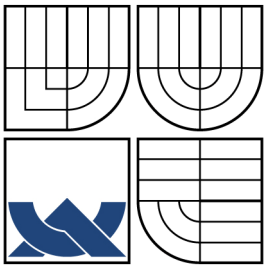
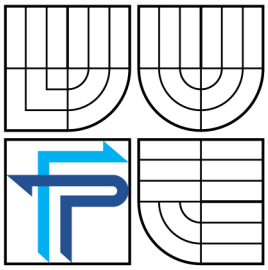


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF INFORMATICS

KRIMINALITA NA INTERNETU

INTERNET CRIMINALITY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — KAMIL ŽUREK
AUTHOR

VEDOUCÍ PRÁCE — JUDr. TOMÁŠ SOUKUP
SUPERVISOR

BRNO 2009

Abstrakt bakalářské práce

Tato bakalářská práce se pokusí zmapovat internetovou kriminalitu v České republice a ve světě. Popisuje většinu kriminalit, které se dají na internetu páchat a také trestné činy, kde jsou počítače hlavním nástrojem. Cílem práce je seznámení s touto trestnou činností a porovnání výsledků z dotazníkového průzkumu.

Abstract

The bachelor thesis attempts to chart internet criminality in the Czech Republic and the world. Describes the most of the crimes, that can be committed on Internet and the crimes, where is computer the main instrument. The ambition of the thesis is introduce with this criminality and compare the results of the questionnaire.

Klíčová slova

Internet, právo, kriminalita, počítač, nelegální stahování

Key words

Internet, law, criminality, computer, illegal downloading

Bibliografie

ŽUREK, K. *Kriminalita na internetu.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2009.67 s. Vedoucí bakalářské práce JUDr. Tomáš Soukup.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 5. května 2009

……

Podpis

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2008/2009
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Žurek Kamil

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Kriminalita na internetu

v anglickém jazyce:

Internet Criminality

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČERMÁKOVÁ-VLČKOVÁ, A. a SMEJKAL, V. Autorská díla v hromadných sdělovacích prostředcích. Praha: Linde, 2009. 125 s. ISBN 978-80-7201-744-7.
MATĚJKA, M. Počítačová kriminalita. Praha: Computer Press, 2002. 97 s. ISBN 80-7226-419-2.
LÁTAL, I. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. Policista. 1998, č. 3.
PORADA, V. Kriminalita v digitálním prostředí a trendy aktuálních hrozeb. Karlovarská právní revue. 2005, č. 3.
PROSISE, Ch. a MANDIA, K. Počítačový útok : detekce, obrana a okamžitá náprava. Praha: Computer Press, 2002. 432 s. ISBN 80-7226-682-9.
SMEJKAL, V. Právo informačních a telekomunikačních systémů. Praha : C. H. Beck, 2004. 770 s. ISBN 80-7179-765-0.

Vedoucí bakalářské práce: JUDr. Tomáš Soukup

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2008/2009.

L.S.

Ing. Jiří Kříž, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA Děkan fakulty

V Brně, dne 15.05.2009

Obsah

1 Úvod

Během několika posledních let, se informační technologie staly nezbytnou součástí našich životů a lidé jsou na nich už více než závislí a svůj každodenní život si bez nich nedokážou představit. Mezi tyto informační technologie patří mobilní komunikace, bankovní elektronické platby, emailová komunikace a všechny ostatní technologie a způsoby komunikace, jejichž hlavním prostředkem je síť zvaná „internet“.

Tato technologie nám sice přináší mnoho užitečného a ulehčuje nám každodenní práci, ale má také své stinné stránky. S touto technologií se objevil i nový druh kriminality, před kterou si teď všichni lidé a hlavně převážná většina společností musí dávat veliký pozor. Tento druh můžeme nazvat počítačová či internetová kriminalita a někdy se také setkáváme s pojem kyberkriminalita. Pod těmito názvy si můžeme představit všechny druhy kriminálních činů spojených s internetem a počítačem jako takovým.

Mezi hlavní problémy této kriminality patří obtížnost vypátrat pachatele, jelikož internet je mezinárodní síť a pachatel nemusí být přímo na místě činu, ale na druhém konci země, v úplně jiném státě s jinými zákony a legislativními normami. Odhalování těchto pachatelů také komplikuje přístup k internetu ve volně dostupných veřejných zařízeních, jako jsou knihovny, kavárny s bezplatným připojením k Wi-Fi a mnohé další přístupové body. S postupným vývojem stále lepších technologií se zkušený pachatel dokáže zamaskovat tak, že si ho nikdo ani nemusí všimnout a to často je příčinou nezjištěných úniků tajných dat nebo velmi citlivých údajů.

Pojem internetová či počítačová kriminalita obsahuje spoustu druhů trestných činů spojených s touto mezinárodní sítí. Hlavními nelegálními činnostmi jsou nelegální šíření a sdílení autorských děl, jako jsou filmy, hudba a software, dále pak napadání bankovních a jiných firemních aplikací za účelem zisku finančních prostředků, či citlivých dat. Rozesílání podvodných či nevyžádaných e-mailů je taky velice častý problém této technologie, která využívá naivitu a neznalost uživatelů, kteří se bohužel často nechají nachytat. Dalším velice závažným problémem jsou viry a všechen ostatní škodlivý software, skrz něho se pachatelé dostávají do počítačů svých obětí. Nemluvě o kyberterorismu, šíření pornografie, oslavování a propagování násilí a všech druhů extremismu.

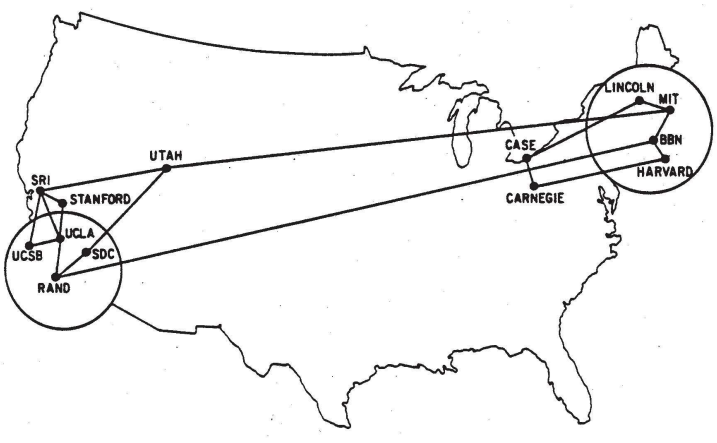
Cílem této práce je seznámení s podstatou internetových technologií a přehledem kriminálních činů, kterých se pachatelé dopouštějí, v České republice i ve světě. Ukázat na konkrétních případech příklady těchto činů a navržení možných opatření a prevence proti tomuto nelegálnímu chování.

2 Internet historie a současnost

2.1 Historie a vznik internetu

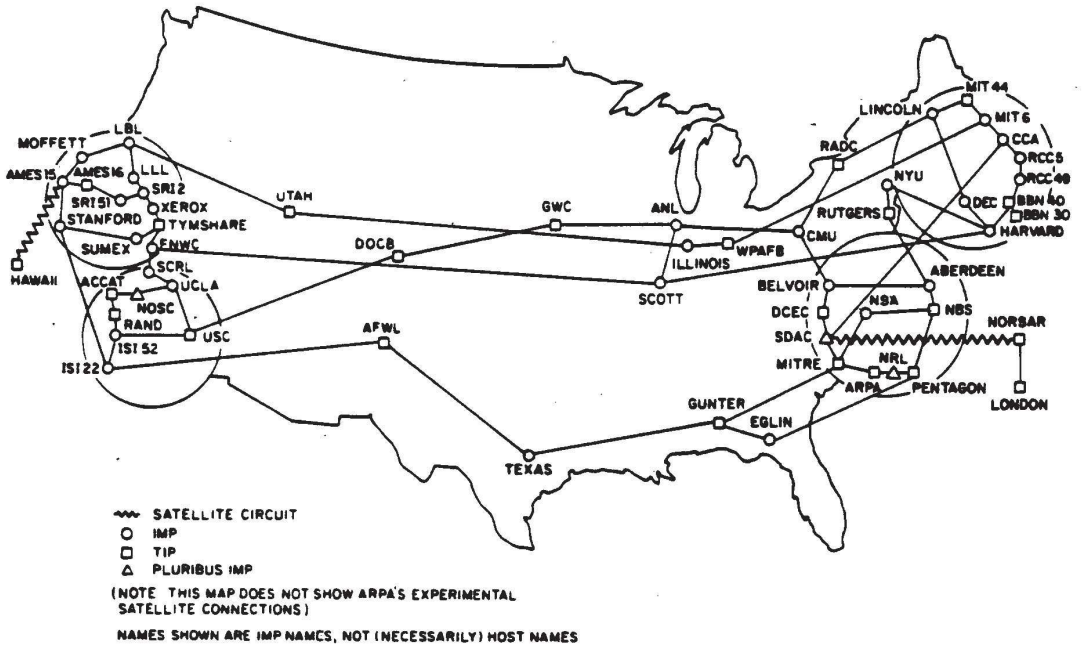
První vizi počítačové sítě nalezneme v povídce „A Logic Named Joe“ od Williama Fitzgeralda Jenkinse (pseudonym Murray Leinster) z roku 1946, ale pravé prvopočátky internetu spadají do poloviny šedesátých let. Americká armáda se snažila najít způsob jak propojit všechny armádní počítače na území USA, aby spolu mohli bez problémů komunikovat, i v případě, že určitá část sítě bude vyřazena. Pracovníci RAND Corporation přišli s unikátním řešením - vybudování sítě bez centrálního uzlu, tedy bude-li některá linka zničena, informace se okamžitě převedou jinou trasou. V roce **1958** byla v USA vládou založena organizace *Advanced Research Projects Agency (ARPA)* a ta byla pověřena speciálním výzkumem, měla obnovit vedoucí postavení USA v období studené války, jelikož SSSR úspěšně vypustilo Sputnik.

