátství stouplo o 6% (560 milionů nosičů), téměř polovina prodaných ilegálních nosičů pochází z Latinské Ameriky,
- DVD pirátství činilo minimálně 20 milionů prodaných kusů,
- zlikvidováno 87 výrobních linek, zadrženo okolo 30 000 vypalovaček, 71 milionů prázdných médií a 12 000 pirátů,
- země s nejvyšší mírou hudebního pirátství: Paraguay (99%!), Čína, Indonésie, Mexiko, Indie, Rusko, Brazílie, Ukrajina, Španělsko (24%).

Dalším seskupením, které se snaží bojovat proti pirátství v České republice, je ***ČPU - Česká protipirátská unie*** (www.cpufilm.cz). Posláním této unie jsou aktivity v oblasti boje proti porušování práv k audiovizuálním dílům s výjimkou videoklipů. Sleduje rippované filmy, downloading via P2P, dekodéry, streaming aj. Na filmové piráty se také pořádají razie[70], jedna z posledních se zaměřila i na Evropu, především Rakousko a Polsko. Celá akce byla pod záštitou Interpolu ve spolupráci s místní policií, bylo zatknuto více než 35 osob a prohledáno přes 300 kanceláří. Podobná akce by se měla konat také v ČR, neboť

[70] Zdroj: http://www.mpx.cz/ZAJIMAVOSTI/Dalsi-velky-zatah-na-piraty-v-Evrope-a-mozna-i-CR.html.

Interpol již požádal české úřady o řádnou spolupráci. Nicméně zatím se česká policie razie nezúčastnila.

Těžko konstatovat, na kolik jsou veškeré publikované statistiky týkající se pirátství důvěryhodné. Sami poskytovatelé dat udávají, že nemají přesné údaje a ztráty propočítávají z celkového počtu pirátských kopií, kdy se předpokládá, že každý vlastník by si místo pirátské kopie pořídil originál. O ignoraci kupní síly obyvatelstva nemluvě. To však nic nemění na faktu, že pirátství představuje hlavní výzvu pro světovou ekonomiku.

4.1.3 Policie ČR

Pojem „softwarová policie" se pomalu, ale jistě dostává do povědomí uživatelů internetu, a to spíše v negativním smyslu. Co má tato skupina na svědomí, kde a kdy se vzala, je přiblíženo v následujícím odstavci. V případě, že bychom chtěli najít konkrétní informace, kontakty na webových stránkách Ministerstva vnitra, budeme neúspěšní. Následující popis vychází z publikovaných rozhovorů a článků na internetu [1], [49] a ročníkové práce Jana Ambrože – *Občan a Policie ČR versus informační kriminalita*.

Oddělení počítačové kriminality vzniklo v Kriminalistickém ústavu Praha (KÚP) oficiálně k 1.1. 1993, věnovalo se pouze rozvíjení a realizaci nového kriminalistického expertizního oboru. Teprve mnohem později (1998) bylo pracoviště pojmenováno výstižněji: **Oddělení počítačové expertizy**. Spadalo pod Ředitelství služby kriminální police Policejní prezidia ČR. Vedoucím této skupiny byl major Dastych a hlavní oblastí činnosti bylo softwarové pirátství. Tato činnost byla postupně přenesena na základní útvary služby a vyšetřování kriminální policie (dále ÚSVKP) na úrovni krajů a okresů. KÚP Policie ČR byl iniciátorem vzniku pracovní skupiny, jejímž cílem je přispět k potírání informační kriminality - **Forensic Information Technology Working Group** (FIT-WG).

Díky změně struktury byla v květnu roku 2005 založena **Skupina informační kriminality**. Toto oddělení tvoří zhruba 20 policistů, denně se v průměru setkají s dvěma internetovými trestnými činy. Zaměřuje se na odhalování, vyšetřování a monitorování informačních kriminálních aktivit. Úkoly spočívají v zajišťování důkazních materiálů na internetu, servisní činnosti a podpoře ÚSKVP. Informace sbírá oddělení od svých informátorů v terénu, od občanů (kontaktují policii e-mailem; zejména o obsahu nelegální pornografie a extremismu) a využívá také poznatků zahraničních oddělení. Skupina informační kriminality také zajišťuje vzdělávací aktivity uvnitř PČR a komunikuje s obdobnými útvary v zahraničí.

Podle Karla Kuchaříka[71] (vedoucího této skupiny) mezi **problémy**, s kterými se musí oddělení informační kriminality potýkat, patří:

- nedostatečná statistická výbava,
- nedostatečná akceschopnost,
- technologické nedostatky,
- právní nedostatky,
- podceňování informační kriminality společností.

Nejčastěji **vyšetřované případy** se týkají pornografického materiálu na internetu, extremistických projevů, zneužití platebních a obchodních systémů, porušování AP, pomluv a diskreditace osob.

Jak je možno postřehnout z různých diskusních fór (např. na www.lupa.cz), je činnost softwarové policie v očích uživatelů spíše pro smích.

Problematiku odhalování, vyšetřování a prevenci počítačové kriminality řeší také **Policejní akademie ČR**. V rámci této činnosti pořádá konference, vydává odborné sborníky a zpracovává studie týkající se problematiky EIK. [31]

4.2 Vybrané zahraniční zkušenosti

Pro porovnání zkušeností a postupů v oblasti EIK bylo vybráno šest zemí. Americký kontinent zastupují svérázné USA a poněkud liberálnější Kanada. Z evropských zemí bylo vybráno tradiční Německo a konzervativní Velká Británie. Dalšími zvolenými zeměmi je Austrálie a Taiwan, které dosahují překvapivých výsledků.

4.2.1 USA

USA jsou asi nejprogresivnější zemí v oblasti používání ICT a tedy i patřičných zákonů a institucí. Situace je zde komplikována koexistencí federálních a státních zákonů, přičemž „počítačové právo" je upravováno jak v trestněprávní, tak veřejnoprávní i soukromoprávní oblasti. [121] V následujících odstavcích jsou uvedena vybraná specifika americké EIK:

- *U.S. Copyright Law* upravuje ochranu **duševního vlastnictví** – rozdíl oproti našemu systému úpravy autorských děl je **registrační princip**, kdy podmínkou pro požívání ochrany je nutnost jeho přihlášení (U.S. Copyright Office). Ochrana SW jako literárního díla je ustanovena v *Computer Software Copyright Act.*
- Trestné činy jsou definovány v článku ***18 U.S.C*** *Crimes and Criminal Procedure.*

[71] Uvádí Jan Ambrož ve své ročníkové práci - Občan a Policie ČR versus informační kriminalita.

- *CAN-SPAM Act* z roku 2003 přikazuje odesílatelům e-mailů, aby příjemci měli možnost odmítnout jakoukoliv budoucí poštu. Současně mají výrazně označovat zprávy se sexuálním podtextem.
- Základní rámec americké právní úpravy EIK tvoří dva americké zákony *Digital Millenium Copyright Act* (DCMA) – upřesňuje podmínky AP především ve vztahu k internetu a *Communication Decency Act* (CDA) – část federální telekomunikačního zákona upravující omezení pro obsah elektronické komunikace. Přijetí těchto zákonů předcházely dvě odlišná soudní rozhodnutí, která se týkala pomluvy via diskusní fórum.

DCMA je poměrně rozsáhlý zákon z roku 1998, skládá se z pěti na sobě nezávislých částí. Jde o poměrně kontroverzní zákon, neboť omezuje uživatele duševního vlastnictví. Vedle jiných nedostatků, jmenujme alespoň omezení uživatele vytvořit si kopii díla pro svou potřebu.

DCA z roku 1996 stanovil kromě jiného poměrně vágní definice obscénního a neslušného obsahu a stanovoval pravomoci státních orgánů v boji proti závadným stránkám. Přijetí zákona vyvolalo vlnu odporu nejen internetových uživatelů, ale i firem jako MS či AOL. Na základě soudního rozhodnutí byly rozporuplné pasáže zrušeny. [85]

- Americké orgány přijímají výklad **teritoriality práva** v souvislosti s internetem – podle některých soudních rozhodnutí je subjektem práva (i trestního stíhání) kdokoliv, kdo publikuje na internetu obsah, k němuž mohou mít přístup uživatelé – občané USA, což tedy v prostředí internetu není žádný problém.
- S vydáním zákona upravující digitální podpis bylo vydáno mnoho **úprav** vztahujících se ke **kyberprostoru**, např. *National Infrastructure Protection Act* z roku 1996, *Cyberspace Electronic Security Act* z roku 1999 či *Patriot Act* z roku 2001 aj.
- K odhalování EIK bylo založeno mnoho **center a agentur** jako *FBI, National Infrastructure Protection Center, National White Collar Crime Center, Internet Fraud Complaint Center, Computer Crime and Intellectual Property Section of DoJ*[72] (provozuje webové stránky www.cybercrime.gov, kde najdeme veškeré aktuální informace týkající kybernetického zločinu – aktuality, legislativa, proběhlé kauzy, tiskové zprávy, informace o kybernetice atd.), *Computer Hacking and Intellectual Property Unit of DoJ* atd.
- Na úrovni každého amerického státu je vytvořeno několik **speciálních center či jednotek policie** typu *Computer Crimes Unit, Hi-Tech Crime Unit/Squad, Computer Crimes Task Force* apod.
- Americká vláda investuje poměrně vysoké finanční prostředky do boje proti kybernetickému zločinu. FBI sestavila oddělení, které vyvinulo sledovací systém *Carnivore* umožňující monitorovat síťovou komunikaci.
- *Internet Crime Complaint Center – IC3* (http://www.ic3.gov) vzniklo ve spolupráci FBI a *National White Collar Crime Center*. IC3 vyřizuje stížnosti obětí kybernetického zločinu, postupuje je dále právním kancelářím (i na

72 Department of Justice – Ministerstvo spravedlnosti.

mezinárodní úrovni). Na svých stránkách zveřejňuje rady, jak se vyhnout internetovému zločinu (Internet crime prevention tips).

- Oblastí informační bezpečnosti se zabývají desítky institucí a je velmi detailně upravena stále zdokonalovanými zákony.
- *Cyber Security Industry Aliance (CSIA)* – sdružení, které zvýšilo povědomí o bezpečnosti v kyberprostrou, zálohování informací, analýzách hrozeb, výzkumu a rozvoji a vzdělávání v oblasti bezpečnosti.
- *FIPS PUB 199* je standardem pro kategorizaci bezpečnosti vládních informací a IS.
- *National Strategy to Secure Cyberspace*[73] je 60-ti stránkový dokument, který shrnuje strategické cíle zahrnující opatření proti kybernetickým útokům, snížení národní zranitelnosti a minimalizace škod způsobených kybernetickým zločinem. Zásadní priority tvoří rozvoj národního bezpečnostního systému v kyberprostoru (program snížení kybernetických hrozeb, školící program, bezpečnost kyberprostoru na všech úrovních atd.)
- Občané státu New Yorku musí být ze zákona informováni o každém bezpečnostním průniku, který se dotýká jejich dat. Obdobná pravidla přijala Kalifornie, ostatní americké státy zavedení zatím zvažují.[74]

Na americké kontinentu jsou nechvalně proslulé aktivity organizací *RIAA* a *MPAA*, které se týkají potírání hudebního a filmového pirátství. Přestože nahrávací a filmová studia nedokáží kvantifikovat počet nelegálních downloadů, dokáží vyčíslit odhadované škody. Jejich obranou jsou žaloby.

RIAA (Recording Industry Association of America) se snaží omezit nebo úplně zamezit stahování MP3 nahrávek z internetu, zejména prostřednictvím P2P sítí. RIAA využívá především žaloby na základě získaných IP adres (celkem již kolem 17 tisíc), které však nemají kýžený výsledek. Obžalovaným hrozí až pět let vězení a pokuta ve výši 250 000 dolarů. V březnu tohoto roku oznámilo Ministerstvo spravedlnosti USA, že byli u Federálního soudu odsouzeni tři členi warezové skupiny *„Apocalypse Crew"* za sdílení písní a alb v síti P2P. Hudbu získávali od interních zaměstnanců nahrávacích studií, recenzentů v časopisech či přímo od prodejců.[75]

Přestože jsou některé nařčené sítě zrušeny, uživatelé začnou používat jiné. Dokonce došlo k případu, kdy byla síť jeden den zrušena a hned den další se na internetu objevila záplata, díky které se P2P opět zprovoznila. V roce 2001 se RIAA snažila prosadit zákon, který by ji dovolil hackovat libovolný počítač na síti a vymazat z něj veškerý obsah.

Díky své „oblíbenosti" se stránky RIAA několikrát staly terčem útoků hackerů. Ti tak dali bezprostředně najevo svou nespokojenost s postupy RIAA proti P2P sítím,

73 HOAR, Sean B. Trends in cybercrime: the darkside of the internet. *Criminal justice*. 2005, vol. 20, no. 3, s. 4-13.

74 Zdroj: http://www.novinky.cz/internet/62724-new-york-informuje-obcany-o-bezpecnosti-jejich-dat.html.

75 Zdroj: http://www.warezblog.net/?p=1630.

pozměnili texty na serveru a vystavili zde nelegální kopie skladeb. Server *Boycott RIAA* (www.boycott-riaa.com) dává také velmi otevřeně najevo svůj nesouhlas s aktivitami RIAA.

MPAA (Motion Picture Association of America) je nejaktivnějším obráncem "práv" vydavatelů DVD a CD disků. MPAA zatím používá mírnější taktiku než RIAA. Prostřednictvím SW firmy *Ranger Online* odposlouchává, co kdo nabízí ke stažení. V případě, že SW najde soubor chráněný AP, zjistí pomocí IP adresy příslušného poskytovatele nelegálního obsahu a automaticky informuje MPAA. Ta odešle poskytovateli upozorňující dopis. V roce 2003 bylo odesláno 54 tisíc takových dopisů, v následujícím roce byl odeslán stejný počet během první poloviny roku. Pokud uživatel nelegální soubory do druhého dne neodstraní, bude mu zablokován jeho přístup k internetu.[76]

4.2.2 Kanada

Kanada je jednou ze zemí s nejvíce počítačově gramotným obyvatelstvem na světě. 25% kanadských domácností má přístup k internetu.

- *Criminal Law Amendment Act* z roku 2001, obsahuje dvě části (neoprávněný přístup k počítačovým systémům, narušení přenosu a poškození, nahrazení a zničení dat).
- *Canadian´s Police´s Information Technology Security Branch* – nejvýznamnější oddělení, které se věnuje boji proti kyberzločinu. Kanadská policie absolvuje speciální internetové školení.
- Nejvyšším dokumentem týkajícím se informační bezpečnosti je *Government Security Policy*, doplněná řadou prováděcích předpisů nazývaných *Operational Standards*. Velký důraz je kladen na zvyšování úrovně znalostí o informační bezpečnosti – program *Information Security: Raising Awareness.*
- Hlavním garantem informační bezpečnosti je *Treasury board of Canada* (Ministerstvo financí).
- Kanadský soud rozhodl, že sdílením a stahováním hudby z PSP nebyl porušen AutZ. Toto rozhodnutí značně pobouřilo nahrávací studia. Případ byl přirovnán ke kopírce v knihovně.[77]

4.2.3 Německo

Německo bylo prvním státem, který zvláštní normou upravil otázku odpovědnosti poskytovatelů volného prostoru – *Teledienstegesetz* (TDG) – přijetí tohoto zákona předcházela kauza společnosti *CompuServe Inc.*

76 Zdroj: http://zvedavec.org/pocitace_354.htm.

77 Zdroj: http://news.com.

- 63% firem vnímá kybernetický zločin jako větší hrozbu než je tradiční kriminalita, pouze 10% německých firem naopak vnímá jako větší hrozbu tradiční kriminalitu (průzkum IBM)[78].
- Německo patří k tradičním zemím, které kladou vysoký důraz na bezpečnost, té se věnuje již řadu let. Dokladem je dlouhodobě zdokonalovaný projekt *IT-Grundschutzhandbuch* (Příručka základní ochrany IT), závazný pro organizace veřejné správy a široce přijímaný jako metodické vodítko v komerčních organizacích.
- Německo má pro boj s EIK různé organizace – jedna se specializuje na organizovaný zločin jako takový, druhá na zločin spojený s ICT. *ZaRD*[79] byla založena v roce 1990 jako specializovaná agentura pro monitorování internetových aktivit, nikoli pro vyšetřování konkrétních případů. Převážná část případů se týká dětské pornografie. [87]
- *Deutsche Bank* oznámila, že začne všechny datové zprávy, které zasílá svým klientům, elektronicky podepisovat a tak zabrání phishingu. Průzkumem bylo totiž zjištěno, že 80% uživatelů online bankovních služeb nerozezná phishingový e-mail.[80]
- Celostátní policejní akce proti internetovým pirátům - dle řídícího státního zastupitelství bylo prohledáno bylo více než 200 bytů a firemních místností. Cílem akce, při níž byly v Německu odhaleny desítky pachatelů, většinou mladých lidí ve věku mezi 16 a 25 roky, bylo zakročit proti pirátskému stahování filmů, hudby, her i různých SW z internetu. Bylo zabaveno pět warez serverů s 6 terabajty ilegálních kopií filmů (cca 7000) a her. Kopie pak pachatelé obratem sami nabízejí za podstatně nižší ceny a vyhýbají se placení autorských poplatků. Podle informací se obdobné akce mají konat častěji a po celé Evropě. [81]
- Využívání internetu pro soukromé potřeby v práci může vést k okamžitému ukončení pracovního poměru. Situace však musí být posuzovány individuálně a náležitě prokázány.[82]
- V Německu může být trestně stíhán i ten, kdo se dopouští trestného činu (podle německého práva) na zahraničních webových stránkách, které jsou přístupné internetovým uživatelům v Německu.[83]

4.2.4 Velká Británie

Ve Spojeném Království stačí k ochraně autorského díla, pouhé vytvoření díla a jeho označení značkou copyrightu. *Copyright Act* z roku 1988 stanovuje ochranu počítačového programu, dokonce zde probíhaly úvahy o ochraně SW jako fotografického nebo filmového díla. Ochrana copyrightem byla počítačovému programu přiznána v roce 1985 dodatkem *Copyright (Computer Software Amendment) Act.*

78 Pro společnost IBM provedla výzkum agentura Braun Research Inc. Výzkumu se zúčastnilo celkem 3002 respondentů, dostupné z http://notebook.cz/ /,clanky,tiskova-zprava,2006,060321-cyber-crime,index.html.

79 Zentrale anlassunabhängige Recherche in Datennetzen.

80 Zdroj: http://www.micr.cz/scripts/detail.php?id=3339.

81 Zdroj: http://www.mpx.cz/ZAJIMAVOSTI/Nemecko-zazilo-velkou-razii-proti-stahovacum-z-internetu.html.

82 Zdroj: http//www.itpravo.cz/index.shtml?x=315830.

83 Zdroj: http//www.itpravo.cz/index.shtml?x=61318.

Kybernetické trestné činy byly upraveny v *Data Protection Act* z roku 1984 a *Computer Misuse Act z roku* 1990, dodatečně byl vydán zákon *Regulation of Investigatory Powers* (RIP) z roku 2000.

V roce 2002 bylo napadeno internetovými piráty téměř 90% britských podniků, které se však báli incidenty hlásit, aby tak nepřišli o dobrou pověst. Proto vyzvala počítačová policie tamější firmy ke spolupráci. V rámci této kampaně byla garantována naprostá anonymita. Ze studie firmy *PriceWaterhouseCoopers* vyplynulo, že britské podniky se spíše soustřeďují na zakrytí následků kybernetických útoků než na jejich prevenci.

- *Directive on Privacy and Telecommunications*[84] z roku 2002 upravuje spamovou problematiku (EU antispamový zákon).
- Založení oddělení *National Criminal Inteligence Service* (NCIS), které se věnuje dešifrování kriminálních materiálů, dále *National Crime Squad.*
- *National Hi-Tech Crime Unit (NHTCU)* byla založena roku 2001 a je jednou z nejefektivnější organizací svého druhu v Evropě. Zaměřuje se převážně na hackery a tvůrce virů, vydírání v důsledku nabourání do systému, doménový spoofing, DDoS a obchod s drogami po internetu. [87]
- *NHTCU* iniciovala *Crime reduction strategy*, podle odhadů[85] stála elektronická kriminalita britské firmy v roce 2004 přibližně 2,45 miliardy liber. NHTCU oslovila v průzkumu 200 firem, z nichž 178 přiznalo, že se v minulém roce setkalo s tímto druhem zločinu. 76% firem vnímá kybernetický zločin jako větší hrozbu než je tradiční kriminalita (dle průzkumu IBM). Virové útoky postihly téměř 100% všech oslovených firem a způsobily tak škodu ve výši 70 milionů liber. NHTCU podotkla, že řadu útoků mají na svědomí vlastní zaměstnanci (zničení nebo zneužití dat).
- Kampaň *Get Safe Online* ke zvýšení povědomí o EIK, zejména elektronického obchodu.
- Velká Británie je z evropských zemí pravděpodobně nejdále v implementaci informační bezpečnosti – má vypracován systém technických i organizačních opatření v podobě *High-level Information Assurance GESG Policy.*

4.2.5 Austrálie

- Tzv. *„Privacy Acts"* jsou zákony chránící data, které upravují sběr, užití a prozrazení osobních citlivých údajů, neupravují soukromí jednotlivce v širším smyslu. V souvislosti s používáním internetu a dalších ICT, jsou provideři povinni dodržovat telekomunikační zákony, tzv. *Telecommuniactions Acts* z roku 1997.
- *Australian Cybercrime Act* z roku 2001 definuje neoprávněný přístup k počítači, modifikaci dat atd.
- *Australia´s Internet Industry Association* vydala *Cybercrime Code,* který upravuje uchovávání dat ISP.

84 Zdroj: http://digiweb.ihned.cz/3-11995160-po%E8%EDta%E8ov%E1+kriminalita-i00000_d-ba.

85 Zdroj: http://digiweb.ihned.cz/?s1=i&s2=9&s3=0&s4=0&s5=0&s6=0&m=d&a[areaid]=10053230&a[id]=15917960&p=i90000_d.

- *Australian National Police Research Unit* schválila program *Computer Investigation Techniques*, jehož cílem je vyvíjet vyšetřovací nástroje, distribuovat informace a školit policejní vyšetřovatele.
- *Electronic Frontiers Australia Inc. (EFA)* je nevýdělečnou národní organizací, která reprezentuje on-line svobodu a práva internetových uživatelů. EFA byla založena roku 1994, přidružena pod *Associations Incorporation Act.*
- Federální soud zakázal do února 2006 svým obyvatelům používat *Kazaa Media Desktop*, do té doby musela společnost *Sharman Network* implementovat do svého klienta Kazaa filtr blokující klíčová slova a tím zabránit stahování souborů, které jsou chráněny autorským zákonem.
- *The Australian Communications and Media Authority (ACMA)* registrovala světově první **antispamový zákon**, který ukládá providerům povinnost provozovat spamový filtr a systém řešící uživatelské stížnosti.
- AusCERT – *Australian Computer Emergency Response Team* pořádá každoročně **konferenci** *AusCERT Asia Pacific Information Technology Security Conference*, zaměřenou na informační bezpečnost (letos se koná 21.5. – Gold Coast).

4.2.6 Taiwan

Taiwan je zemí, kde disponuje téměř 40% domácností připojením k internetu, což je v celosvětovém kontextu poměrně vysoká míra. Expanze přístupu k internetu pochopitelně vyvolává nárůst kybernetického zločinu.

- Taiwanská vláda v roce 2003 doplnila deset článků *Criminal Law* z roku 1997 o opatření, aby se vypořádala s kybernetickým zločinem.
- V listopadu 2003 proběhl třídenní seminář policejních úředníků a státních zástupců z celého Taiwanu. Akci sponzorovalo Ministerstvo spravedlnosti a cílem bylo sdílení informací a strategií v boji s kybernetickým zločinem.
- Pro vynucení práva byly založeny instituce: *Cybercrime Prevention and Fighting Center of the Investigation Bureau, Telecommunication Police Squad* a *Computer Crime Squad of the Criminal Investigation Bureau.*
- *Criminal Investigation Bureau* vyvinula vlastní softwarové nástroje a hardwarové vybavení pro výzkum případů týkající se kybernetického zločinu (např. *Internet Patrol Agent, Globe IP Tracer, Evidence Collector, Packet Analyzer* a *Remote Monitor*). [17]

4.3 Mezinárodní spolupráce

Jak již bylo mnohokrát zmíněno, internet je globálním médiem, bez hranic. **Kybernetický zločin** ovlivňuje jednotlivce, korporace, ekonomiky i národní bezpečnost všech zemí díky rozšířenosti internetu. Ten předpokládá mezinárodní spolupráci, harmonizaci právních předpisů a vývoj bezpečnostních nástrojů. Spolupráce již mj. probíhá např. mezi výrobci bezpečnostního SW, kteří sdílejí informace o virových nákazách a spywaru, z důvodu jednotného boje proti tomuto

malwaru. Nutnost **úzké spolupráce** uznávají i zástupci soukromého a veřejného sektoru - ta je charakterizována otevřeností a intenzivní oboustrannou komunikací. V následujících odstavcích jsou zmíněny různá seskupení a webové portály věnující se EIK. Dále jsou zde obsaženy informace o letošních vybraných významných konferencích a organizacích, které se věnují potírání EIK. Pochopitelně podobných akcí a subjektů existuje mnohem více, zejména na národních úrovních.

V globálním měřítku je zde třeba zmínit akci **FBI** *„Site Down"*. FBI spolupracovala s policí z následujících zemí: Austrálie, Belgie, Dánsko, Kanada, Francie, Německo, Izrael, Nizozemí, Portugalsko a Velká Británie. Bylo prověřeno více než 90 podezřelých aktivit, z toho bylo 20 mimo USA. Hlavním cílem operace však bylo zatčení 22 warez skupin, které se starají o distribuci filmů, cracknutých verzí programů, her apod. Výsledkem akce jsou čtyři zatčení a osm zrušených nelegálních aktivit.