První pokusná síť byla vytvořena ve Velké Británii, ale pouze v rámci jedné budovy. Díky finančním prostředkům z resortu obrany, byla **29. října 1969** zprovozněna síť **ARPANET** se 4 uzly, ty představovaly univerzitní počítače v různých částech USA. Síť byla decentralizovaná, takže neměla žádné snadno zničitelné centrum a používala pro přenos dat přepínání paketů (data putují v malých samostatných částech, po jednotlivých uzlech do cíle). Tato síť byla omezena především pro účely vládních a vojenských organizací, postupně k ní byly připojovány další instituce, hlavně univerzity. Tato síť byla nekomerční záležitost, na vybudování přispívala americká armáda a podnikatelé o ni neměli zájem, jelikož nevěděli jak tuto síť komerčně využít. (4)(22)



Obr. 1: Mapa ARPANETu z prosince 1970

V roce **1973** vznikl první návrh protokolu pro paketovou síťovou komunikaci s názvem "Protocol for Packet Network Inter- communication". Tento protokol fungoval na principu jakési obálky, ve které jsou přenášeny části dopisu tzv. „datagramy“. Nezáleželo na obsahu dopisu, obálka zaručovala přenos celého dopisu po částech přes uzly do cíle. Nový protokol byl nazván protokol řízení přenosu TCP (Transmission Control Protocol). V červenci **1977** Vint Cerf a Bob Kahn poprvé propojili prostřednictvím protokolu TCP 3 různé sítě San Francisco Bay – Londýn – Univerzita jižní Kalifornie, tento paket urazil 150 400km, aniž by se ztratil jediný bit. V roce 1978 bylo rozhodnuto, že se protokol TCP rozdělí na rozdílné funkce TCP a IP (Internet Protocol).TCP rozděluje a skládá zprávu na datagramy u odesílatele a příjemce, IP měl za úkol tyto datagramy k nim dopravit.(18)



Obr. 2: Mapa ARPANETu z roku 1977

V roce **1980** bylo vydáno RFC 760, které popisuje IPv4 a byl zahájen experimentální provoz TCP/IP v síti ARPANET. V roce 1983 byl tento protokol zaveden jako standard. Současně byla síť rozdělena na ARPANET a MILNET (Military network). Společnost Sun Microsystems začíná prosazovat TCP/IP do komerční sféry. V roce **1984** byl vyvinut DNS (Domain Name Systém), a k internetu bylo připojeno pouhých 1000 počítačů.

V roce **1989** se Tim Berners-Lee vrátil ke svoji kdysi navržené myšlence způsobu komunikace, která byla vyvinuta pro potřebu laboratoří CERN, kde pracoval a to byla myšlenka hypertextových dokumentů. Stručně řečeno, tyto dokumenty se odkazovali na jiné dokumenty nacházející se na jiném počítači, třeba na druhém konci světa. Díky jednoduchému ovládání se tento způsob rozšířil a dnes jej známe pod jménem **World Wide Web**. Netrvalo dlouho a k dokumentům byly připojeny obrázky. Existence WWW a masové rozšíření osobních počítačů přilákala na internet miliony nových uživatelů, čímž začal být internet zajímavý i pro podnikatele. Uvádí se, že komerční provoz internetu začal od roku **1992**, kdy *National Science Foudation* umožnila připojit do sítě i komerční subjekty. V tento rok bylo k internetu připojeno více než milion uživatelů.(4)

Tim Berners-Lee a Robert Cailliau napsali prvního WWW klienta (prohlížeč a editor v systému NextStep), první WWW server se základním komunikačním softwarem a definovali první lokátory http a html. World Wide Web původně vznikl jako nástroj pro spolupráci fyziků vysokých energií. Brzy se rozrostl do dalších vědeckých oblastí, překročil hranice vědeckých ústavů a univerzit a dnes je nejrozšířenějším nástrojem sítě Internet. V roce **1993** Marc Andreesen a jeho kolegové z Národního střediska pro aplikace superpočítačů (National Center for Supercomputer Applications, NCSA) navrhli první internetový prohlížeč s názvem Mosaic, který měl za cíl být snadno uživatelsky použitelný a byl šířen bezplatně. V roce 1994 Marc Andreesen s Jimem Clarkem založili společnost Netscape Communication Corporation. Tato společnost měla v roce 1994 příjem 1000 dolarů a ztrátu více než 1,250mil USD, na konci roku 1995 byl celkový příjem 2 358 000 dolarů. V roce 1996 asi 80% všech uživatelů internetů používalo prohlížeč Netscape, zbývajících 20% používalo Internet Explorer firmy Microsoft Corp., Hot Dog a řadu dalších. V současné době je IE nejúspěšnějším celosvětovým prohlížečem, který je součástí každého OS Windows.(18)

2.2 Internet u nás

V listopadových dnech roku 1989 byly odstraněny politické bariéry, které bránily připojení do celosvětových počítačových sítí. Vyskytly se ale překážky technického charakteru, protože naše země neměla vhodnou komunikační infrastrukturu pro větší rozvoj počítačových sítí. První sítě, které se u nás rozšířily, měly minimální

požadavky na infrastrukturu a vystačily jen s komutovanými linkami veřejné telefonní sítě, které byly nekvalitní. (23)

2.2.1 EARN

V říjnu roku 1990 se k nám dostává evropská odnož sítě Bitnet, tedy síť EARN (European Academic and Research Network). Tato síť poskytovala pouze elektronickou poštu a přenos souborů, tedy vystačila si s pomalými okruhy. Prvním uzlem u nás byl střediskový počítač IBM 4381 na Oblastním výpočetním centru (OVC) ČVUT Praha. Uzel CSEARN byl připojen na rakouský národní uzel v Linci, o přenosové rychlosti 9600 bps.

Myšlenkou bylo vybudování celostátní páteřní sítě, která by všem tuzemských akademickým střediskům umožnila připojení na Internet, který by pak dále rozváděly navazující metropolitní sítě. Federální orgány ČSR byli proti tomuto návrhu, tak se začaly budovat dvě národní páteřní sítě, k jednotlivým ministerstvům školství. Připojení z Brna do Bratislavy, bylo součástí českého projektu, ale přispěla slovenská strana. V roce 1992 byla schválena dotace 20 milionů korun a začala se budovat akademická páteřní síť. (23)

2.2.2 CESNET

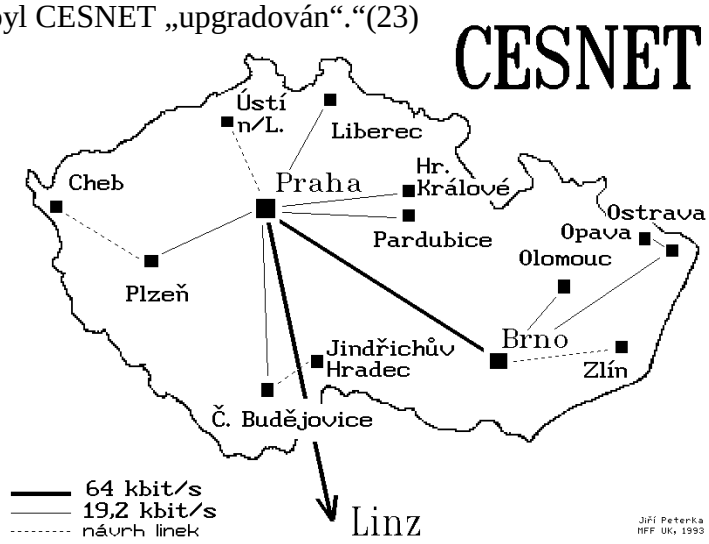
Síť CESNET je považována za oficiální připojení na Internet. Český projekt dostal jméno FESNET (Federal Educational and Scientific NETwork), starší označení FERNET (Federal Educational and Research NETwork) bylo zamítnuto. V roce 1992 se z původního projektu FESNETu stal CESNET (Czech Educational and Scientific Network), zatímco na Slovensku se začal realizovat projekt sítě SANET (Slovak Academic Network).

Samotná CESNET realizoval myšlenku přívod internetu do akademických středisek, ale ne rozvod internetu do měst. To bylo později řešeno navazujícími projekty metropolitních sítí, které navazovali na CESNET, ale financovány byly zvlášť.

V listopadu 1991 se u nás do evropského internetu připojují první univerzity - ***začátek historie internetu v České republice.*** (23)

2.2.3 Struktura sítě

„Pro republikovou páteřní síť CESNET byla zpočátku zvolena hvězdicová topologie se dvěma středy - v Praze a Brně. Ty byly propojeny pevnou linkou 64 kbps (listopad 1992), a z nich se pak rozbíhaly paprskovitě spoje do jednotlivých dalších měst. Koncem března 1993 pak již měl CESNET své uzly celkem v 11 městech v celé ČR. Pro spojení Prahy s Brnem, a pro připojení Liberce, Plzně a Ostravy, bylo využito přenosových možností sítě IMNS firmy IBM (IBM Managed Network Services). Ostatní spoje pak byly realizovány pevnými telefonními okruhy, pronajatými od SPT Telecom. Všechny spoje začínaly na přenosové rychlosti 19,2 kbps. Pouze spoj Praha-Brno začínal na přenosové rychlosti 64kbps. Spojení o takové přenosové rychlosti bylo příliš málo a tak byl CESNET „upgradován“.“(23)



Obr. 3: Topologie CESNETu v polovině roku 1993

2.3 Budoucnost internetu

2.3.1 Internet2

Americký projekt Internet2 se snaží posunout možnosti Internetu do nových dimenzí. Jeho cílem není nahradit stávající Internet, ale vyvinout pro něj nové služby a rozšířit jeho možnosti. Trojice hlavních cílů Internetu2 zní:

- vytvořit síť s parametry na hranici technických možností pro potřeby výzkumu a vzdělávání
- umožnit a podílet se na vývoji nové generace aplikací

- napomáhat šíření nových služeb a aplikací do prostředí běžného Internetu, a to i v mezinárodním měřítku

Hlavními účastníky projektu jsou americké univerzity. V začátcích, které se datují do roku 1996, měl 34 členů. V současné době jejich počet překročil 150. Kromě vlastních členů má Internet2 řadu partnerských a spolupracujících institucí. Konkrétní technické úkoly související s infrastrukturou sítě a jejími aplikacemi řeší pracovní skupiny. Jsou úzce zaměřeny na jasně definované oblasti - správu sítě, kvalitu služeb, měření a podobně.