ICC - International Chamber of Commerce (Mezinárodní obchodní komora) je jedinou celosvětovou obchodní organizací, která reprezentuje podniky všech sektorů ze všech koutů světa. Jedna z komisí se věnuje **e-byznysu a ICT** a jejím posláním je pomáhat při tvorbě podnikatelských podmínek v této oblasti. Kromě jiných, je zde vytvořena **speciální jednotka** pro potírání kybernetické kriminality (zejména internetové podvody). Cílem jednotky je provádět šetření ohledně identifikace původu podvodných internetových stránek a nebezpečných e-mailů a zvyšovat povědomí o rozsahu EIK.

Computer Emergency Response Team Coordination Center (CERT/CC) je nevládním sdružení kvalifikovaných odborníků informujících ostatní profesionály o bezpečnostních problémech a reagujících na probíhající útoky. Jde o počítačové týmy nouzové reakce, mezi jejich hlavní funkce patří [136]:

- poskytování komplexního přehledu o metodách útoku, slabých místech a účincích útoku na IS a sítě a také trendech,
- budování infrastrukturu stále kvalifikovanějších bezpečnostních pracovníků,
- poskytování metod pro hodnocení, zlepšování a udržování bezpečnosti a funkční schopnosti propojených systémů,
- spolupráce s komerčním sektorem na zvyšování bezpečnosti dodávaných výrobků.

Internet Governance Forum[86] ***(IGF)*** – platforma pro diskusi zabývající se širokým spektrem otázek (spam, ochrana osobních údajů, internetová kriminalita apod.). Cílem IGF je zejména zvýšit vzájemné porozumění a spolupráci institucí zabývajících se prosazováním práva, poskytovatelů počítačových služeb, síťových operátorů,

86 Zdroj: http://cybercrime-forum.jrc.it/default.

spotřebitelských organizací, orgánů zabývajících se ochranou dat, občanských organizací a dalších zainteresovaných stran. Dále zvýšit uvědomění si rizik vyvolaných působením počítačových pirátů, identifikovat efektivní prostředky a způsoby boje proti počítačové kriminalitě a další vývoj mechanismů včasného varování a krizového řízení. Jsou zde zastoupeny vlády jednotlivých zemí, subjekty občanské společnosti, ISP a dalších organizací. První setkání proběhne v Aténách na konci října tohoto roku (www.igfgreece2006.gr).

Computer Crime Research Center – CCRC (www.crime-research.org) je nevýdělečnou, nevládní a vědecko-výzkumnou organizací, ve které se angažují dobrovolníci z řady zemí. Centrum bylo založeno roku 2001 s cílem zkoumat a varovat před nelegálními činy týkající se ICT. Shromažďují zkušenosti a provádí různé analýzy, poskytují školení. Centrum pořádá semináře, konference a mezinárodní sympózia týkající se kyberzločinu a kyberterorismu. Výsledkem jejich činnosti jsou publikované články a knihy.

International Association for Computer Information Systems - IACIS (www.iacis.org) je mezinárodní společností tvořenou profesionály z oblasti práva, kteří se věnují vzdělání v oblasti forenzní počítačové vědy. Společnost byla založena roku 1960, je zaměřená na zdokonalování IS. Společnost pořádá každý rok mezinárodní konferenci, vydává *Journal of Computer Information Systems* a *Issues in Information Systems*.

Webový portál ***Cyber Criminals most Wanted*** (www.ccmwanted. com) poskytuje světový přehled legislativy vztahující se k EIK. Dále zde nalezneme aktuální zpravodajství, možnost vyhledávání podle mnoha oblastí (např. internetová bezpečnost, právo, uživatelé, měsíční zpravodaje atd.). Umožňuje podávání stížností prostřednictvím *Internet Crime Computer Center*.

The e-Crime Congress 2006 (www.e-crimecongress.org)

Toto setkání již probíhá po několikáté (letos na konci března). Kongres je zaměřen na spolupráci podnikatelských, vládních a právních aktivit v boji proti hrozbám elektronického zločinu, které snižují veřejnou důvěryhodnost v internet jako komerčního média.

DoD Cyber Crime Conference 2006 (www.technologyforums.com)

Zaměření konference pokrývá všechny aspekty počítačového zločinu, od vyšetřování průniků, kybernetického práva, důvěryhodnosti informací až po testování a hodnocení soudních digitálních nástrojů.

Infosecurity Europe 2006 (www.infosec.co.uk)

Tato konference zabývající se informační bezpečnosti je významnou evropskou událostí. Letos probíhá již 11. ročník (Londýn, duben). Jsou zde představovány vzdělávací programy, nové produkty a služby.

4.3.1 OSN

Valné shromáždění OSN podporuje mezinárodní snahy v oblasti pomoci členským státům při řešení počítačové kriminality již řadu let. V akčních plánech implementace *Vídeňské deklarace o kriminalitě a justici: Odpověď na výzvy 21. století*, je jedna sekce nazvána *„Postup proti kriminalitě využívající moderní technologie a proti počítačové kriminalitě"*. [136]

- Již od roku 1990 se aktivně zapojuje do řešení různých aspektů vývoje v oblasti počítačů. V roce 1994 byla vydána *Příručka OSN pro prevenci a kontrolu počítačové kriminality*. V roce 2000 se v rámci 10. kongresu konal workshop o trestné činnosti související s počítačovými sítěmi.
- V *Deklaraci principů*, přijaté Světovým summitem o informační společnosti, je obsažena společná vize informační společnosti. Jedním z pilířů OSN pro 21. století je uznání **digitální propasti**.
- Výsledkem první fáze **Světového summitu** o informační společnosti bylo zřízení *Pracovní skupiny pro správu internetu* (*Working Group on Internet Governance*), která má za úkol zkoumat spamy, počítačovou bezpečnost a další otázky související s internetem.
- Každoročně pořádá **kongres** zaměřený na prevenci kriminality a trestní justici.
- *Úmluva OSN o nadnárodním organizovaném zločinu*, která je rozsahem globální, ovšem počítačové kriminality se týká jen nepřímo, a to tehdy, když je páchána skupinami organizovaného zločinu.

4.3.2 Skupina G8

Tvořena hlavami osmi vyspělých států: USA, Velká Británie, Rusko, Francie, Itálie, Japonsko, Německo a Kanada.

- V roce 1997 G8 iniciovala **akční plán** a principy k potlačení kybernetického zločinu (10 bodů), které shrnují cíle zúčastněných států v boji s „high-tech" zločinem.
- Založení *Podskupiny pro kriminalitu spojenou s vyspělou technologií,* která již od roku 1997 začala připravovat „24 hodinové kontakty" pro mezinárodní kriminalitu spojenou s vyspělou technologií a počítačovou kriminalitou. Kontaktní síť, která v současnosti zahrnuje 40 zemí, je nedílnou součástí Úmluvy Rady Evropy o počítačové kriminalitě. [136]
- Mezi **základní postuláty** patří: koordinace veškerých aktivit na mezinárodní úrovni, vyškolení a vybavení orgánů prosazující zákonnost, právní systémy musí chránit důvěrnost, integritu a přístupnost dat, vývoj forenzních standardů pro vyhledávání a ověřování elektronických dat, zřízení kontaktních center dostupných 24/7 atd. [31]

- Zásada - nesmí existovat bezpečné útočiště pro ty, kteří zneužívají IT.
- Rozvoj řady podmínek pro zlepšení schopností identifikovat zločince v ICT (uchování a ochrana dat, ISP, uživatelská autentizace).

4.3.3 Evropská Unie

EU iniciuje programy *eEurope,* jedním z cílů Akčního plánu z roku 2005 je vytvoření tzv. *Cyber Security Task Force*. Mezi další významné akční programy a plány patří *Safer Internet* či *User-friendly information society*. Nicméně **Rada Evropy** projevuje zájem o řešení problematiky EIK již od konce 80. let. V roce 1989 publikovala studii o počítačové kriminalitě, jejímž výsledkem bylo doporučení pro úpravy a vytváření nových zákonů. Další studie (1995), která obsahovala principy týkající se trestněprávního postupu souvisejícího s IT. V roce 1997 vznikla Komise expertů pro zločin v kyberprostoru (*Commitee of Experts on Crime in Cyber-Space*) pro práci na návrhu mezinárodní dohody, která by usnadnila mezinárodní spolupráci při zjišťování a pronásledování počítačových zločinů. Výsledkem je **Úmluva Rady Evropy o počítačové kriminalitě** *(Convention on cybercrime)* z roku 2001 – první mezinárodní úmluva týkající se internetové kriminality. Kromě členských států Rady Evropy ji podepsaly USA, Kanada, Japonsko a JAR. Jejím obsahem je především porušování AP, počítačové podvody, dětská pornografie a hacking. Úmluva zavazuje smluvní státy, aby harmonizovaly vnitrostátní trestní právo hmotné, upravující trestné činy (proti důvěrnosti, integritě a dostupnosti počítačových údajů a systémů, jakož i trestné činy související s užíváním počítače, porušením AP a dětskou pornografií). Tzv. „zločiny z nenávisti" páchané online vyvolaly přijetí dodatkové protokolu k Úmluvě, který zavazuje kriminalizovat činy **rasistické či xenofobií povahy** (2003). Mezi hlavní cíle patří inovace trestně právní politiky a posilování mezinárodní spolupráce. Další úprava je dána:

- *Směrnicí 95/46/ES*, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů.
- *Směrnicí 2000/31/ES,* o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu. Směrnice, jejíž snahou je harmonizovat legislativu jednotlivých členských zemí EU, se věnuje elektronickému obchodu a kromě jiného upravuje odpovědnost poskytovatelů volného prostoru.
- *Směrnicí 2002/58/ES,* o zpracování osobních údajů a ochrany soukromí v elektronických komunikací.
- *Direktivou o vynutitelnosti práva na intelektuální vlastnictví (Enforcement Directive)* z roku 2004. Jejím cílem je poskytnout státům EU nástroje a směrnice, které mohou použít pro ochranu a podporu odvětví, jejichž prosperita úzce souvisí s dodržováním autorského práva. Termín implementace je stanoven na duben 2006. Očekává se, že členské státy přehodnotí své systémy ochrany AP, neboť softwarové pirátství snižuje daňové výnosy v jednotlivých zemích, omezuje počet pracovních příležitostí a oslabuje lokální softwarové trhy, aj.

Zajímavým počinem je **Eurozatykač** *(Evropský zatýkací rozkaz),* jehož účelem je zefektivnit a zejména urychlit stíhání pachatelů trestných činů spáchaných na území EU. Došlo k prolomení tzv. **zásady oboustranné trestnosti**[87] a **nevydávání vlastních občanů** k trestnímu stíhání do jiných států. Článek 2 odst. 2 zabývající se „computer-related crime", stanoví pouze určité typy jednání, ne kvalifikaci trestného činu a jeho podřazení pod určitou skutkovou podstatu (určuje stát vyžadující vydání pachatele). V případě, že by došlo k implementaci Eurozatykače do právních řádů členských zemí EU, bude na celém území EU uplatňována ta nejpřísnější trestněprávní úprava ze všech těchto států, bez ohledu na legislativu zemí s mírnější úpravou. Eurozatykač klade na všechny subjekty internetu požadavek - seznámit se se všemi relevantními legislativami a chovat se podle té nejpřísnější (bez ohledu na národní legislativu), aby se absolutně vyhnuli jakékoli možnosti trestního stíhání v některém z členských států. [84]

[87] Čin, za který je pachatel vydáván, musí být trestný jak ve státě vydání požadujícím, tak ve státě vydávajícím.

5 Elektronická informační kriminalita z pohledu informační společnosti

Informační společnost netřeba důkladně charakterizovat - již nejde v našem prostředí o pojem z oblasti „sci-fi", ale o živou realitu. Veškeré informační procesy jsou digitalizovány, dochází ke snížení prostorového a časového omezení a zvýšení přístupu k různorodým informacím. **Digitální informace** jsou univerzálně použitelné, duplikovatelné a transformovatelné, a tudíž i velmi lehce zneužitelné. Za tím vším stojí **ICT**, ty jsou jednak nezměrným přínosem pro lidskou společnost, ale v případě zneužití jsou zároveň velmi nebezpečnou zbraní. Jinými slovy technologický pokrok dává vzniknout pokroku kriminálnímu. Tempo technologického pokroku je nezadržitelné (Mooreův zákon)[88] a s ním i vynalézavost pachatelů EIK. Zvyšuje se (do jisté míry) počítačová gramotnost uživatelů a přístup k internetu má díky nízkým cenovým nabídkám téměř každý. Všechny tyto aspekty prohlubují možnosti zneužití ICT. V souvislosti s rozšiřováním ICT do celého světa, je nutné zmínit jejich nevyvážené pokrytí a vznik tzv. **digitální propasti** (digital divide). Rozvojové země s minimální technologickou úrovní se pak mohou stát výhodnou základnou nebo přestupní stanicí kybernetických útoků. V takovýchto zemích se předpokládá nízká, popř. nulová úroveň legislativy, což je pochopitelně pro útočníky neodolatelným lákadlem.