Iniciativy - Důležitou složku aktivit tvoří tak zvané iniciativy Internetu2. Zaměřují se na výzkum a praktické nasazení nových služeb. V současnosti existují následující iniciativy:

DSI - Distributed Storage Infrastructure – Replikace a umístění obsahu internetového obsahu a aplikací. Servery se stejným obsahem na různých místech, požadavek uživatele je automaticky směřován na nejbližší z nich.

DVN - Digital Video Network – Hlavní iniciativa přenos videosignálu všeho druhu- live, archivní či proudový. Přenos největších datových toků jako např. HDTV signálu ve studiové kvalitě napříč USA. Zabudované videoknihovny pro členy Internetu2

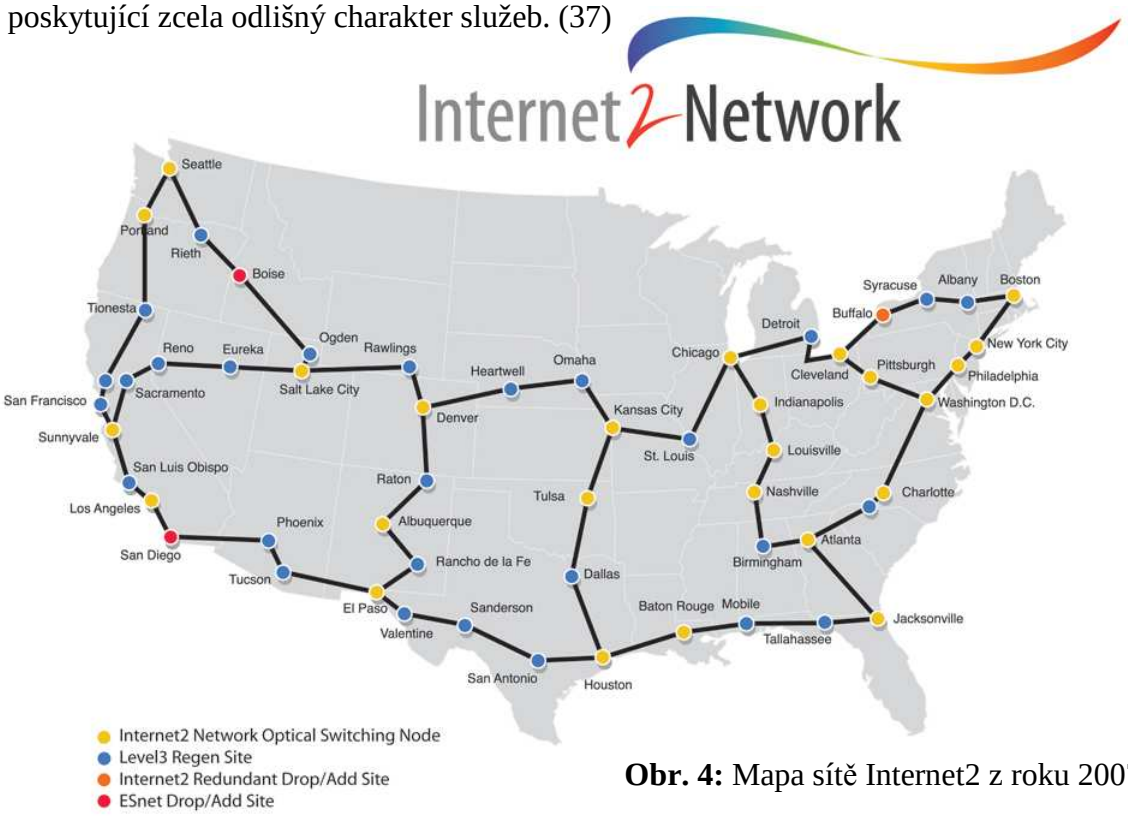
QBone – Poskytování služeb se zaručenou kvalitou. QBone zajišťuje testovací platformu pro jejich vývoj a nasazení.

Infrastruktura - Základem Internetu2 je vysokorychlostní páteřní síť, jejíž existence činí myslitelné další cíle projektu. Páteřní síť byla nazvána *Abilene* a pokrývá celé území USA ve dvou navzájem zálohujících se větvích. V akademických centrech jsou vybudovány přístupové body *gigaPoPs*, skrz které se připojují jednotliví členové. (24)

Sít Abilene, zahájila provoz v roce 1998 a budování skončilo o rok později. Představovala Internetovou páteř propojující univerzity a další instituce zapojené do projektu internet2. Původní rychlost byla 2,5 Gbit/s, ale později s rozvojem technologií přešla na 10 Gbit/s.

Přenosové trasy pro síť Internet2, poskytuje společnost Level 3 Communications, která provozuje také DWDM zařízení a zajišťuje tak pro Internet2

kompletní páteřní DWDM infrastrukturu. Na jejích jednotlivých trasách má Internet2 k dispozici 40 kanálů, jejichž řízení je plně v jeho moci. Aktuálně je oživeno vždy deset z nich, což při rychlosti 10 Gbit/s na kanál dává celkovou kapacitu páteře úctyhodných 100 Gbit/s. Toto DWDM jádro využívají pro svou činnost dvě logicky nezávislé sítě poskytující zcela odlišný charakter služeb. (37)



Obr. 4: Mapa sítě Internet2 z roku 2007

Spolupráce s Evropou – Internet2 spolupracuje s projekty evropských páteřních sítí. Řada pracovních skupin mají podobná zaměření a členové mezi sebou komunikují. Z technologického hlediska sítě Abilene a GÉANT jsou navzájem propojeny okruhem s odpovídajícími si parametry. Díky této spolupráci, mohou uživatelé plnohodnotně využívat služeb obou sítí. Oficiálně byly blízké vztahy obou projektů vyjádřeny podpisem dokumentu nazvaného *Memorandum of Understanding*.(24)

2.3.2 GEANT 2

První generace evropské páteřní akademické sítě GÉANT byla oficiálně uvedena do provozu 1. prosince 2001, propojila národní sítě pro vědu, výzkum a vzdělávání v Evropských zemích a zajistila jejich spojení s analogickými světovými sítěmi (především v Severní Americe a v Asii). Rozvoj sítě je podporován Evropskou unií v rámci 6. rámcového programu v podobě projektu *GN2 - Multi-Gigabit European*

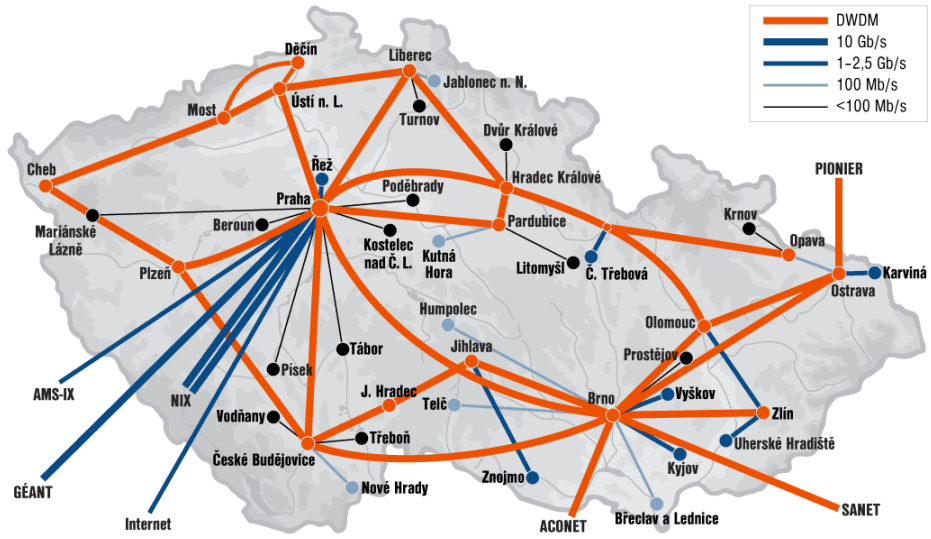
Academic Network, který byl oficiálně zahájen 1. září 2004. Je zaměřen především na další rozvoj evropské akademické páteřní sítě pod názvem GÉANT2. Doba jeho trvání byla stanovena na čtyři roky. Konkrétní cíle a vlastnosti sítě, která by měl být vybudována, jsou následující:

Hybridní síť - Nová generace sítě GÉANT by měla vedle klasické IP služby nabídnout i přepínání optický tras či vlnových délek.
Vysokorychlostní síť - Předpokládá se nárůst rychlosti jádra sítě ze stávajících 10 Gb/s na několikanásobek.
Služby s definovanou kvalitou - Síť by měla dokázat poskytovat i prioritní služby a služby s definovanou vyžadované některými náročnými aplikacemi.
Globální konektivita - Stávající mezikontinentální propojení většinou vzniká na základě dvoustranných dohod. Projekt GN2 bude usilovat o větší celosvětovou integraci sítí pro vědu, výzkum a vzdělávání a jejich intenzívnější spolupráci.
Mobilita uživatelů - V rámci projektu budou vyvinuty prostředky, které umožní uživatelům volný pohyb v síti a připojování k ní v různých lokalitách, aniž by vyžadovaly dodatečné administrativní kroky.
Výzkumný program - Vzhledem k velmi ambiciózním technickým cílům vyžaduje projekt intenzivní výzkumnou činnost. Především v oblasti integrace IP a optických služeb je řada dosud otevřených otázek a problémů, které je třeba vyřešit. (16)

Obr. 5: Topologie sítě GÉANT2

2.3.3 CESNET2

CESNET2 je národní vysokorychlostní síť určená pro vědu, výzkum, vývoj a vzdělávání. Páteřní síť propojuje největší univerzitní města ČR vysokorychlostními přenosovými okruhy. Uživateli jsou především vysoké školy, Akademie věd, ale i některé střední školy, knihovny a nemocnice. Těmto uživatelům, krom standardního připojení k internetu a velkých přenosových kapacit, nabízí také další pokrokové služby, jako jsou IP telefonie, videokonference či superpočítačové Metacentrum. (38)



Obr. 6: Topografie CESNET2 duben 2009

2.4 Struktura internetu

Internetu vzniknul spojením mnoha menších sítí. V každé této síti existuje jeden či více hlavních počítačů, na kterých se ukládají data či spouštějí aplikace, tyto počítače jsou nazvány servery. V Internetu se těmto počítačům říká Internet host (hostitelský PC) a přístup na něj bývá zpravidla otevřený pro všechny uživatele. Dalším typem počítačů připojených v síti jsou pracovní stanice, tedy klientské počítače, které jsou napojeny na svůj server. Uživateli je tak vcelku jedno, na kterém počítači pracuje, jelikož data a aplikace jsou uloženy na ústředním serveru.