V čem však spočívá „oblíbenost" EIK? Vždyť zájem o informace, přestože byly zpracovány, přenášeny a uchovávány klasickým způsobem, trápí společnost odnepaměti. Příčinou valné většiny problémů je samotný **internet**. Je distribučním kanálem malwaru či ilegálního obsahu, zdrojem různorodých pomůcek a v neposlední řadě nástrojem k páchání útoků. Můžeme říci, že internet je přesně takový, jací jsou lidé, kteří ho užívají. Zločiny v kyberprostoru jsou geograficky neomezeny. Pachatelům stačí pouze počítač a připojení k internetu, aby mohli napadat data a informace jednotlivců, obchodních společností či vládních institucí na celém světě, aniž by museli opustit pokoj svého domova. Následující výčet faktorů, které naznačuje SMEJKAL [121] podává další snadné vysvětlení:

- **Složitost ICT** - většině uživatelů ICT je jejich podstata a provoz (tedy i možnosti zneužití) neznámá, často tak může být zneužívána **důvěra uživatelů**.

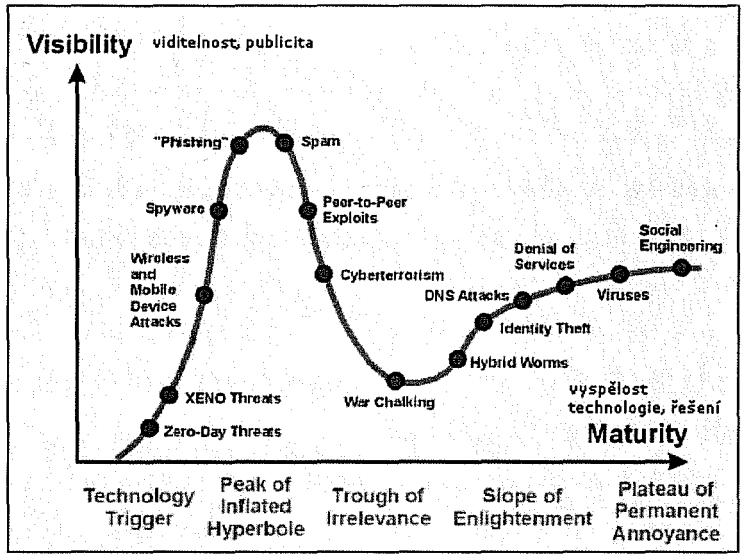
88 Mooreův zákon (1965, Gordon Moore – Intel) stanoví, že každých 18 měsíců dojde k zdvojnásobení výkonu mikroprocesoru za stejnou cenu nebo ekvivalentně pokles ceny na polovinu při nezměněném výkonu. K podobnému efektu dochází u kapacity komunikačních spojů, která se rovněž zvyšuje exponenciálně s poločasem zhruba 8 měsíců. Intel dodává, že zákon vydrží nejvýše do roku 2021 (zdroj: www.zive.cz).

- **Enormní objem** vysoce ceněných **informací**, které kolují internetem (citlivé osobní údaje, ekonomické údaje apod.). Získání databáze dostupné na internetu je nesrovnatelné např. s vloupáním do instituce a odcizení klasické kartotéky.
- Spáchání trestného činu **na dálku** - od „stolu" a jednoduché **zahlazování či skrývání důkazů**.
- **Anonymita pachatelů –** stav, kdy není možné identifikovat subjekt. Je jasné, že anonymní „komunikace" umožňuje pachateli provádět zcela kuriózní kousky, za které „nenese" odpovědnost.
- **Nedokonalost legislativy** – právní normy upravující oblast ICT jsou mnohdy obtížně vyložitelné a nepostihují všechny jevy. Vzhledem k dynamickému vývoji ICT není ani v jejich možnostech tuto oblast aktuálně pokrýt.
- Dostupnost **kryptografických technologií**, které mohou být - stejně jako kterýkoliv jiný nástroj – zneužity.
- **Nízké právní vědomí** populace, je v oblasti ICT nižší než v ostatních oblastech. A to díky již zmíněné složitosti těchto právních předpisů.
- **Cenová dostupnost** HW, SW a připojení k internetu a naopak **cenová nedostupnost** některých originálních produktů, resp. neadekvátní cenová politika prosazovaná některými firmami.

K porušování AP v oblasti elektronických informací bychom mohli ještě dodat, že někdy jsou na vině sami **vydavatelé a distributoři** hudby, filmů či SW. Využívají marketingové strategické triky v podobě vyvolání „umělého nedostatku". Produkty jsou pak uvolňovány na trh postupně - v malém množství, např. v týdenních intervalech, s nadějí, že se tak zvýší prodej. To však s pomocí ICT vede k zcela jinému efektu. V této souvislosti je třeba zmínit i fakt, že filmy jsou do kin naší republiky distribuovány až s tříměsíčním zpožděním a tak filmoví fanoušci mnohdy sáhnou po filmové verzi šířené v prostředí P2P. Dalším problémem může být např. u her – vyžadování online registrace produktu. V případě, že by uživatel neměl přístup k internetu, sáhne opět raději po nelegální, cracknuté verzi, která navíc nevyžaduje přítomnost instalačního CD v mechanice počítače. Podobné je to i s hudebními produkty, kdy se firmy všemožně snaží zabránit nelegálnímu šíření prostřednictvím ochran proti kopírování. První pokusy spočívaly v záměrném poškozování hlavičky CD, aby CD nebylo možno přehrát v počítači. CD však občas nešla přehrát ani v běžných CD a autopřehrávačích. Dále přišlo na řadu poškozování opravných CRC kódů na CD, tato ochrana sice funguje efektivně, ale při poškrábání média přehrávači opravné kódy chybí. Z uvedených příkladů vyplývá, že nejen cena produktu vede k jeho nelegálnímu šíření. Ilegálně získaný SW, hudba či film disponuje mnohem lepší distribucí a mnohdy kvalitou předčí originál, co se uživatelova požitku týče. Všechny tyto aspekty by se měly v boji proti pirátství zvážit.

Rozhodně by se neměla upírat vážnost deliktům vztahujícím se k porušování AP (každý autor má právo na svou odměnu), ale vzhledem k naznačeným problémům je možné dojít k závěru, že kriminalizace některých „banálních" provinění domácího uživatele je poněkud nesmyslná. Postihy by se měly zaměřit nejprve na komerční porušování AP a zejména na útoky na data, které jsou považovány za mnohem závažnější informační hrozby v kyberprostoru.

Zajímavý pohled na EIK provedla analytická firma *Gartner*, která jednotlivé hrozby znázornila podle jejich **životního cyklu**, neboť každý jev EIK prochází určitým vývojem. Znázornění míry výskytu dané hrozby, jakési její popularity na časové ose, nejlépe vystihuje tzv. *HypeCycle* diagram. Na následujícím obrázku č. 10 můžeme sledovat stav z konce roku 2004. Svislá osa diagramu (visibility) vyjadřuje míru výskytu hrozby a horizontální osa (maturity) vyspělost hrozby – to znamená, že nejnovější hrozby se nachází v levé části horizontální osy, ustálené hrozby v části pravé. Životní cyklus hrozby rozeznává pět vývojových oblastí – některé jevy nemusí projít všemi etapami. Může se stát, že se některé hrozby díky vhodným opatřením či překonání technologie vytratí. [102]



obr. č. 10 – Kybernetické hrozby z konce roku 2004, převzato z [116]

V první oblasti, tzv. technologických spouštěčů se - jak již název napovídá - vyskytují hrozby, které se objevují s novými technologiemi. Obecně můžeme říci, že jde o novinky na trhu nebo ve sledované oblasti.[89] **Druhou oblastí** je tzv. vrchol zvýšeného zájmu, vrchol očekávání. Sem patří hrozby, o kterých se nejvíce hovoří a

89 Zahrnujeme sem tzv. „zero-day" útoky, které jsou zaměřeny na chyby výrobců SW a HW, dříve než stačí distribuovat opravné nástroje. Dále tzv. XENO (eXtended Enterprise Network Overseas), které se objevují v souvislosti s outsourcingem v oblasti IT. Poslední hrozbou v této oblasti jsou útoky na mobilní zařízení a bezdrátové produkty.

6 Závěr

ICT způsobily v našem pracovním i osobním životě velké změny. Vedle usnadnění a zkvalitnění různorodých činností dochází zároveň ke zneužívání technologií, zejména internetu. Ten přináší problémy v rovině technologické, etické i legislativní a čím dál častěji se stává nástrojem informační kriminality v kybernetickém prostoru.

Nejzávažnější problémy tvoří **ztráty důvěrných informací** - které mohou být následně využívány pro další ilegální činnosti, **masové porušování AP** v prostředí internetu - kde vládne naprostá anarchie a v neposlední řadě i **oblast internetových podvodů a obtěžování**. Důsledkem jmenovaných jevů může být jak ohrožení obchodních aktivit a ztráta soukromí, tak ztracení důvěry uživatelů v ICT. Proto je nezbytné, aby jednotliví uživatelé a společnosti věděli, jakým způsobem může EIK ohrozit jejich informace a data a jakým následkům se v případě nedostatečné připravenosti či ignorace takových jevů vystavují.

Opatření proti EIK by měla být především **preventivního charakteru**. Mělo by být rozšiřováno obecné povědomí o možných hrozbách a následcích EIK. Pro řešení problému EIK je nezbytný **komplexní přístup** – od zajištění bezpečného internetového obchodování, soukromí jednotlivce, zvyšování povědomí o IB až po zahrnutí výuky do studijních plánů policistů, soudců atd. Ale aby se změnilo smýšlení uživatelů o beztrestném kopírování či jiných deliktech, je zapotřebí **spolupráce** institucí soukromého, veřejného i mezinárodního charakteru. Další výzvou je **aktualizace právních předpisů**, které by měly držet krok s dynamickým vývojem ICT a postihovat tak charakter trestných činů v kyberprostoru. V zásadě by měla být dodržována myšlenka *„act locally, think globally"*.

Vyhlídky na vymýcení EIK z našeho života jsou poměrně nerealistické, alespoň ne v dohledné době. V každé společnosti, i té informační, se vždy najdou jedinci, kteří budou obcházet daná etická i legislativně zakotvená pravidla a zneužívat důvěry občanů. Při pomyšlení, že dojde k integraci všech technologií a „virtualizaci" digitálního prostředí do podoby elektronického domova či kanceláře, můžeme jen čekat, jaké přínosy či nové hrozby tato vize přinese...

Seznam použité literatury

[1] AMBROŽ, Jan. *Jak silná je naše "softwarová policie"?* [online]. 24.5.2005 [cit. 2005-11-19]. Dostupný z WWW: <http://www.lupa.cz/clanky/jak-silna-je-nase-softwarova-policie>.

[2] AMBROŽ, Jan. *Vězení za diskusi na webu* [online]. 29.3.2005 [cit. 2005-11-19]. Dostupný z WWW: <http://www.lupa.cz/clanky/vezeni-za-diskusi-na-webu>.

[3] AMSTRONG, H. L.; FORDE, P. J. Internet anonymity practises in computer crime. *Information Management & Computer Security*. 2003, vol. 11, no. 5, s. 209-215.

[4] Anti-Phishing Working Group. *Phishing Activity Trends* [online]. 8/2005 [cit. 2006-01-19]. Dostupný z WWW: <http://www.ustreas.gov/offices/domestic-finance/financial-institution/cip/ pdf/apwg_phishing_activity_report_august_05.pdf>.

[5] BAREŠ, Michal; BEHRENSE, Daniel. Internetové podvody : jak se bránit nejrůznějším podlým trikům na internetu. *PC World*. 2005, č. 11, s. 66-72.

[6] BEDNÁŘ, Vojtěch. Data proti vykradení odolná: je se čeho bát? *PC World*. 2003, č. 3, s. 30-33.

[7] BEDNÁŘ, Vojtěch. Jak dlouho budeme sdílet?: budoucnost jedné zajímavé techniky. *PC World*. 2003, č. 2, s. 42-43.

[8] BEDNÁŘ, Vojtěch. Má výměna P2P naději? : možné alternativy vývoje. *PC World*. 2003, č. 7-8, s. 90-93.

[9] BERNÁTOVÁ, Anička. *Hackeři a ti druzí – kdo jsou a co dělají* [online]. 24. 08. 2004 [cit. 2004-12-16]. Dostupný z WWW: <http://www.zive.cz/h/Uzivatel/AR.asp?AR=118060>.

[10] BIGAS, Jiří. *Konec pirátství v Česku* [online]. 28.8.2001 [cit. 2006-02-10]. Dostupný z WWW: <http://www.gameplanet.cz/index1.php?sel_id=129>.

[11] BÍMOVÁ, Alena. *Počítačová kriminalita a naše doba*. Praha : IDG Czechoslowakia, 2004. 137 s. ISBN 80-900872-2.

[12] BROŽ, Vladimír. Organizovaná počítačová kriminalita. *PC World Security*. 2005, č. 1, s. 6-7.

[13] BRYANT, John. *Information Crime* [online][cit. 2004-12-16]. Dostupný z WWW: <http://www.thebirdman.org/Index/Intro/Intro-InfoCrime.html>.

[14] BSA. *První výroční studie BSA-IDC o softwarovém pirátství ve světě : globální trendy v oblasti softwarového piráctví pirátství* [online] [cit. 2005-12-10]. Dostupný z WWW: <http://www.bsa.cz/downloads/2003/2003idcstudie.pdf>.

[15] BSA. *Software piracy and the law : software piracy in the United States* [online] [cit. 2005-12-10]. Dostupný z WWW: <http://www.bsa.cz/downloads/2003/2003idcstudie.pdf>.

[16] *Bude podle navrhované novely trestního zákona věda (kryptoanalýza) trestná?* [online]. 11.10.2005 [cit. 2005-11-20]. Dostupný z WWW: <www.itpravo.cz/index.shtml?x=694071>.

[17] CHANG, Weiping et al. An International Perspective on Fighting Cybercrime. *LNCS*. 2003, no. 2665, s. 379-384.

[18] ČEPIČKA, David [et al.]. *Co všechno o nás ví Microsoft?* [online]. 3.10.2005 [cit. 2006-02-10]. Dostupný z WWW: <http://www.pcworldsecurity.cz/pcws.nsf/bezpecnost/26BD4B2686235E96C125708F0033D4D6>.

[19] ČEPIČKA, David [et al.]. Exkluzivní zpráva o hackerech : způsob práce hackerů a triky, jak se nabourávají do cizích serverů. *PC World*. 2005, č. 4, s. 49-52.

[20] ČEPIČKA, David; BRANDT, Andrew. Odhalujeme nebezpečné programy : identifikujeme malware skrytý v systémových složkých Windows. *PC World*. 2005, č. 9, s. 74-77.

[21] ČEPIČKA, David; BEHRENSE, Daniel. Prolomte každé heslo! : sada rad a doporučení pro případy, kdy zapomenete heslo. *PC World*. 2005, č. 10, s. 30-36.

[22] ČEPIČKA, David; BÜTIKOFER, Christian. Spyware a hijackery : ochraňte svůj počítač a soukromí před útoky z internetu! *PC World*. 2004, č. 10, s. 58-63.

[23] ČEPIČKA, David; WEIDEMANN, Tobias. Zapomněli jste heslo? *PC World*. 2003, č. 2, s. 44-48.

[24] ČERMÁK, Jiří. *Licence a licenční smlouvy k software* [online]. 24.6.2003 [cit. 2005-10-12]. Dostupný z WWW: <www.itpravo.cz/index.shtml?x=138962>.

[25] ČERMÁK, Jiří. *Právní aspekty odkazů (hyperlinků) : část I : úvod* [online]. 25.2.2002 [cit. 2005-10-12]. Dostupný z WWW:<www.itpravo.cz/index.shtml?x=71655>.

[26] ČERMÁK, Jiří. Právní *aspekty odkazů (hyperlinků) : část II : odpovědnost za odkazovaný cizí obsah* [online]. 5.6.2002 [cit. 2005-10-12]. Dostupný z WWW:<www.itpravo.cz/index.shtml?x=9288>.

[27] ČERMÁK, Jiří. *Vztah principu teritoriality a polohy serveru při určení rozhodného autorského práva na Internetu* [online]. 19.11.2001 [cit. 2005-11-19]. Dostupný z WWW: <http://www.itpravo.cz/index.shtml?x=47573>.

[28] *Česká protipirátská unie* [portál][cit. 2006-02-19]. Dostupný z WWW: <http://www.cpufilm.cz>.

[29] *České firmy a informační bezpečnost*[online]. 20.1.2006 [cit. 2006-02-25]. Dostupný z WWW: <http://www.isdn.cz/clanek.php?cid=7510>.

[30] Česko. *Autorský zákon* [online] [cit. 2005-09-07]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/autorsky>.

[31] Česko. Ministerstvo vnitra ČR. *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení* [online][cit. 2005-23-07]. Dostupný z WWW: <http://www.mvcr.cz/dokumenty/technologie/uvod.html>.

[32] Česko. *Trestní zákon* [online] [cit. 2005-09-07]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/trestn_zakon>.

[33] Česko. *Zákon o některých službách informační společnosti* [online] [cit. 2005-09-07]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/info_spol>.

[34] Česko. *Zákon o ochraně osobních údajů* [online] [cit. 2005-09-07]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/oou>.

[35] ČTK. *Sony BMG nebude vyrábět protipirátská CD* [online]. 13.11.2005 [cit. 2005-12-25]. Dostupný z WWW: <http://aktualne.centrum.cz/ekonomika/svetove-firmy/clanek.phtml?id=1819>.

[36] ČTK. *Softwarové pirátství stojí ČR miliardy* [online]. 8.12.2005 [cit. 2005-12-25]. Dostupný z WWW: <http://aktualne.centrum.cz/ekonomika/cesko-a-ekonomika/clanek.phtml?id=26042>.

[37] DASTYCH, Jiří. *Extremismus na Internetu* [online].11/2000 [cit. 2006-03-16]. Dostupný z WWW: <http://www.interdata.cz/sluknovsko_cz/sluknovsko/noviny/rn/rn2000/clanek.php3?kod1=262&cislo=11&typ=>.

[38] DASTYCH, Jiří. *Počítačová kriminalita* [online]. 26.4.1998 [cit. 2004-12-16]. Dostupný z WWW: <http://www.dolphin.cz/policie/brezen98/pocitace.html>.

[39] *Doménová jména versus ochranné známky* [online]. 5.12.2005 [cit. 2006-02-10]. Dostupný z WWW: <http://www.konjunktura.cz/index.php3?w=art&id=140&rub=96&s=>.

[40] DOUČEK, Petr. *Bezpečnost informačních systémů a mezinárodní standardy*[online]. 4.12.2000 [cit. 2006-02-07]. Dostupný z WWW: <http://si.vse.cz/archiv/clanky/2004/148.pdf>.

[41] *E-komerce a kriminalita : nové strategie zvládání rizika zákon* [online]. 4.12.2000 [cit. 2006-02-07]. Dostupný z WWW: <http://www.e-komerce.cz/ec/ec.nsf/0/225CBE9A1289A6DDC12569AB004901FA>.

[42] FAŤUN, Martin. Autorský zákon v. softwarové patenty. *Lidové noviny*. 11.3.2005, s. 11.

[43] FOLTZ, Bryan C. Cyberterrorism, computer crime and reality. *Information Management & Computer Security*. 2004, vol. 12, no. 2, s. 154-166.

[44] F.S.C. *Zavedení systému řízení informační bezpečnosti – ISMS*. [online]. xxxxx [cit. 2006-02-12]. Dostupný z WWW: <http://www.fsc-ov.cz/produkt.php?id=106>.

[45] FURNELL, Steven M.; DOWLAND, P. S.; SANDERS, P. W. Dissecting the "Hacker Manifesto". *Information Management & Computer Security*. 1999, vol. 7, no. 2, s. 69-75.

[46] FURNELL, Steven M.; WARREN, Mathew J. Computer abuse : vandalizing the information society. *Internet Research : Electronic Networking Applications and Policy*. 1997, vol. 7, no. 1, s. 61-66.

[47] GOLL, Jan. *Národní strategie informační bezpečnosti ČR*. [online]. 3.3.2005 [cit. 2006-01-12]. Dostupný z WWW: <http://www.micr.cz/files/2705/04_NSIB_CR_v0_8_3_.pdf>.

[48] HLAVÁČ, Jan. *Studie BSA a IDC poukazuje na ekonomické zisky, které Česká republika může získat ze snížení softwarového pirátství* [online]. 30.1.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://www.bsa.org/czechrepublic/press/newsreleases/8-12-2005.cfm>.

[49] HLAVÁČEK, Jan. *U policie nejsou jen blbci bez počítačů aneb pedofil z Internetu byl odhalen* [online]. 20.11.2005 [cit. 2006-02-10]. Dostupný z WWW: <http://archiv.neviditelnypes.zpravy.cz/krimi/0217krim.htm>.

[50] HLAVENKA, Jiří. *Phishing : když si hacker podá ruku se zločincem* [online]. 6.7.2004 [cit. 2004-12-16]. Dostupný z WWW <http://www.zive.cz/h/Uzivatel/AR.asp?ARI=117286>.

[51] HOLČÍK, Tomáš. *Ruský hacker zatčen po projevu na DefConu* [online]. 18.7.2001 [cit. 2006-02-10]. Dostupný z WWW: <http://www.zive.cz/h/Byznys/AR.asp?ARI=100916&CAI=2033>.

[52] IGNJATOVIČ, Martin. Jak myslí a pracují hackeři : studie skutečného případu zcizení dat. *PC World*. 2003, č. 7-8, s. 100-105.

[53] IGNJATOVIČ, Martin. Jak zabezpečit domácí počítač : zásady bezpečného připojení k internetu. *PC World*. 2003, č. 5, s. 78-79.

[54] IGNJATOVIČ, Martin. Nebezpečná síť : jak se útokům bránit. *PC World*. 2002, č. 10, s. 82-84.

[55] IGNJATOVIČ, Martin. Prolamování hesel populárně : nástroje pro práci s hesly a jejich odhalování. *PC World*. 2003, č. 7-8, s. 84-85.

[56] IGNJATOVIČ, Martin. Rádce uživatele internetu. *PC World*. 2002, č. 2, s. 86-89.

[57] IGNJATOVIČ, Martin. Zabarikádujte se! : firewally bez tajemství. *PC World*. 2003, č. 3, s. 62-65.

[58] IGNJATOVIČ, Martin. Ze života hackerů. *PC World*. 2002, č. 7-8, s. 88-95.

[59] *Invaze kyberšpionů* [online]. 20.11.2005 [cit. 2006-02-10]. Dostupný z WWW: <http://stoplusjedna.newtonit.cz/stare/200520/so20a26a.asp>.

[60] *Jak se z člověka stane „hacker"?* [online]. 1.6.2004 [cit. 2005-01-05]. Dostupný z WWW: <http://www.systemonline.cz/systemnews/websysnews_04-0526.htm>.

[61] *Ještě jednou k freeware - druhá strana barikády* [online]. [cit. 2006-02-07]. Dostupný z WWW: <http://www.pravnik.cz/art/article.php?id=161>.

[62] *K trestnému činu podvodu spáchanému prostřednictvím Internetu* [online]. 9.3.2004 [cit. 2005-10-12]. Dostupný z WWW: <http://www.itpravo.cz/index.shtml?x=147455>.

[63] *Když se nedostatek intelektu nazývá novinařinou* [online]. 20.1.2005 [cit. 2006-02-07]. Dostupný z WWW: <http://www.pooh.cz/cybercave/a.asp?a=2011487>.

[64] KOŠATA, Béda. *Hacker? : kdo to je*? [online]. 1.11.200 [cit. 2004-12-16]. Dostupný z WWW: <http://www.root.cz/clanek.php4?id=516>.

[65] KŘÍŽ, Lukáš. *X-vize budoucí bezpečnosti* [online]. 1.1.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://www.computerworld.cz/cw.nsf/ID/B7AE352FC15C49A9C12570E9006B5837?OpenDocument&cast=1>.

[66] KROTIL, Jiří. *Odpovědnost za nelegální software bezpečnosti* [online]. 15.1.2004 [cit. 2006-02-10]. Dostupný z WWW: <http://www.reseni.com/default.php?uid=&rub=14&prub=23&akce=zclanek&nocache=1134885516>.

[67] KUČERA, Jan. *Vývoj a nároky na bezpečnost v IT* [online].[cit. 2005-01-05]. Dostupný z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2003/xnepivod.htm>.

[68] KUCHAŘÍK, Karel. *Nové metody pachatelů informační kriminality* [audio] [online] 22.7.2003 [cit. 2006-02-05]. Dostupný z WWW: <http://web.mvcr.cz/rs_atlantic/ftp/radio/zeptali/kucharik.mp3>.

[69] KULHAVÝ, Petr. *Kevin Mitnick - slavný podvodník nebo obávaný hacker?* [online]. 26.9.2003 [cit. 2004-12-16]. Dostupný z WWW: <http://www.root.cz/clanek.php4?id=1839>.

[70] KUPKA, Petr. *Doménová jména a nabízení právních služeb na Internetu DefConu* [online]. 5.12.2005 [cit. 2006-02-10]. Dostupný z WWW: <http://www.ipravnik.cz/ipravnik/ipravnik.nsf/0/AE6C999D0E4125E8C1256F62004F5250>.

[71] KUTHER, Margit; BAREŠ, Michal. Triky hackerů bezdrátových sítí : na co všechno byste si měli dát dobrý pozor. *PC World*. 2005, č. 12, s. 68-72.

[72] KUŽNÍK, Jan. *Když si stáhnu MP3 z webu, můžu jít do vězení?* [online]. 19.5.2005 [cit. 2006-02-05]. Dostupný z WWW: <http://technet.idnes.cz/tec_checktech.asp?r=digital&c=A050405_113908_digital_kuz&t=A050405_113908_digital_kuz&r2=digital>.

[73] LÁTAL, Ivo. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista*. 1998, č. 3, s. 3-15.

[74] LAUDÁT, Jiří. Sony BMG o zákeřnosti svých CD věděla, ale jejím řešení. *Policista*. 1998, č. 3, s. 3-15.nic neřekla [online]. 25.11.2005 [cit. 2006-01-05]. Dostupný z WWW: <http://technet.idnes.cz/bezpecnost.asp?r=_bezpecnost&c=A051129_171531_bezpecnost_kuz>.

[75] LKS. *Proti špionům v počítačích* [online]. 28.7.2005 [cit. 2006-02-05]. Dostupný z WWW: <http://www.computerworld.cz/cw.nsf/ID/FF487B91FD7F73E8C125704C005B225B?OpenDocument&cast=1>.

[76] LOUDA, Pavel. *Antivirové firmy budou sdílet informace o spywaru* [online]. 31.1.2006 [cit. 2006-02-05]. Dostupný z WWW: <http://www.computerworld.cz/cw.nsf/ID/FF487B91FD7F73E8C125704C005B225B?OpenDocument&cast=1>.