2.4.1 Pojmy

Protokoly - Protokol je v informatice konvence nebo standard, podle kterého probíhá elektronická komunikace a přenos dat mezi dvěma koncovými body (realizované nejčastěji počítači).

TCP/IP – Přenosový a komunikační protokol, který se stal jedním z nejpoužívanějších standardů. Umožňuje kvalitní používání vrstev OSI – nejčastěji pracuje v třetí a čtvrté vrstvě OSI. Je použitelný v kabelážích typů X.25 a Ethernet. (1)

TCP – Transmission Control Protocol vytváří virtuální okruh mezi koncovými aplikacemi, tedy spolehlivý přenos dat.

IP - Internet Protocol je základní protokol síťové vrstvy a celého Internetu. Provádí vysílání datagramů na základě síťových IP adres obsažených v jejich záhlaví. Doručení datagramu není zaručeno, spolehlivost musí zajistit vyšší vrstvy (TCP, aplikace). (41)

FTP - File Transfer Protocol je v informatice protokol aplikační vrstvy z rodiny TCP/IP. Je určen pro přenos souborů mezi počítači, na kterých mohou běžet rozdílné operační systémy (je platformě nezávislý). Jeho podpora je součástí webových prohlížečů nebo specializovaných programů. (15)

Server – Řídící počítač lokální sítě (LAN). Server řídí předávání dat po síti a umožňuje stanicím zapojeným v síti přístup k datům a k periferiím, zapojeným v síti. Serverů může být v síti i více a mohou mít i specifické významy, jako je např. databázový server, tiskový server atd.

Klient - je v informatice aplikace nebo systém, který zpřístupňuje vzdálenou službu na jiném počítačovém systému, označovaném jako server. Nejčastěji se tak děje prostřednictvím počítačové sítě. (27)

DNS - (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. (14)

Doména nejvyššího řádu - (**TLD**, z anglického **Top Level Domain**) je internetová doména na nejvyšší úrovni stromu internetových domén. V doménovém jméně je doména nejvyšší úrovně uvedena na konci (např. u www.fbm.vutbr.cz je doménou nejvyššího řádu *.cz*). TLD popisuje základní skupinu doménových jmen, např. všechna doménová jména daného státu.

Některé domény nejvyššího řádu:

- .com – pro komerční organizace
- .net – pro organ. zajišťující provoz sítě
- .edu – pro vzdělávací instituce v USA
- .org – pro neziskové organizace
- .gov – pro vládu USA
- .mil – pro armádu USA

IRC, Chat - (Internet Realy Chat) Služba umožňující současnou konverzaci více uživatelů v reálném čase po internetu pomocí klávesnice svého počítače, tj. pomocí textu zobrazovaného na obrazovce.

IP Adresa - je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP protokol. V současné době je nejrozšířenější verze IPv4, která používá 32bitové adresy zapsané dekadicky po jednotlivých oktetech (osmicích bitů), například `192.168.0.1`. Z důvodu nedostatku IP adres bude nahrazen protokolem IPv6, který používá 128bitové IP adresy.

E-mail - (Electronic Mail) Elektronická pošta. Tato služba umožňuje uživatelům internetu vzájemnou výměnu nejrůznějších zpráv, které mohou obsahovat např. texty, grafiku, soubory, audio a video záznamy atd. Doručení takovéto zprávy trvá zpravidla několik minut.

URL - (Uniform Resource Locator) Adresa určité informace na internetu, která označuje přenosový protokol, adresu serveru, umístění souboru v adresářové struktuře, popř. další informace.

WWW - (World Wide Web) Nejvíce využívaná služba internetu založená na hypertextových dokumentech - www stránkách. Poskytuje virtuální informační prostor internetu, přístupný pomocí prohlížeče.

HTML - (Hyper Text Markup Language) Jazyk popisující strukturu www stránky

2.5 Netiketa

Netiketa, tento výraz vzniknul spojením dvou slov NET (síť) a ETIKETA, a vyjadřuje zásady či pravidla slušného chování na internetu. Tento soubor pravidel byl poprvé zformulován a vydán v roce 1995 organizací IETF. Termín „netiketa“ se používá od roku 1998 a má mnoho podob, pravidla jsou psaná i nepsaná, objektivní i subjektivní, ale žádná nejsou ta jediná dobrá.

Většina pravidel ale obsahuje následující body:

1. **Dávat si pozor na to, co píšete** – každý by si měl uvědomit, že když si s někým píše přes internet, tak by se měl chovat stejně, jako kdyby daný člověk byl právě před ním. A nespoléhat se na to, že jsme od sebe daleko a nebude to mít následky.
2. **Být maximálně taktní** – ve věcech týkající se náboženství, národností, politických názorů či sexuální orientace, bychom si měli uvědomit, že nevhodné vtipkování nebo narážky mohou v psané komunikaci vyznít sarkasticky až urážlivě.
3. **Být tolerantní k ostatním a přísnější k sobě** – každý dělá chyby, tak by bylo vhodné je odpouštět, nenadávejte a nevysmívejte se jim.
4. **Než se začnete ptát, přečtěte si FAQ** – na své otázky, si zkuste najít odpovědi sami, zkuste předchozí příspěvky, své otázky piště stručně a k věci, snažte se vyhýbat sporům a na urážky neodpovídat.
5. **Nerozesílat SPAM, reklamu, HOAX a řetězové dopisy** - každého tyto emaily jen obtěžují, tak proč to přeposílat dál, můžete odesílatele upozornit na nevhodnost obsahu, snad se příště poučí a také je nebude dále přeposílat.
6. **Nestahovat warez a neporušovat autorská práva –** asi by vám nebylo příjemné, kdybyste měli k něčemu autorská práva a někdo je porušoval, taky byste se bránili.
7. **Neposílat zbytečně velké soubory přes e-mail –** zkuste omezit posílání velkých souboru e-mailem (schránky nejsou neomezené), ale když už to je nutné, uvědomte majitele předem.
8. **Snažte se psát spisovně –** nepoužívejte zkratky, akronymy a smajlíky, když si nejste jistí, že jim adresát porozumí a nedojde k omylu.

Smyslem netikety je chránit uživatele Internetu před různými obtěžujícími a urážlivými projevy, respektive jim ukázat, jak se před nimi chránit vzájemně. Téměř každý z nás podvědomě tuší, co je „správné“ a co „špatné“. (21)

3 Internet a právo

3.1 Internet z právního hlediska

„Internet jako takový 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. **Objekty** práva jsou hmotné i nehmotné objekty, chování, resp. výsledky určitého chování apod. Z naznačených charakteristik internetu vyplývá jakási bezmocnost uchopit ho v rámci stávajícího 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.“ (32)

„Internet z právního hlediska jako subjekt neexistuje (nemá jako celek majitele), není upraven žádnými speciálními právními normami. Globální charakter Internetu je v přímém rozporu s národními či regionálními právními normami. Na Internetu však platí všechny obecně platné právní normy (občanský a obchodní zákoník, atd.), tj. lze uzavírat smluvní vztahy apod.

Internet má mnoho tváří: elektronická pošta, vydavatelství, knižní nakladatelství, reklamní nástěnka (WWW stránka), masový sdělovací prostředek, prostředí pro poskytování různých služeb. Nehmotné statky na Internetu jsou v zásadě chráněny podle autorského zákona.“ (39)

3.2 Charakteristika trestného činu a pachatele dle zákona

Jelikož internet je celosvětový a jako takový se nedá postihnout, postrádá i vlastní právní normy, tak uživatelé a provozovatelé se musí řídit zákony v dané zemi.

Dle zákona č. 140/1961 Sb., trestního zákona je:

§ 3 Trestný čin

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

§ 9 Pachatel a spolupachatel

(1) Pachatelem trestného činu je, kdo trestný čin spáchal sám.
(2) Byl-li trestný čin spáchán společným jednáním dvou nebo více osob, odpovídá každá z nich, jako by trestný čin spáchala sama (spolupachatelé).

§ 10 Účastník trestného činu

(1) Účastníkem na dokonaném trestném činu nebo jeho pokusu je, kdo úmyslně
a) spáchání trestného činu zosnoval nebo řídil (organizátor),
b) navedl jiného k spáchání trestného činu (návodce),
c) poskytl jinému pomoc k spáchání trestného činu, zejména opatřením prostředků, odstraněním překážek, radou, utvrzováním v předsevzetí, slibem přispět po trestném činu (pomocník).
(2) Na trestní odpovědnost a trestnost účastníka se užije ustanovení o trestní odpovědnosti a trestnosti pachatele, jestliže tento zákon nestanoví něco jiného.

Z teoretického hlediska můžeme rozdělit trestné činy následujícím způsobem:

1. trestné činy ve vztahu k počítači, jeho příslušenstvím a jiným nosičům informací jako věcem movitým (zejm. § 250 Trestního zákona)
2. trestné činy ve vztahu k datům, resp. uloženým informacím (zejm. § 257 a § 178 Trestního zákona)
3. trestné činy, při nichž je počítač prostředkem k jejich páchání (zejm. § 125 Trestního zákona)
4. trestné činy ve vztahu k programům jako autorským dílům (zejm. § 152 Trestního zákona a § 65-66 Autorského zákona)
   (28)

„Soudní znalec prof. Smejkal rozděluje počítačovou kriminalitu při určitém zjednodušení do dvou základních skupin:

1. delikty, kde počítač, program, data, informační systém apod. jsou nástrojem trestné činnosti pachatele,

2. 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. „(3)

3.3 Počítačové kriminální činy dle Rady Evropy

Členění počítačových kriminálních činů za účelem sjednocení legislativy v evropských zemích přijala Rada Evropy, jelikož tato trestná činnost má mezinárodní charakter a uvádí že:

Do seznamu trestných činu jsou zahrnovány (3):

- počítačové podvody,
- počítačové falzifikace,
- poškozování počítačových dat a programů,
- počítačová sabotáž,
- neoprávněný přístup,
- neoprávněný průnik,
- neoprávněné kopírování autorsky chráněného programu,
- neoprávněné kopírování fotografie.
- změna v datech nebo počítačových programech,
- počítačová špionáž,
- neoprávněné užívání počítače,
- neoprávněné užívání autorsky chráněného programu.

3.3.1 Srovnání těchto trestných činů s legislativou ČR

Rada Evropy	**Česká republika**
počítačové podvody	podvod - § 250, 250a
počítačové falzifikace	?
poškozování počítačových dat programů	poškození a zneužití a programů záznamu na nosiči informací (§ 257a Tr. Z.)
počítačová sabotáž	sabotáž - § 97, obecné ohrožení - § 179-180, poškozování cizí věci - § 257
neoprávněný přístup	neoprávněné užívání cizí věci-§ 249
neoprávněný průnik	neoprávněné užívání cizí věci-§ 249 (?)
Neoprávněné kopírování autorsky chráněného programu	porušování autorského práva - § 152
neoprávněné kopírování fotografie	porušování autorského práva - § 152
změna v datech nebo počítačových programech	poškození a zneužití záznamu na nosiči informací (§ 257a Tr. Z.), zkreslování údajů hospodářské a obchodní evidence - § 125 (?)

počítačová špionáž	vyzvědačství- § 105, ohrožení státního tajemství – § 106, ohrožení hospodářského tajemství - § 122, ohrožení služebního tajemství - § 173
neoprávněné užívání počítače	neoprávněné užívání cizí věci-§ 249
neoprávněné užívání autorsky chráněného programu	porušování autorského práva - § 152

Tab. 1: Srovnáni legislativy u nás a v Evropě (2)

4 Trestné činy na internetu

4.1 Pachatelé

„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).

Někteří pachatelé provádějí 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.“ (32)

4.1.1 Hackeři

„Hackeři jsou počítačoví specialisté či programátoři s detailními znalostmi fungování systému, dokážou ho výborně používat, ale především si ho i upravit podle svých potřeb. V masmédiích se však tento termín začal mylně používat pro počítačové zločince a narušitele počítačových sítí, kteří se správně označují termínem *cracker*. Dnes jsou oba pojmy často nesprávně zaměňovány a jako pojem blízký původnímu významu se používají také termíny *geek*, *guru*, *nerd*.

V užším významu se slovo hacker používá ve významu **průnikář**, tedy osoba, která svoji odbornou převahu používá k průniku do systému nebo obecně k získání většího vlivu, než jaký měla předtím. Takoví hackeři své znalosti tají nebo si je vyměňují jen mezi sebou.“ (17)

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. 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.

4.1.2 Crackeři

„Označení **cracker** 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** je činnost, kdy dojde k narušení informačního systému zvenčí (prolomení ochrany). Cracker zpravidla nepracuje sám, ale ve skupinách. Členové skupiny bývají hierarchicky rozděleni, každý má na starosti konkrétní činnost. Skupiny bývají tematicky specializované na herní oblasti, weby a aplikace. Mezi skupinami panuje poměrně vysoká soutěživost, své úspěchy pečlivě dokumentují a zpravidla i zpřístupňují na internetu. 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. 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 dokážou 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,

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,

knacker – útočníci, který odstraňují ochranný kód programů za účelem jeho volného používání,

looser/lamer – uživatelé neznalí prostředí IT.

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“ (32)

Dalšími, kdo páchají trestnou činnost, ať už si to uvědomují nebo ne jsou uživatelé internetu, kteří stahují hudbu, filmy a software z různých serverů, ale o to budeme rozebírat v jiné kapitole.

4.2 Způsoby napadání

4.2.1 Virus

Mezi asi nejznámější způsoby, kterým může být počítač, či jiné stanice napadeny jsou viry

„Počítačové viry jsou malé softwarové programy určené k šíření z jednoho počítače do jiného a narušování fungování počítače. Virus může poškodit nebo odstranit data v počítači, využít vaši emailovou aplikaci k vlastnímu rozšíření do jiných počítačů, nebo dokonce vymazat všechna data na pevném disku.

Viry se nejsnadněji šíří v přílohách e-mailových zpráv nebo rychlých zpráv. Proto je důležité nikdy neotevírat přílohy e-mailů, pokud neznáte odesílatele a neočekáváte je. Viry mohou být zamaskovány jako přílohy v podobě zábavných obrázků, přání či zvukových souborů a videosouborů. Šíří se také stahováním z Internetu. Mohou být skryty v nelegálním softwaru a dalších souborech či programech, které můžete stáhnout.“ (29)

Je několik důvodů vzniku virů:

- „Vytvářejí je programátoři velkých softwarových firem, kteří byli propuštěni ze zaměstnání. Ti se svým zaměstnavatelům pomstí vytvořením nějakého viru a jeho vpuštěním do jejich lokální (firemní) sítě, aby zničili nebo poškodili firmu.
- Vytvářejí je mladí programátoři, kteří si chtějí vyzkoušet své schopnosti. Pokud se takové viry rozšíří, může to být důsledek chyby nebo neuvědomění si celkového dopadu svojí činnosti.
- (málo pravděpodobná verze) Viry vytvářejí programátoři softwarových firem, které vytvářejí antivirové programy, za účelem zvýšení prodeje svých výrobků.
- Viry jsou jednou z cest, jak ovládnout a řídit větší množství počítačů a využívat je např. k rozesílání spamu.
- Jsou prostředkem, jak zdiskreditovat platformu, která není schopna sama sebe uchránit před jejich šířením.“ (35)

4.2.2 Červ

„Červ je stejně jako virus formován tak, aby kopíroval sám sebe z jednoho počítače do jiného, ale činí tak automaticky. Nejprve převezme kontrolu nad funkcemi v počítači, které mohou přenášet soubory nebo informace. Jakmile se červ ocitne v systému, může se přenášet samostatně.

Vysokým nebezpečím červů je jejich schopnost replikace ve velkých objemech. Červ může například rozesílat kopie sebe sama všem členům vašeho e-mailového adresáře, jejichž počítače poté provedou to stejné, což způsobí domino efekt nebo rozsáhlý síťový přenos, který může zpomalit pracovní sítě i Internet jako celek. Pokud se noví červi uvolní, velmi rychle se šíří. Zahlcují sítě a mohou způsobit, že vám (i komukoli jinému) bude dlouho trvat zobrazování webových stránek na Internetu.

Vzhledem k tomu, že se červi nemusejí šířit prostřednictvím hostitelského programu nebo souboru, mohou také proniknout do vašeho systému a umožnit převzetí vzdálené kontroly nad vaším počítačem jinému uživateli.“ (30)

4.2.3 Trojský kůň

„Stejně jako byl mytologický Trojský kůň zdánlivým darem, z něhož později vyskočili řečtí vojáci, kteří se zmocnili Tróji, jsou dnešní trojští koně počítačové programy, které se jeví jako užitečný software, ale místo toho naruší vaše zabezpečení a napáchají spousty škod.

Trojští koně se šíří tím, že jsou uživatelé zlákáni k otevření programu, protože si myslí, že pochází z legitimního zdroje. Trojský kůň může být rovněž součástí softwaru, který stáhnete zdarma.“ (30)

4.2.4 Spyware

„Spyware, neboli česky špión, je prográmek který se uhnízdí na Vašem PC a dokonale špehuje a krade Vaše hesla, historii navštívených stránek, čísla kreditních karet, mění Vaše úvodní stránky na internetu a podobné hanebnosti. Vše, co vyslídí, pak zasílá určitému uživateli, který dále zpracovává všechny údaje, které jsou samozřejmě velmi jednoduše zneužitelné. Jedná se o velice nebezpečné programy, které se stále více a více rozmáhají. Většinu těchto špiónů "dostanete" při surfování na internetu (hlavně warez a porno stránky), či instalací pochybného software.“ (13)

Spyware rozdělujeme do několika skupin:

Adware - Spyware, které Vás většinou obtěžuje při surfování na internetu reklamou (pop-up okna, apod.)

Browser helper object - DLL knihovna, která umožňuje programátorům změnit a sledovat nastavení Internet Exploreru.

Hijacker - Spyware, které dokáže měnit domovskou stránku.

Dialery - Spyware, které přesměrovává telefonní linku na drahé telefonní tarify (tzv. Žluté linky).

Keystroke Logger (Keylogger) - Spyware, které sledují každé zmáčknutí klávesy Vaší klávesnice, toto pak ukládají do určitého souboru, který poté pošlou svému autorovi, či třetí osobě.

Malware - Všechny programy, které jsou vytvářeny s cílem, nějakým způsobem poškodit uživatele počítače, na kterém jsou bez jeho vědomí nainstalovány.

Miscellaneous - Spyware, které je mixem skupin spyware. Obsahuje od každého něco.

Remote Administration Tools (RAT) - Spyware, které umožní vzdálenému uživateli ovládat Vaše PC.

4.2.5 Phishing

Phishing (česky „rhybaření“) je druh internetového podvodu, kterým se podvodníci pomocí falešných e-mailů snaží z uživatelů internetového bankovnictví vylákat přístupové údaje k účtům, či jiným internetovým aplikacím a zneužít je pro svoje obohacení.

Základní znaky phishingového e-mailu:

- Snaží se vyvolat dojem, že byl odeslán organizací, z jejichž klientů se snaží vylákat důvěrné informace. Toho se snaží docílit grafickou podobou e-mailu a zfalšováním adresy odesílatele.