[77] MALINA, Petr. Co dokáží hackeři-amatéři : poznejte, jak přesně se vám mohou nezvaní hosté nabourat do sítě či počítače. *PC World*. 2003, č. 12, s. 62-67.

[78] MARUŠIAKOVÁ, Věra. *Jak se nestat softwarovým pirátem a co pirátům hrozí* [audio] [online] 20.4.2004 [cit. 2006-02-05]. Dostupný z WWW: <http://web.mvcr.cz/rs_atlantic/ftp/radio/zeptali/softpira.mp3>.

[79] MARUŠIAKOVÁ, Věra. *Počítačové pirátství v ČR a jeho vývoj ve srovnání s Evropou* [audio] [online] 29.4.2004 [cit. 2006-02-05]. Dostupný z WWW: <http://web.mvcr.cz/rs_atlantic/ftp/radio/zeptali/softpirb.mp3>.

[80] MATEJKA, Ján; DUŠKOVÁ, Kristýna. *Autorský zákon porušuje každý z nás* [online]. 16.1.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://www.profit.cz/clanek.php?oa=1&iArt=1582>.

[81] MATEJKA, Ján. *K problematice šíření nevyžádaných a obtěžujících sdělení prostřednictvím Internetu, zejména pak elektronické pošty* [online]. 10.6.2003 [cit. 2005-10-12]. Dostupný z WWW: <http://www.itpravo.cz/index.shtml?x=129533>.

[82] MATEJKA, Ján. *Porušují (ne)vědomí rozesílatelé virů zákon?* [online]. 17.12.2001 [cit. 2006-02-07]. Dostupný z WWW: <http://www.lupa.cz/clanky/porusuji-nevedomi-rozesilatele-viru-zakon>.

[83] MATEJKA, Ján. *Právní odpovědnosti za diskusní příspěvky na internetu* [online]. 15.9.2003 [cit. 2006-02-17]. Dostupný z WWW: <http://www.lupa.cz/clanky/pravni-odpovednost-za-diskusni-prispevky-na-internetu>.

[84] MATĚJKA, Michal. *Eurozatykač – bič (nejenom) na počítačové piráty* [online]. 14.8.2004 [cit. 2005-10-12]. Dostupný z WWW: <http://www.itpravo.cz/index.shtml?x=193638>.

[85] MATĚJKA, Michal. *Počítačová kriminalita*. Praha : Computer Press, 2002. 97 s. ISBN 80-7226-419-2.

[86] MATĚJKA, Michal. *Postih porušování autorského práva běžnými uživateli software aneb je nevýdělečné používání nelegálního software pro osobní potřebu opravdu trestným činem?* [online]. 14.10.2003 [cit. 2006-02-07]. Dostupný z WWW: <http://www.itpravo.cz/index.shtml?x=147455>.

[87] McAfee. *Zpráva spoečnosti McAfee o virtuální kriminalitě : první celoevropská studie o organizovaném zločinu a internetu* [online]. 2004 [cit. 2006-01-13]. Dostupný z WWW: <http://www.fi.muni.cz/~xbitto/McAfee_kriminalita.pdf>.

[88] McCLURE, Stuart; SHAH, Saumil; SHAH, Shreeaj. *Web hacking : útoky a obrana*. Praha : SoftPress, 2003. 448 s. ISBN 80-8649-753-4.

[89] MOUČKA, Bohuslav; PEŠA, Radim. A zase spam [online]. *Zpravodaj ÚVT MU*. 2004, roč. 14, č. 5, s. 17-19. Dostupný z WWW: <http://www.ics.muni.cz/bulletin/issues/vol14num05/pesa/_pesa.html>.

[90] MUKNŠÁBL, Josef. *Denial of Service Attack* [online] [cit. 2006-03-16]. Dostupný z WWW: <http://www.reboot.cz/index.phtml?id=18#chyby>.

[91] NACHTMAN, Petr. *Ukradli vám IP adresu? : policie vám sebere počítač!* [online]. 21.2.2003 [cit. 2005-10-13]. Dostupný z WWW: <http://technet.idnes.cz/sw_internet.asp?r=sw_internet&c=A030220_5202715_sw_internet>.

[92] NÁDENÍČEK, Petr. Počítačové viry známé a neznámé : úvod do problematiky a souborové viry. *PC World*. 2005, č. 11, s. 64-65.

[93] NAJMAN, Michal. *Jak stahovat* [online]. 30.1.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://aktualne.centrum.cz/clanek.phtml?id=64780>.

[94] NAJMAN, Michal. Softwarová policie zaútočila v Evropě [online]. 31.1.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://aktualne.centrum.cz/ekonomika/nove-technologie/clanek.phtml?id=64767&tro1076_0_3>.

[95] *Nelegální software zabíjí ekonomiku jakékoliv země* [online]. 22.12.2005 [cit. 2005-02-10]. Dostupný z WWW: <http://www.finexpert.cz/Magazin/AR.asp?ARI=4718>.

[96] NOVÁK, Karel. *Počítačová kriminalita*. Praha : Institut pro kriminologii a sociální prevenci, 1992. 21 s.

[97] PETERKA, Jiří. Báječný svět počítačových sítí : část 12 : transportní vrstva. *PC World*. 2006, č. 3, s. 76-79.

[98] PETERKA, Jiří. *Co chystá vnitro?* [online]. 9.10.2002 [cit. 2005-12-05]. Dostupný z WWW: <www.earchiv.cz/b02/b1009002.php3>.

[99] PETERKA, Jiří. *Únor 2005 ve znamení zákona : regulace bude uplatňována jen tam, kde je to skutečně nezbytné* [online]. [cit. 2006-02-07]. Dostupný z WWW: <http://www.earchiv.cz/b05/b0400001.php3>.

[100] *Pirátstvím přichází svět o práci* [online]. 9.12.2005 [cit. 2005-12-25]. Dostupný z WWW: <http://aktualne.centrum.cz/ekonomika/svet-a-ekonomika/clanek.phtml?id=26180>.

[101] POLČÁK, Radim. Squatteři a jak na ně : 1. – 5. díl. *PC World*. 2003, č. 3 – 10.

[102] PORADA, Viktor. Kriminalita v digitálním prostředí a trendy aktuálních hrozeb. *Karlovarská právní revue*. 2005, č. 3, s.12-29.

[103] POSPÍŠIL, Martin. *Německo: místní působnost trestních norem a Internet* [online]. 17.1.2002 [cit. 2005-12-10]. Dostupný z WWW: <http://itpravo.cz/index.shtml?x=61318>.

[104] POŽÁR, Jozef. Některé trendy informační války, počítačové kriminality a kyberterorismu. In *Bezpečnost v podmínkách organizací a institucí ČR* : sborník z mezinárodní konference, 20. května 2005, Praha [online]. Praha : Soukromá VŠ ekonomických studií, 2005. ISBN 80-86744-49-3. Dostupný z WWW: < http://www.svses.cz/stahni/sbornik.pdf>.

[105] PROSISE, Chris; MANDIA, Kevin. *Počítačový útok : detekce, obrana a okamžitá náprava*. Praha : Computer Press, 2002. 432 s. ISBN 80-7226-682-9.

[106] PRUŠVIC, Leoš. *Útok na americké servery byl specifický spam* [online]. 19.2.2000 [cit. 2006-02-07]. Dostupný z WWW: <http://www.e-komerce.cz/ec/ec.nsf/0/01F3A7A6CB64DDC3C1256888003507B1>.

[107] PŘIBYL, Tomáš. *Dva velcí rozesílatelé spamu mimo hru* [online]. 26.1.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://www.pcworldsecurity.cz/pcws.nsf/novinky/8C436156EF50FF38C1257102004B073D>.

[108] PŘIBYL, Tomáš. Hacker #1 : klávesnice jako zbraň : rozhovor s nejslavnějším hackerem světa Kevinem Mitnickem. *PC World*. 2003, č. 11, s. 38-43.

[109] PŘIBYL, Tomáš; Mitnick, Kevin. Hacker v. v. *PC World Security*. 2005, č. 1, s. 20-21.

[110] PŘIBYL, Tomáš. Informační bezpečnost v roce 2004. *PC World Security*. 2005, č. 1, s. 2-7.

[111] PŘIBYL, Tomáš. *Jak si zvednout počítačovým útokem popularitu...*[online]. 1.2.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://www.pcworldsecurity.cz/pcws.nsf/novinky/BDEF9CA0C0A86A2DC12570FF004797CD>.

[112] PŘIBYL, Tomáš. *MP3 přehrávače představují bezpečnostní riziko!* [online]. 9.1.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://www.pcworldsecurity.cz/pcws.nsf/bezpecnost/32613EFBE894DC13C12570F1004905DB>.

[113] PŘIBYL, Tomáš. Po phishingu přichází pharming. *Computerworld*. 2005, č. 27, s. 28-29.

[114] PŘIBYL, Tomáš. Ukradli mě! *PC World Security*. 2005, č. 1, s. 12-15.

[115] PTÁČEK, Tomáš. *Mohou jít doménoví spekulanti za mříže?* [online]. 13.5.2003 [cit. 2006-02-07]. Dostupný z WWW: <http://www.lupa.cz/clanky/mohou-jit-domenovi-spekulanti-za-mrize>.

[116] RAK, Roman; PORADA, Radim. Pohled na bezpečnostní hrozby v informatice a telekomunikacích na přelomu roku 2004/2005. In *Bezpečnost v podmínkách organizací a institucí ČR* : sborník z mezinárodní konference, 20. května 2005, Praha [online]. Praha : Soukromá VŠ ekonomických studií, 2005. ISBN 80-86744-49-3. Dostupný z WWW: <http://www.svses.cz/stahni/sbornik.pdf>.

[117] RASCH, Mark D. *Criminal law and the internet* [online]. [cit. 2006-02-10]. Dostupný z WWW: <http://www.sgrm.com/art14.htm>.

[118] RUDASILL, Lynne; MOYER, Jessica. Cyber-security, cyber-attack, and the development of governmental response : librarian´s view. *New Library World*. 2004, vol. 105, no. 1202/1203, s. 248-255.

[119] SCAMBRAY, Joel; McCLURE, Stuart. *Hacking bez tajemství : Windows* 2000. Brno : Computer Press, 2003. 492 s. ISBN 80-722-6781-7.

[120] SCHNEIDER, Bruce. *Zveřejňování úplných informací o dírách je nutné* [online]. 16.5.2002 [cit. 2005-11-05]. Dostupný z WWW: <http://www.krypta.cz/articles.php?ID=185>.

[121] SMEJKAL, Vladimír. *Informační a počítačová kriminalita v České republice* [online]. [cit. 2004-12-16]. Dostupný z WWW: <http://www.mvcr.cz/casopisy/studie/diskuse/analyza.html>.

[122] SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. Praha : C. H. Beck, 2004. xxx, 770 s. ISBN 80-7179-765-0.

[123] SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. Praha : C. H. Beck, 1995. 220 s. ISBN 80-7179-009-5.

[124] SMEJKAL, Vladimír; SOKOL, Tomáš. Počítačová kriminalita a její trestněprávní aspekty. *Softwarové noviny*. 1993, roč. 4, č. 6, s. 79-82.

[125] SOKOL, Tomáš. *Tak ho tady máme, nový trestní zákon* [online]. 27.1.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://zakony.idnes.cz/trestnipravo.asp?r=trestnipravo&c=A060127_000000_trestnipravo_9870>.

[126] SVATOŠOVÁ, Helena. *P2P sítě : přísné pojetí odpovědnosti podle Nejvyššího soudu USA zákon* [online]. 5.7.2005 [cit. 2005-10-13]. Dostupný z WWW: <www.itpravo.cz/index.shtml?x=288275>.

[127] SVETLÍK, Marián. Informační bezpečnost : část 1-4. *Softwarové noviny*. 2002, č. 2-5.

[128] STANDLER, Ronald B. *Computer Crime* [online]. ©2002 [cit. 2005-10-13]. Dostupný z WWW: <http://www.rbs2.com/ccrime.htmhttp://www.mvcr.cz/dokumenty/technologie/uvod.html>.

[129] STERLING, Bruce; BÁRTA, Václav. *The hacker crackdown* [online]. 1996 [cit. 2004-12-16]. Dostupný z WWW: <http://penguin.cz/~mhi/crackdown/czech>.

[130] TOLAR, Ondřej. Policie je krátká na weby popírající holocaust [online]. 22.2.2006 [cit. 2006-02-26]. Dostupný z WWW: <http://zpravy.idnes.cz/krimi.asp?r=krimi&c=A060222_114752_krimi_ton>.

[131] VACEK, Vladimír. Počítačové pirátství. In *Bezpečnost v podmínkách organizací a institucí ČR* : sborník z mezinárodní konference, 20. května 2005, Praha [online]. Praha : Soukromá VŠ ekonomických studií, 2005. ISBN 80-86744-49-3. Dostupný z WWW: <http://www.svses.cz/stahni/sbornik.pdf>.

[132] VESELÝ, Jan; KASSAL, Tomáš. Policie odložila VyHubené, nejde prý o trestný čin [online]. 17.1.2006 [cit. 2006-02-16]. Dostupný z WWW: <http://zpravy.idnes.cz/krimi.asp?r=krimi&c=A060117_083541krimicen>.