- Text může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu či platební karty, výzkum klientské spokojenosti nebo jako elektronický bulletin pro klienty.
- V textu zprávy je link, který na první pohled většinou vypadá, že směřuje na stránky organizace (banky). Při jeho bližším prozkoumání zjistíte, že ve skutečnosti odkazuje na jiné místo, kde jsou umístěné podvodné stránky.
- Formulář vybízí k vyplnění důvěrných informací, které by banka neměla požadovat.
- V adresním řádku prohlížeče se zobrazuje adresa, která nepatří organizaci, jejichž stránky se snaží napodobit. Uvedená adresa se může snažit originální napodobit, ale vždy bude jiná, případně může začínat číselným kódem IP adresy. Vyskytují se i případy, kdy se podvodníci snaží tuto skutečnost maskovat.
- Ve většině případů komunikace probíhá po běžném, nezabezpečeném protokolu (adresa začíná http://).

4.2.5.1 Proč se tento druh podvodu nazývá phishing?

„O původu slova jsou dvě teorie. Jedna tvrdí, že vzniklo undergroundovou úpravou slova fishing - rybaření , kdy "f" bylo zaměněno za dvojici písmen "ph". Druhá předpokládá, že jde o zkratku: **p**assword **h**arvesting f**ishing** - sběr hesel rybařením. V češtině se začal používat výraz "rhybaření". Postup podvodníků připomíná rybaření. Rozešlou e-maily na mnoho náhodných adres (jako když rybáři hodí sítě do vody) a čekají, kdo se nachytá a sdělí důvěrné informace.“ (9)

4.2.5.2 První útok na české klienty

První útok na české klienty se objevil v březnu 2006 a napadenou bankou byla CITIBANK. Znění celého podvodného e-mailu je součástí přílohy, zde jen provedeme analýzu podvodu:

1) V podvodné zprávě je využito sociální inženýrství, kdy je uživateli vysvětleno, aby se vyhnul případným problémům při použití bankomatu, je dobré bance sdělit určité údaje. Přestože je tato žádost nesmyslná, vyplývá z různých statistik, že až 5% oslovených uživatelů své údaje vyplní.

2) V e-mailu je uveden link, na který se má kliknout a tím by měl uživatel vstoupit na stránku banky. Přestože text odkazu v e-mailu vypadá, že uživatel bude přesměrován na server banky, skutečné přesměrování bude provedeno na jiné místo.

3) Odkaz v e-mailu přesměruje na stránku podvodníků udělanou ve stejném stylu, jako je originální stránka banky a proto nepozorný návštěvník si ani nemusí uvědomit, že je na cizím serveru. Po uživateli je požadováno, aby ve formuláři vyplnil důvěrné informace o jeho platební kartě. Pak už by podvodníkům nebránilo nic v její zneužití. (6)

Podvod je velice jednoduchý, spoléhá na neznalost lidí v oblasti těchto podvodů a přehlédnutí jistých detailů. Bohužel dle statistik přece jen dost lidí se nechá nachytat na tyto podvodné emaily a jejich údaje jsou posléze zneužity. Ale myslím si, že v dnešní době povědomost lidí roste a přece jen jsou opatrnější, kam zadávají své citlivé data.

V příloze je přesné znění phishingového emailu a obrázek podvodné stránky.

4.2.6 Pharming

„Další z podvodných technik provozovaných na internetu k získávání citlivých údajů je Pharming. Principem této techniky je napadení DNS a přepsání IP adresy, čímž útočník způsobí přesměrování klienta na falešné stránky internetbankingu po napsání adresy dané banky do webového prohlížeče. Tyto stránky jsou detailně napodobené a běžný uživatel je nemá šanci rozeznat. Tento způsob podvodu na rozdíl od phishingu je důmyslněji propracován, proto je mnohem nebezpečnější a zákeřnější než předešlý podvod, jelikož uživatel o tom nebude nijak informován, a tak se tento čin odehraje bez jeho účasti na vědomí.“ (33)

Jak předcházet pharming útoku:

- „Zkontrolujte adresu URL každého webu, který požaduje identifikační údaje. Přesvědčte se, zda vaše relace začíná na známé pravé adrese webového serveru a nejsou k ní přidány žádné další znaky.
- Udržujte účinnou a aktuální antivirovou ochranu.

- Používejte důvěryhodného a uznávaného poskytovatele služeb Internetu. Nekompromisní zabezpečení na úrovni poskytovatele služeb Internetu je vaší první linií obrany proti pharmingu.
- Kontrolujte certifikáty. K ověření toho, zda vstupujete na legální web, stačí pouze několik sekund.
- Potřebujete-li vstoupit na citlivý web, nikdy neklepejte přímo na odkaz v e-mailu nebo na webové stránce. Text odkazu vždy vyjměte a vložte do nového okna prohlížeče nebo použijte vaše záložky.“ (34)

4.2.7 SPAM

Označením spam se značí masově rozesílané nevyžádané sdělení (většinou reklamní), původně se tento výraz používal jen pro nevyžádané reklamní e-maily, ale postupem času se jev projevil i v dalších druzích internetové komunikace – diskuzní fóra, komentáře, ICQ, atd.

4.2.7.1 Původ slova SPAM

„Název pochází ze značky amerických konzerv lančmítu, která se vyrábí od 30. let dodnes (v současnosti ale výrobce trvá na psaní velkým písmem **SPAM**). Za 2. světové války a po ní byla hojně rozšířená a stále méně oblíbená ve Velké Británii. Proto se objevuje v závěrečné skeči 25. dílu seriálu „Monty Pythonův létající cirkus“, kde všechny položky jídelního lístku v restauraci obsahují **spam**, i mnohokrát opakovaně. Spory zákazníků s číšnicí o objednávky přerušuje skupina Vikingů zpívajících „**Spam, spam, spam…**“

Označení tak bylo přijato nejprve pro praktiku mnohonásobného rozesílání téže zprávy na Usenetu, ale později se význam slova rozšířil o zneužívání skupin k šíření různých nepřípadných textů a přímo reklamy. Zachoval se i poté, co se těžiště takových aktivit přesunulo do e-mailu.“ (7)

4.2.7.2 Zákony proti SPAMU:

„Od 7. září 2004 začal platit nový **Zákon o některých službách informační společnosti** (č. 480/2004), který problematiku spamu upravuje a vyžaduje prokazatelný souhlas příjemce zprávy. Dohledem nad dodržování zákona byl pověřen **Úřad pro ochranu osobních údajů**. Zákon byl vytvořen podle norem Evropské unie. Spam

definuje jako obchodní sdělení, což jsou všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby. Zákon řeší nejen internetový spam, ale také jiné formy elektronické komunikace (SMS, telemarketing). „ (7)

Přesné znění změněného zákona č. 138/2002 Sb., o regulaci reklamy v § 2 odst. 1 písmeno e) včetně poznámky pod čarou č. 5a) zní:

"e) šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje; na šíření reklamy elektronickými prostředky a jeho omezení se vztahuje zvláštní právní předpis, 5a) za reklamu, která obtěžuje, se považuje reklama směřující ke konkrétnímu adresátovi za podmínky, že adresát dal předem jasně a srozumitelně najevo, že si nepřeje, aby vůči němu byla nevyžádaná reklama šířena. 5a) § 7 zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)."

4.2.7.3 Legální spam??

Toto označení by se dalo použít pro e-maily, které nám chodí do schránek po „vlastní“ žádosti. Po registraci na několika stránkách, e-shopy, diskusní fóra, cestovní agentury apod. se Vás na každé této stránce zeptají, jestli například chcete být informováni o novinkách, akcích, slevách… Člověku to ani nepřijde, ale najednou mu denně začne chodit několik (i desítek) „vyžádaných“ emailových zpráv. A jelikož jsou internetové firmy rozmístěny po celém světě, tak jsou i rozdílné zákony o šíření emailové databáze, a tudíž i tyto informační maily Vám budou chodit z jiných firem. Rozdíl od nevyžádaných spamů je v tom, že zasílání těchto informativních emailů by se mělo dát bez problému zrušit.

Neexistuje žádný univerzální způsob jak se již příchozích spamů jednou pro vždy zbavit, lze sice nastavit filtrování pošty dle určitých parametrů, ale ani to není stoprocentní ochrana. Snad jedinou účinnou obranou proti této nevyžádané poště je založení nového emailového účtu a posléze si dobře rozmyslet, kam tento email budeme dávat, nevýhodou je ztráta dosavadního adresáře a nové přeposílání všem změnu emailové adresy.

Dalším možným řešením je používáním několika různých emailových účtů, a následné používání dle důvěryhodnosti. Například jeden pro práci a komunikaci se zaměstnanci, další svůj osobní email, pro komunikaci s přáteli a rodinou a ten poslední pro ostatní účely, registraci do diskusních fór, aktivační emaily, a také pro zveřejnění na veřejnosti.

4.2.8 HOAX

Tímto výrazem z angličtiny vyjadřujeme nějakou poplašnou, falešnou či jinou podvodnou zprávu za účelem vytvoření zmatku či rozruchu ve společnosti. V počítačové oblasti to je nejčastěji „varování“ před neexistujícím virem, který většinou má napáchat velkou škodu či jinak ublížit uživateli a zároveň ho vyzývá k dalšímu rozesílání. Snad každého obtěžuje, když mu někdo na email či jinam pošle zprávu, která na konci obsahuje text smyslu „přepošlete ji několika dalším lidem, nebo se vám něco nesplní…budete mít roky smůlu…nepotkáte lásku, atd.“

Typický text poplašné zprávy obsahuje většinou tyto body:

- **Popis nebezpečí (viru)** - Smyšlené nebezpečí (vir) bývá stručně popsané.
- **Ničivé účinky viru** - Zde záleží převážně na autorově fantazii. Ničivé účinky mohou být celkem obyčejné, třeba zformátování disku nebo už míň důvěryhodné - zběsilý útěk myši do ledničky, roztočení HDD opačným směrem, výbuch počítače…
- **Důvěryhodné zdroje varují** - Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů ("IBM a FBI varují" nebo "Microsoft upozorňuje" atd.)
- **Výzva k dalšímu rozeslání** - Tento bod HOAX vždy obsahuje! Mnoho nezkušených uživatelů se nechá zprávou napálit a bez přemýšlení výzvu uposlechnou. Právě proto se tyto nesmysly lavinovitě šíří.

Klasické HOAXy můžeme rozdělit následně:

- Varování před smyšlenými viry a různými útoky na počítač nebo popis jiného nereálného nebezpečí
- Falešné prosby o pomoc, petice a výzvy
- Fámy o mobilních telefonech
- Pyramidové hry a různé nabídky na snadné výdělky či podvodné loterie

- Řetězové dopisy štěstí
- Žertovné zprávy

(8)

4.2.8.1 Čím HOAX škodí a proč je nebezpečný

Může se zdát, že HOAX nemůže být ničím škodlivý, ale opak je pravdou, jestliže chodí několikrát denně každému obdobné zprávy, tak to příjemce **obtěžuje** (stejně jako spamy) a zároveň **zatěžuje linky a servery** společností, v dnešní době tvoří spam přes 90% emailové komunikace, tak proč ho ještě podporovat dalšími zbytečnými HOAXy. Velké množství HOAXů rozesílají uživatelé způsobem předat dál a na všechny adresy. Tím dochází k postupnému přidávání adres k textu zprávy a samozřejmě narůstá velikost zprávy. Jestliže se tyto zprávy šíří daným způsobem, tak **dává k dispozici obrovský seznam emailových adres, čímž je vlastně rájem pro spamery**.

Dalším problém by mohl nastat, kdyby se například Váš seznam adres klientů a obchodních partnerů dostal ke konkurenci. A v případě falešných petic a podpisových akcí se můžou dostat **citlivé údaje** (jméno, adresa a rodné číslo) **do rukou lidí, kteří toho zneužijí**.

Tyto zprávy **můžou přímo poškodit určitou osobu nebo společnost**. V případě rozesílání zpráv, obsahujících úplné kontakty, konkrétní čísla, adresu, či další údaje, tak jsou pak dané údaje prakticky nepoužitelné (v případě telefonu a emailu, jsou přetížené). Polopravdy, falešné informace či jiné poplašné zprávy mohou poškodit dobré jméno společnosti a tím způsobit finanční i společenskou újmu.

Rozesíláním HOAXů jistě **nezvyšujete důvěryhodnost společnosti či úřadu** pro své obchodní partnery a klienty. Zásadní chybou může být i přeposílání HOAXů s automatickým podpisem (jméno, kontakt, telefon). Takto odeslaná zpráva z Vás dělá autora a případné následky může nést tato podepsaná osoba.

Na HOAX se dá reagovat jediným způsobem: Nepřeposílat dál, dříve než se ujistíme, že je tato zpráva opravdová a potvrzená. Stačí se podívat ve vyhledávači např. www.google.com, jedná-li se o HOAX, jistě naleznete na internetu obdobný text. (11)

4.2.9 Cybersquatting

Cybersquatting neboli doménové spekulantství, je v podstatě registrace domény shodné nebo podobné s obchodní firmou či ochrannou známkou za účelem finančního prospěchu či konkurenčního boje. Tato doména nemusí být vůbec majitelem využívána, jelikož mu stačí, když ji posléze za nemalou částku prodá té firmě, kterou „poškozoval“.

4.2.9.1 Zloději domén u nás a ve světě

V posledních letech touto formou parazituje na pověsti známých firem stále více spekulantů. Stěžují si nejen společnosti z oblasti farmacie, bankovnictví či maloobchodu. Obětí cybersquattingu se stávají i celebrity. Možná právě proto nejvíce stížností pochází z USA.

U nás je známým případem spor o doménu ceskapojistovna.cz. Česká pojišťovna má na tento název ochrannou známku, nebylo tedy možné, aby jej používal ještě někdo jiný. Soud dal pojišťovně samozřejmě za pravdu.

4.2.9.2 Zákon a cybersquatting

„Spekulanti se svým jednáním dopouštějí několika porušení právních povinností. Jejich jednání tak často představuje:

a) porušení práv k obchodní firmě (§ 12 obchodního zákoníku);
b) porušení práv k ochranné známce (§ 8 zákona o ochranných známkách);
c) vyvolání nebezpečí záměny (§ 47 obchodního zákoníku);
d) parazitování na pověsti (§ 48 obchodního zákoníku);

V určitých závažnějších případech může dojít k naplnění některých podstat trestných činů jako např. dle § 150 trestního zákona - porušování práv k ochranné známce, obchodnímu jménu.“ (25)

4.2.9.3 Cybersquatting má v praxi několik podob

- **cybersquatting v užším slova smyslu** – registrace domény shodné či podobné s obchodní firmou či ochrannou známkou jiné osoby.;
- **domain grabbing** – jde o hromadnou registraci shodných či zaměnitelných domén s tzn. blokačním úmyslem;

- **typosquatting** – jedná se o registraci zaměnitelné domény s tím, že spekulant spoléhá na překlepy uživatelů internetu. Jako příklad lze uvést www.gogle.cz nebo www.seynam.cz ;
- **trademark infrigement** – jde o cílenou spekulativní registraci doménových jmen shodných a zaměnitelných s názvem ochranné známky;
- **plánovaný či předběžný cybersquatting** – jedná se předvídání určité skutečnosti, kdy spekulant spoléhá na to, že dojde k určité skutečnosti a pak bude z této situace těžit. (25)

V dnešní době se cena za registraci domény pohybuje od několika stovek do pár tisíc korun, tak spekulanti mají docela otevřenou možnost tuto činnost dále provozovat. I když někteří po jednom ročním období, co tuto doménu vlastní zjistí, že jim to moc nevydělává a jsou ochotni prodat za docela směšné částky, aby aspoň něco vydělali.

4.3 Kopírování, stahování a sdílení autorských děl

4.3.1 Co je legální a co nelegální

Kolem stahování hudby, filmů a programů se všude šíří mnoho falešných informací, polopravd a omylů, tak se budu snažit trochu přiblížit, co je vůbec legální a co legální není. V českém právu užívání a kopírování hudby, filmů a software řeší **zákon č. 121/2000 Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)**.

4.3.2 Filmy a hudba

Legální je pořizovat si kopie filmů či hudby, ale spoustu věcí si musíme pohlídat. V § 30 (Volná užití) autorský zákon stanoví, že je v pořádku pořizovat si záznamy, kopie či napodobeniny čehokoli, pokud se tak bude dít pro vlastní, soukromou potřebu nabyvatele a pokud mu to nepřinese nějaké peníze či jiné hmotné „výhody“. Ale jsou zde také uvedeny výjimky, kdy takové jednání v pořádku není.

Hlavně je zde uvedeno, že tato věta, o pořizování záznamech a kopiích, neplatí pro počítačové programy. Dále je zde uvedeno, že se nesmí pořizovat „záznam audiovizuálního díla při jeho provozování ze záznamu nebo při přenosu“, vlastními slovy to znamená, že se třeba nemůžete vypravit do kina s kamerou, a v pohodě ho celý

natočit aniž by se tím porušil zákon. Ale v případě živého koncertu, či představení již záznam pořídit smíte, pokud Vám to pořadatel výslovně nezakáže.

Další věcí, na kterou je třeba si dát pozor, je spojení „ pro soukromou potřebu“. Zákon nedefinuje přesně, co to vlastně je, a právní výklady se v praxi liší. Shodují se, že je v pořádku, pokud si takto pořízenou kopii pustíte někde sami pro sebe, tak by v tom neměl být žádný problém, ale už je sporné, zda tuto stejnou kopii můžete pouštět i jiným osobám, či jim je půjčovat, nebo dokonce dále kopírovat – přepalovat. Obecně tedy platí, že: Na tyto filmy a hudbu se vztahují stejná pravidla, jako na písničky nahrané z rádia či filmy z televize.

V zákoně je také ale napsáno, že je zakázáno obcházet „účinné technické prostředky ochrany“. Ovšem opět nikde není přesně definováno, co to účinný prostředek vlastně je. Prozatím nám zbývá jediné, řídit se vlastním rozumem a raději neprolamovat různé ochrany proti kopírování, ale pořídíme-li si kopii, kde tato ochrana již není, tak nic v tomhle smyslu zákona neporušujeme.

Důležité je mít na paměti, že zákon sice dovoluje pořizovat si kopie CD nebo filmů, a je legální si je stahovat z internetu nebo přepalovat od známých, ale už nedovoluje jiným, aby Vám kopírování, stahování či přepalování umožnili. Je trestným činem, vystavit (zdarma, natož za poplatek) filmy nebo hudební záznamy ke stáhnutí z internetu.

4.3.3 Software

Jak už jsem zmínil na předchozí stránce, je sice legální pořizovat si kopie hudby a filmů, ale to se netýká softwarových programů.

Tedy abych to upřesnil, dle autorského zákona smí „oprávněný uživatel“ (v § 66 odst. 6 je „osoba, která má vlastnické či jiné právo k rozmnožení tohoto programu; dále oprávněný nabyvatel licence nebo osoba oprávněná program užívat“) pořizovat „záložní rozmnoženinu nezbytnou pro užívání programu“. O co to tedy jde, neznamená to, že když si koupíte originální CD s drahým softwarem, můžete ho dle libosti přepalovat dál a Vaše „originálka“ bude někde v šuplíku v bezpečí a bez hrozby jakékoli újmy. V zákoně je totiž psáno, že „záložní rozmnoženinou“ se rozumí instalace programu do počítače. Z toho tedy plyne, že oprávněný uživatel si smí legálně nainstalovat program do počítače, ale jen tehdy, je-li to nezbytné k jeho spuštění.

Jednoduše řečeno, nejste-li oprávněný uživatel softwaru, tak s ním nemůžete dělat vůbec nic.

Každý softwarový pirát se dopouští trestného činu porušování autorských práv podle § 152 trestního zákona. V případě že celková škoda, nedosáhne půl milionu, hrozí mu vězení maximálně na 2 roky, většinou to znamená, že pachatel dostane podmínku, pokutu a zabaví mu počítač. V opačném případě, že škoda je větší než půl milionu, pohybuje se sazba od půl roku do 5 let vězení, krom možnosti udělení pokuty, opět zabavení počítače a náhradu soudních výloh a finanční kompenzaci poškozeným softwarovým firmám.