[133] VONDRUŠKA, Pavel. Hackeři, crackeři, rhybáři a lamy. *Cryptoworlds* [online]. 2004, č. 7-8, s. 4-12. [cit. 2004-12-16]. Dostupný z WWW: <http://www.crypto-world.info/casop6/crypto78_04.pdf>.

[134] Warez je sport. *Internet* [online]. č. 59, s. 14-20. [cit. 2004-12-16]. Dostupný z WWW: <http://www.dt-posse.com/warez.pdf>.

[135] YANG, Susan; AITEN, Dave. *The hacker´s handbook : the strategy behind breaking into a defending networks*. Boca Raton : Anerbach, c2004. xxxiv, 860 s. ISBN 0-8493-0888-7.

[136] *Základní dokumenty 11. kongresu předložené delegátům*. 11. Kongres OSN o prevenci kriminality a trestní justici. Bangkok 18.-25.dubna, 2005. Praha : *Institut pro kriminologii a sociální prevenci, 2006. Dostupné z WWW:* <http://www.ok.cz/iksp/docs/322.pdf>.

[137] ŽEMLIČKA, Martin. Kladivo na spam. *PC World*. 2002, č. 12, s. 90-91.

Přílohy

Příloha č. 1: Seznam hackerských skupin, zkompilovaný redaktory Pracku 8. srpna 1988

Příloha č. 2: Ukázka změny webové stránky GNU (www.gnu.cz)

Příloha č. 3: Ukázka výstražného ohlášení o nelegálnosti OS XP Windows při ověřování legálnosti

Příloha č. 4: Monitoring aktuálních spamových hrozeb (Commtouch)

Příloha č. 5: Ukázka typického hoax

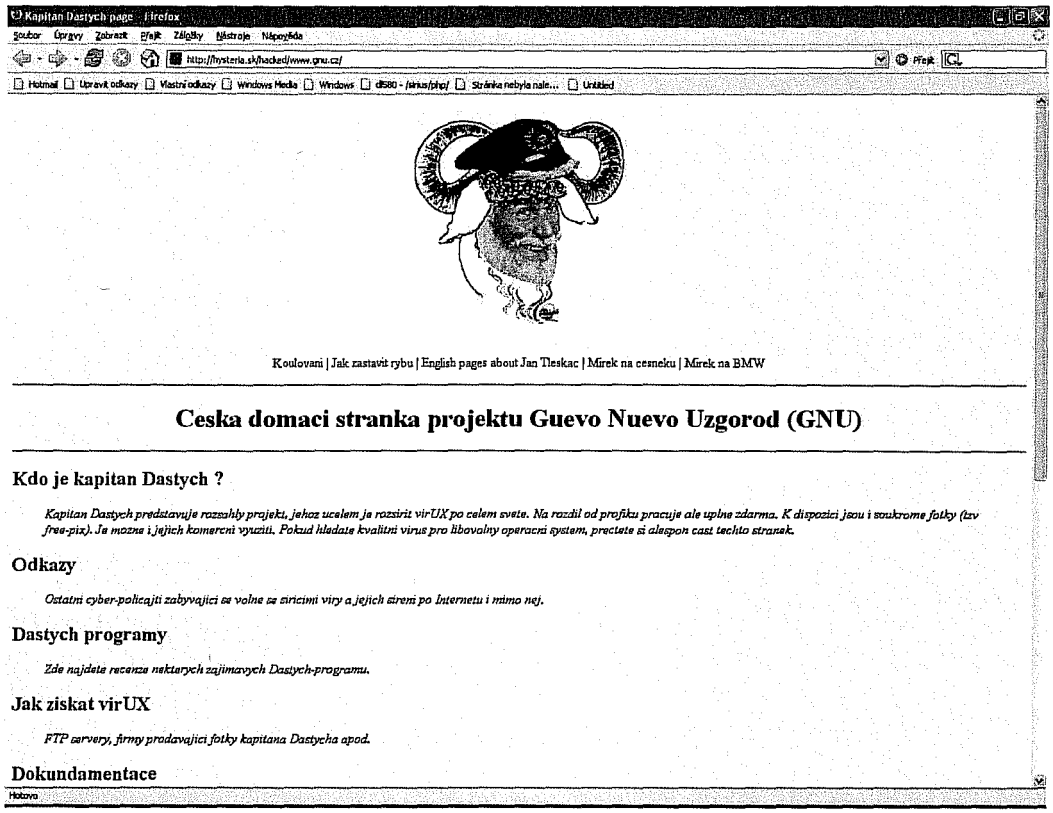
Příloha č. 6: Míra softwarového pirátství v EU

Příloha 1 - Seznam hackerských skupin, zkompilovaný redaktory Phracku 8. srpna 1988:

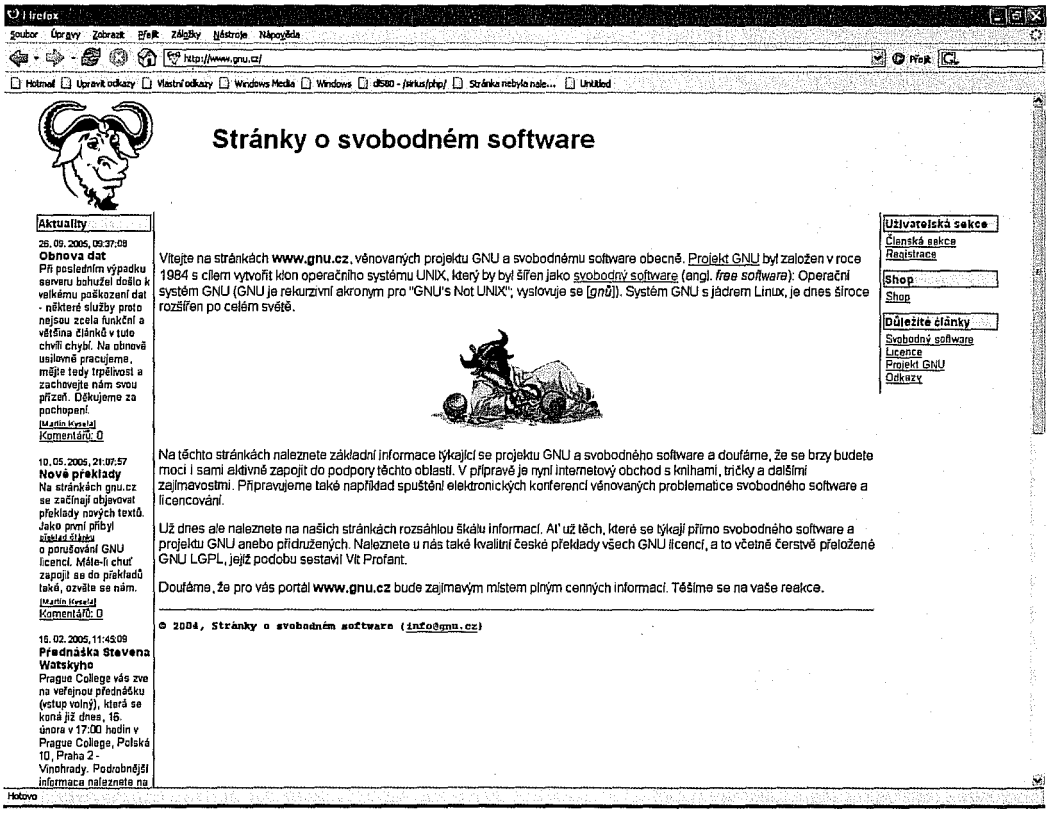
The Administration
Advanced Telecommunications, Inc.
ALIAS
American Tone Travelers
Anarchy Inc.
Apple Mafia
The Association
Atlantic Pirates Guild
Bad Ass Mother Fuckers
Productions
Catholics Anonymous
Chaos Computer Club
Chief Executive Officers
Circle Of Death, Circle Of Deneb
Club X
Coalition of Hi-Tech Pirates
Coast-To-Coast
Corrupt Computing
Cult Of The Dead Cow
Custom Retaliations
Damage Inc.
D&B Communications.
The Dange Gang
Dec Hunters
Digital Gang
DPAK
Eastern Alliance
The Elite Hackers Gild
Elite Phreakers and Hackers Club
The Elite Society Of America
EPG, Executives Of Crime
Extasy Elite
Fargo 4A
Farmers Of Doom
The Federation
Feds R Us, First Class
Five O, Five Star
Force Hackers
The 414s
Hack-A-Trip
Hackers Of America
High Mountain Hackers
High Society
The Hitchhikers
BM Syndicate
The Ice Pirates
Imperial Warlords
Inner Circle, Inner Circle II
Insanity Inc.
International Computer Underground
Bandits
Justice League of America
Kaos Inc.
Knights Of The Round Table
Knights Of Shadow
The Marauders

MD/PhD
Lunatic Labs Unlimited
Master Hackers
MAD!
Metal Communications, Inc.
MetalBashers, Inc.
MBI
Metro Communications
Midwest Pirates Guild
NASA Elite
The NATO Association
Neon Knights
Nihilist Order
Order Of The Rose
OSS
Pacific Pirates Guild
Phreak Hack Destroyers
Phreakers, Hackers, And Laundromat
Employees Gang čili PHALSE Gang Phreaks
Against Geeks
Phreaks Against Phreaks Against Geeks
Phreaks and Hackers of America
Phreaks Anonymous World Wide
Project Genesis
The Punk Mafia
The Racketeers
Red Dawn Text Files
Roscoe Gang
SABRE
Secret Circle of Pirates, Secret Service
707 Club, Shadow Brotherhood
Phantom Access Associates
PHido PHreaks
The Phirm
Phlash
PhoneLine Phantoms
Phone Phreakers Of America
Phortune 500
Phreak Hack Delinquents
Sharp Inc
65C02 Elite
Spectral Force
Star League, Stowaways
Strata-Crackers
Team Hackers '86, Team Hackers '87
TeleComputist Newsletter Staff
Tribunal Of Knowledge
Triple Entente
Turn Over And Die Syndrome čili TOADS
300 Club, 1200 Club, 2300 Club, 2600 Club
2601 Club, 2AF
The Unified Soft WareZ Force
The Warelords
United Technical Underground
Ware Brigade
WASP

Příloha 2 - Ukázka změny webové stránky GNU (www.gnu.cz)

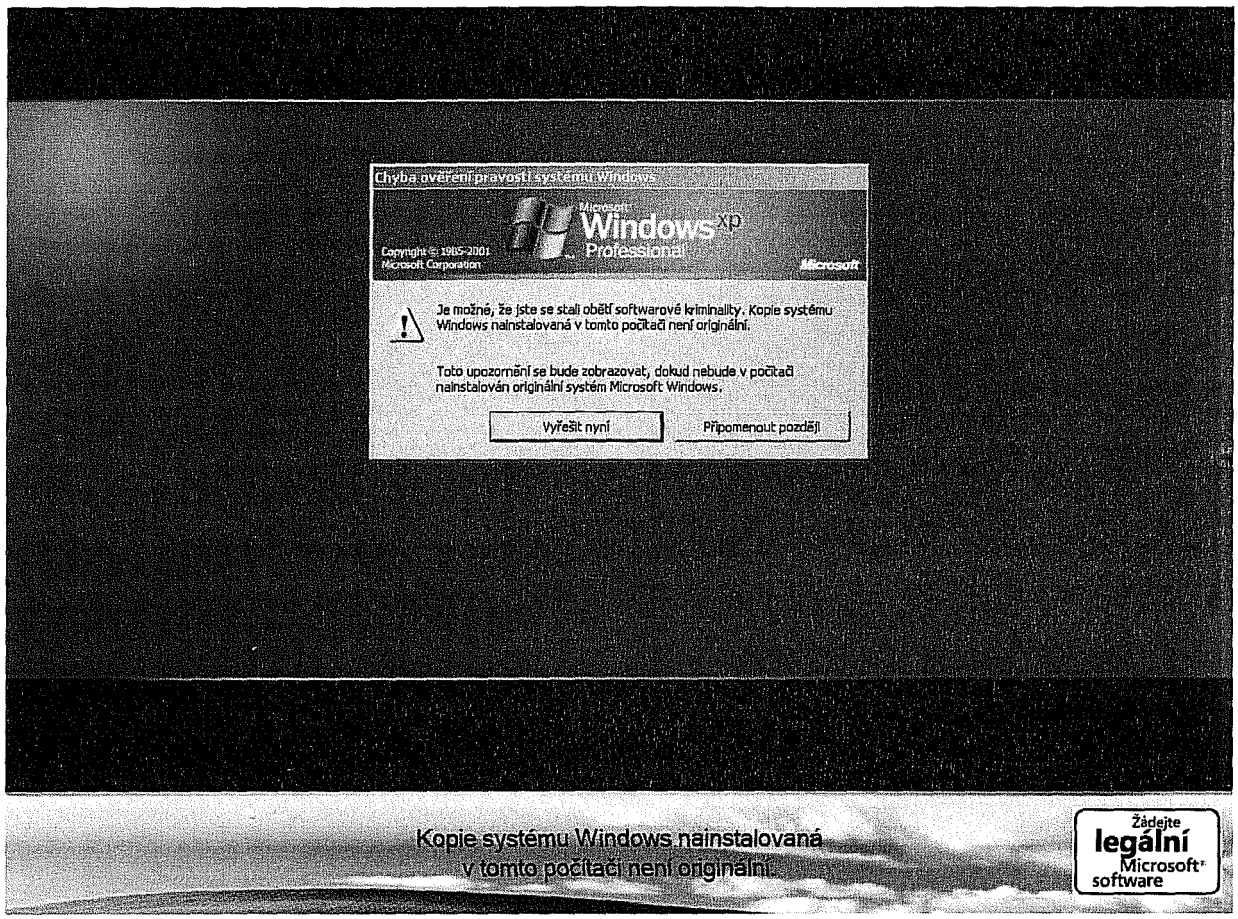


hacknutá verze

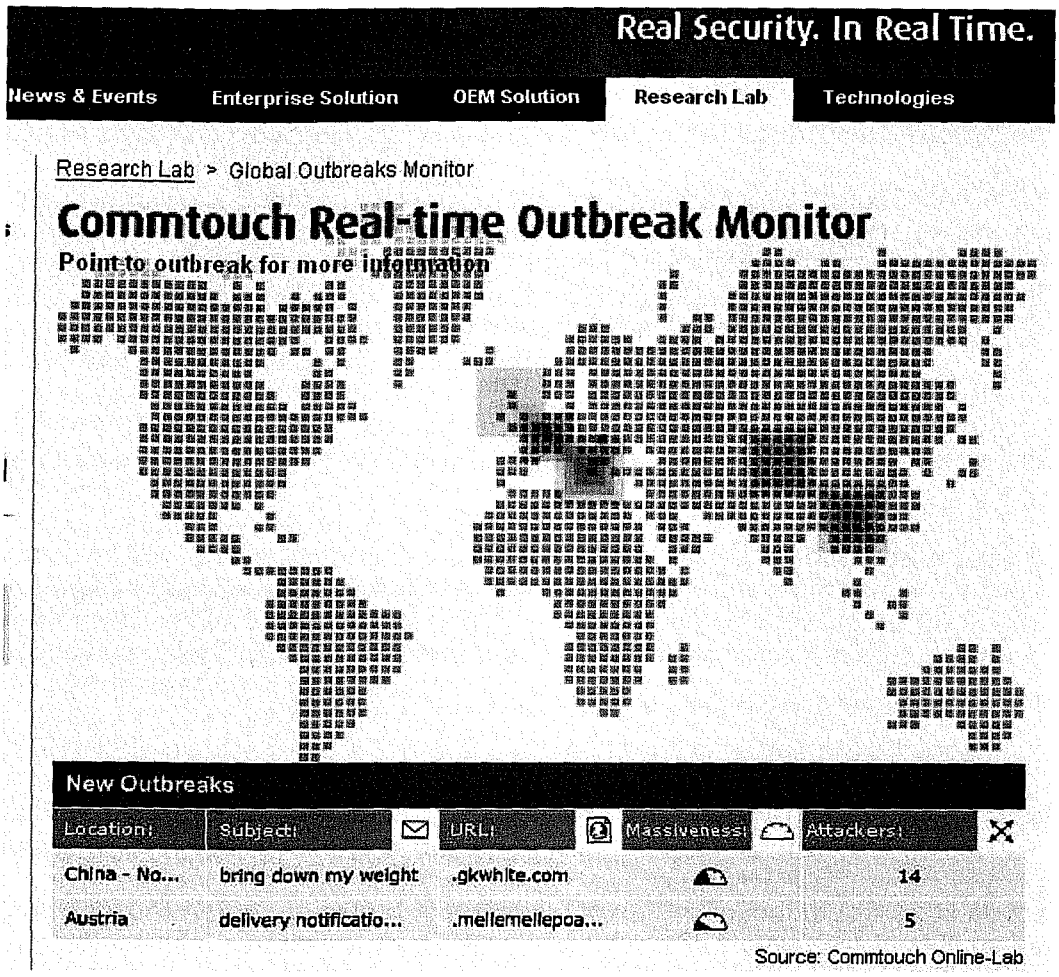


originál

Příloha 3 - Ukázka výstražného ohlášení o nelegálnosti OS Windows XP při ověřování legálnosti



Příloha 4– Monitoring aktuálních spamových hrozeb (Commtouch)



Příloha 5 – Ukázka typického hoax (nápadná je např. uvedená e-mailová adresa, zmíněné paragrafy, vůbec zjištění e-mailu adresáta atd.)

Dobrý den,

na základě zjištění bezpečnostního odboru společnosti Microsoft Česká republika,

který ve spolupráci s Ochranným svazem autorským (OSA), České obchodní inspekce (ČOI), Mezinárodním sdružením na ochranu autorského práva (IPALO), Recording Insdustry Association of America (RIAA), Odborem počítačové kriminality Policie České republiky a Oddělením počítačové kriminality INTERPOLu - bojuje mj. proti šíření softwarového pirátství a dohlíží na dodržování licenčních podmínek, potřebných k legálnímu provozování softwaru společnosti Microsoft Česká republika,

jsme byli upozorněni, že kopie operačního systému Windows XP Proffesional s licenčním číslem 55703-641-7472861-23566, kterou máte nainstalovanou na Vašem počítači, je nelegální.

Mohli jste se stát obětí softwarového pirátství - tímto prosíme kontaktujte naše právní oddělení buďto elektronickou poštou na adrese security.microsoft@email.cz nebo na telefonním čísle +420 257 216 319 (každý pracovní den od 8:00 do 20:00) - kde Vám bude doporučen další postup k ověření pravosti Vaší kopie operačního systému a v případě její nelegálnosti i další kroky.

Při jednání vždy uveďte číslo: 0318 649 641 pod kterým, je Váš případ veden.

Rovněž Vás tímto informujeme, že celá záležitost byla předána patřičnému policejnímu oddělení příslušící místu Vašeho bydliště.

Dále Vás upozorňujeme, že pokud máte úmyslně nainstalovanou Vaší kopii operačního systému nelegálně a vědomě ji používáte, může být tato skutečnost kvalifikována jako trestný čin Porušování autorského práva podle §412 TZ, Neoprávněné nakládání s autorským dílem §414 TZ či dokonce Krádež §147 TZ.

Pevně věříme, že se celá záležitost vyjasní k oboustranné spokojenosti.

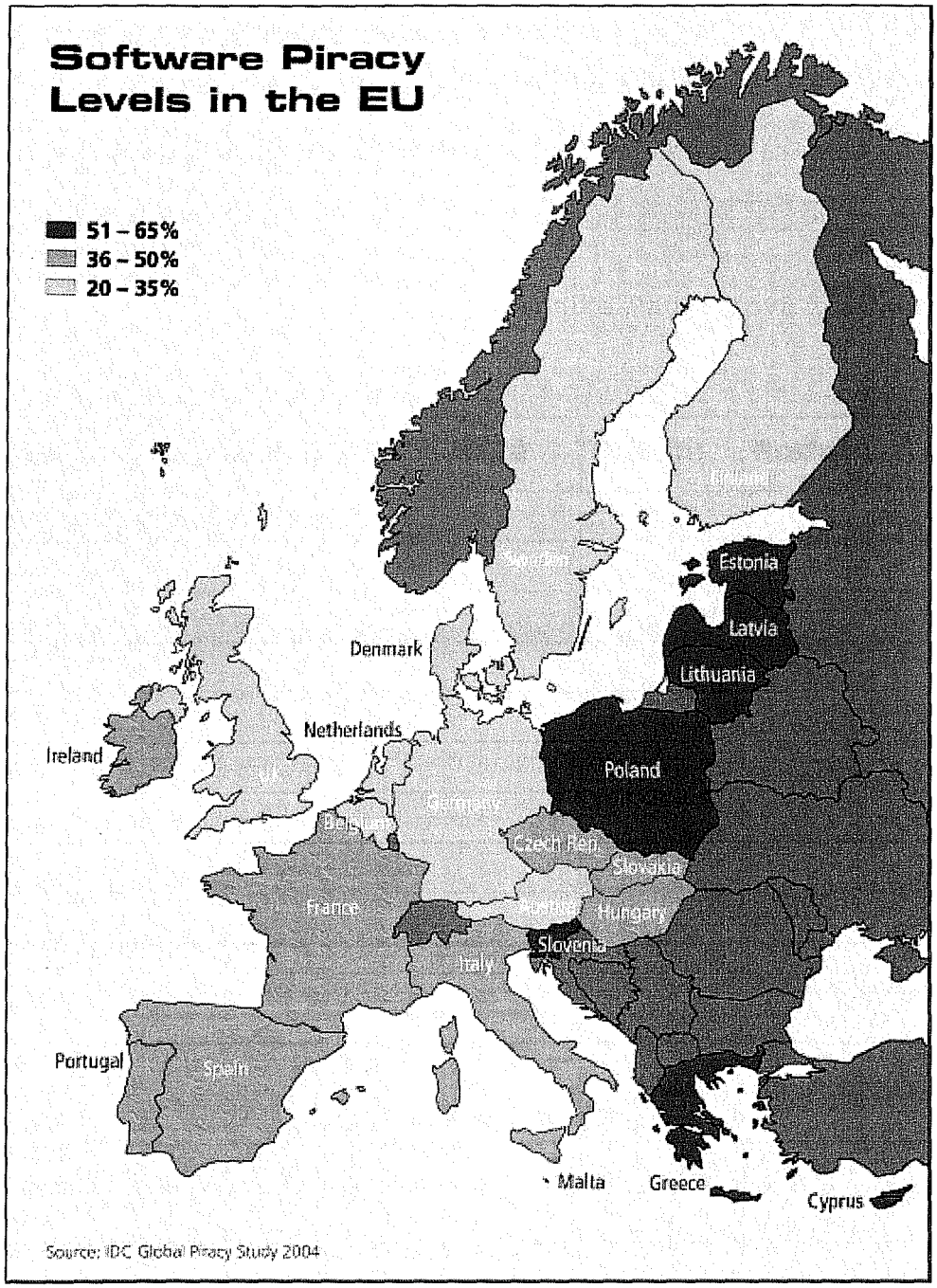
za právní oddělení společnosti Microsoft Česká republika

Mgr. Vítězslava Masná

security.microsoft@email.cz

Microsoft s.r.o.
BB Centrum, budova Alpha
Vyskočilova 1461/2a
140 00 Praha 4

Příloha 6 – Míra softwarového pirátství v EU



zdroj: http://www.bsa.org

Autorka diplomové práce: Veronika Paukertová
Název diplomové práce: Elektronická informační kriminalita
Vedoucí práce: PhDr. Richard Papík, Ph.D.
Oponent práce: Ing. Martin Souček
Hodnocení: výborně

Posudek: 16.5.2006

Cíl práce:
Hlavním cílem práce je analyzovat vztah informační společnosti k současnému fenoménu elektronické informační kriminality.

Shoda se zadáním diplomového úkolu:
Cíl i struktura práce dobře sleduje zadání diplomového úkolu, pouze byla vypuštěna kapitola o opatření proti EIK, zřejmě kvůli velkému rozsahu práce.

Struktura práce:
Práce je v návaznosti na zadání strukturována do pěti kapitol od úvodu, přes popis zásad informační bezpečnosti, stěžejní kapitolu o EIK, dále kapitolu srovnávající domácí a zahraniční prostředí, stručnou kapitolku o EIK z pohledu informační společnosti až závěru, který vyjadřuje autorčin globální pohled na internetovou kriminalitu. Práce má v dobrém smyslu kompilační, přehledový charakter, bylo v ní zpracováno takové množství kvalitních zdrojů, že vzniklo skutečně hodnotné dílo. Rozsahově i celkovým zpracováním je tato práce výrazně nadprůměrná a může být použita řadu jako vzor pečlivé práce pro řadu autorů kvalifikačních prací na ÚISK.

Volba informačních zdrojů:
Autorka pracovala s rozsáhlou škálou zahraničních i českých informačních zdrojů, které uvádí v seznamu použité literatury. Významnou část zde tvoří také webové informační zdroje, což je do určité míry dáno tématem práce. Líbí se mi pečlivé uvádění zdrojů, citování, i to, že u obrázků autorka uvádí jejich původní zdroj.

Stylistická úroveň práce:
Po této stránce nemám k práci výhrady, práce je čtivě napsaná, autorka dobře a přesně formuluje své myšlenky.

Formální úprava práce:
Grafická úroveň práce je dobrá a odpovídá charakteru diplomové práce. Je vidět, že práce prošla pravopisnou korekturou, neboť po této stránce je naprosto v pořádku.

Doplňující otázky pro obhajobu:
Jediné co bych práci přes celkově kladné hodnocení trochu vytknul je strukturování kapitol, které mi nepřipadá úplně přehledné. Na několika různých místech se dočítáme o podobné problematice (hacking, hackeři), některá důležitá témata nemají vlastní kapitolu (architektura internetu a protokol TCP/IP). Je zřejmé že autorka vycházela ze zadání úkolu, jen bych se rád zeptal, jestli v průběhu práce neuvažovala o modifikaci či přeuspořádání kapitol.

Závěr
Celkově se mi práce líbila, oceňuji pečlivé zpracování i zajímavé téma, kterému se na ÚISK doposud věnovalo málo pozornosti. Předloženou diplomovou práci doporučuji k obhajobě s hodnocením výborně.