4.3.3.1 Jak nelegální šíření poškozuje majitele autorských práv a společnost – Pirátství

Podle zdrojů české protipirátské unie se „pirátstvím rozumí jakékoliv neoprávněné užití autorského díla a ostatních předmětů ochrany podle práv souvisejících s právem autorským takovým způsobem, který přísluší pouze nositelům práv k těmto dílům a ostatním předmětům. Pirátství je parazitování na duševním vlastnictví někoho jiného.

V České republice se často se setkáváme s názorem veřejnosti, že pirátství je problém pouze úzké skupiny subjektů - nositelů práv k dílům, které jsou neoprávněně užívány. Tento názor však značně nepřesný a nezohledňuje většinu aspektů pirátství. Poškozeným je nejen přímý nositel práva k předmětnému dílu či jinému předmětu, ale také další subjekty. Zřejmým je poškozování všech subjektů v určitém odvětví, neboť pirát je pro ně nekalou konkurencí, která nabízí stejné nebo podobné zboží za nižší cenu, neboť nemá náklady na pořízení práv k užití. Přesto však má pirát z každého případu větší zisky než legální podnikatel.

Pirátskými aktivitami je poškozována celá společnost. Černý trh snižuje legální zisky, ze kterých jsou odváděny daně, přitom zisky z tohoto nelegálního podnikání jsou nemalé. Poškozeným je samozřejmě i spotřebitel, který dostává za cenu podobnou originálnímu výrobku nekvalitní produkt bez možnosti reklamace.

V oblasti filmového průmyslu má pirátství i další negativní dopady. Komerční pirátství totiž poškozuje nejen nositele práv a subjekty, které se podílejí na exploataci filmů, ale také film samotný. Pirátství narušuje trh jako takový; piráti se soustředí zejména na

tituly, které si najdou širokou diváckou obec, a tyto potom nabízejí za cenu, které nemůže legální distributor dosáhnout. Cena je však pro mnoho diváků určující.“ (10)

4.3.4 Ne/Legální stahování

Jak už jsme se dověděli v předešlém textu, není nelegální stahovat filmy a hudbu, ale je nelegální stahovat software, tedy pokud to není freeware (zdarma a volně k šíření bez poplatku), shareware (na zkoušku, časově omezený) nebo Public domain (software, se kterým si můžete dělat úplně všechno). A tyto softwary je doporučeno stahovat buď z oficiálních stránek výrobce, nebo z prověřených portálů, např. www.slunecnice.cz, www.stahuj.cz, kteří ručí za to, že stahujete legálně a že si do počítače nestáhnete různou havěť ve formě viru, či jiného nebezpečného prográmku. Co se týká hudby a filmů, jsou na internetu portály, které se specializují na legální stahování a pořizování hudby a filmů. U hudby to je například www.i-legalne.cz, kde si za poplatek stáhnete album či určitou skladbu ve formátu mp3 do počítače. U filmů to spíš znamená „půjčení“ filmu, za poplatek si stáhnete do počítače určitý film, ale na ten můžete podívat jen po omezenou dobu např. jednoho měsíce.

4.3.5 Způsoby nelegálního stahování

Nelegální stahování jako takové, jak už jsme si řekli, existuje pouze u softwaru, který podléhá autorskému zákonu. A většinou se odehrává uživatelem, který si najde odkaz na stažení na určitém fóru, a ten se odkazuje na portály a servery, které umožňují legální sdílení souborů, ty které bychom mohli sdílet, např. vlastní hudební tvorbu, vlastní fotky, apod. Vlastníci takových to serverů mají povinnost kontrolovat uložené data a všechen warez (označení nelegálně stahovaných děl podléhajícím autorským právům), vymazat ze svého serveru, ale nezodpovídají za takto uložený obsah. Příklad portálů: www.leteckaposta.cz, http://uloz.to, www.rapidshare.com.

4.3.6 Nelegální sdílení

Sdílení jako takové není nelegální, sdílet můžete vlastní data, například, fotky, soubory a další, které nepodléhají autorskému zákonu. Ale bohužel většina sdílených souborů n a internetu je warez. Ten kdo sdílí filmy, hudbu a software se dopouští trestného činu dle § 152 trestního zákona – „Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi“. A hrozí mu až 5 let vězení

4.3.7 Způsoby nelegálního stahování

Převážnou většinou nelegálního sdílení warezu tvoří tzv. P2P programy,torrenty a samozřejmě nelegální sdílení warezu na veřejně dostupných internetových portálech.

P2P programy – Peer-to-peer sítě tvoří architekturu, kdy spolu komunikují přímo klientské stanice. Přes tyto programy uživatelé nejen komunikují, ale právě velkou část obsahu sdílení těchto sítí tvoří warez, což je v rozporu se zákonem. Nejznámějším P2P programem je asi DC++.

Torrenty – jsou součástí P2P sítí, při distribuci pomocí BitTorrentu jsou soubory (může jich být víc) rozděleny klientem na menší bloky (jejich velikost resp. počet lze nastavit, obvykle mají okolo 250kB). Principem torrent klientů je, že zároveň Vámi stahovaný soubor okamžitě sdílíte pro ostatní, tudíž čím více je lidí, co sdílí/stahují stejný soubor, tím je rychlost stahování větší. Opět při sdílení warezu, je v rozporu se zákonem.

5 Instituce a orgány zabývající se potlačením počítačové kriminality

Vzhledem k tomu, že činnosti týkající se internetové kriminality stále rostou, a jsou mezinárodního charakteru, tak jako internet, jsou určité organizace, které bojují s touto činností, ve většině případů se jedná o softwarové pirátství a porušování autorských práv, se zaměřením na nelegální sdílení audiovizuálních děl a skladeb. Nejznámější organizacemi, kterými se budu zabývat, jsou: Business Software Aliance (BSA), Česká protipirátská unie (ČPU), International Federation of the Phonographic Industry (IFPI) a v neposledním případě to je spolupráce s Policií ČR.

5.1 Business Software Alliance (BSA)

O ochranu autorských práv a potlačení softwarového pirátství se snaží světová organizace Business Software Alliance (BSA), která byla založena v r. 1988 v USA. V České republice působí od r. 1993 partnerská firma BSA CS v Praze, která vznikla jako lokální sdružení pro Čechy. Sdružuje významné výrobce software v ČR - Microsoft, Software 602, Autodesk, APP Group a další členy. V současné době působí BSA ve více než 80 zemích světa, ve kterých hájí zájmy komerčního softwarového průmyslu a jeho hardwarových partnerů. Posláním BSA je podporovat kroky a iniciativy, které

vedou k technologickým inovacím, investicím do informačních technologií a důvěře ve výpočetní techniku.

Kromě preventivní činnosti se tato organizace také zabývá praktickými činnostmi, kterými jsou:

- Osvětová činnost, odborné konzultace a činnost, která vede k ochraně zájmů výrobců software a svých členů
- Vydávání odborných stanovisek na vyžádání k jednotlivým případům nelegálního užívání software
- Provádění auditu u firem, zda je na jejich počítačích užíván legální software
- Podávání občansko-právních žalob pro porušení autorských práv, případně podání trestního oznámení, při zjištění nelegálního rozšiřování softwaru.

BSA spolupracuje s policejními orgány, při odhalování softwarového pirátství a pomoci jeho zdokumentování. Tato spolupráce s policií z hlediska činnosti BSA je stěžejní a nejvýznamnější. (3)(5)

5.2 Česká protipirátská unie (ČPU)

„Česká protipirátská unie (ČPU) byla založena v roce 1992 za účelem ochrany autorského práva a práv souvisejících s právem autorským k audiovizuálním dílům a potírání všech forem pirátství v oblasti výroby, dovozu a šíření audiovizuálních děl. ČPU se konstituovala z Protipirátské sekce Unie videodistributorů, která vyvíjela protipirátské aktivity v oblasti audiovize již od počátku 90. let. Činnost ČPU spočívá především v ochraně autorských práv k filmovým dílům, sledování a analýze informací týkajících se autorských práv, přípravě právních kroků proti jejich porušování, spolupráci s orgány činnými v trestním řízení a ostatními institucemi a spolupráci na přípravě nových právních předpisů. V současné době je kladen velký důraz na prevenci a vzdělávání. ČPU sdružuje filmové a home video distributory a poskytovatele kabelového a televizního vysílání. Na činnosti ČPU se podílí též protipirátské oddělení mezinárodní organizace Motion Picture Association a čestným členem ČPU je Národní filmový archiv.“ (12)

5.3 International Federation of the Phonographic Industry (IFPI)

„*International Federation of the Phonographic Industry*“ (Mezinárodní federace hudebního průmyslu) - Tato nevládní organizace se sídlem v Curychu (Švýcarsko), která má přes 1400 členů ve více než 70 zemích světa (včetně ČR), se hlavně zabývá, jak už tomu napovídá název, ochranou autorských práv v hudebním průmyslu. Struktura této organizace je více než zajímavá, pomyslně se dělí na tři skupiny: mezinárodní, regionální a národní. **Mezinárodní sekretariát** se sídlem v Londýně je zodpovědný za koordinaci mezinárodních strategií v klíčových oblastech tvůrčí práce - protipirátského boje, lobování za přísnější právní úpravu u národních vlád či vládních organizací. **Regionální úřady** v Asii, Evropě a Latinské Americe mají za úkol implementaci strategií přijatých londýnským sekretariátem na regionální úrovni, koordinaci prací národních skupin a lobování zaměřující se na konkrétní region. **Národní skupiny** přidružených států se snaží dodržovat postupy přijaté na regionální úrovni s přesným zaměřením na národní trh s hudebními nahrávkami a jejich autorskoprávní ochranou. (20)

Hlavním posláním IFPI je:

- Podporovat hodnotu nahrané hudby
- Chránit práva producentů hudby
- Rozšířit komerční využití nahrané hudby

5.4 Policie ČR

V České republice docela nedávno (1. května 2005) vzniklo Oddělení Informační Kriminality (OIK), a jakožto složka součásti Policie ČR konkrétně Úřadu služby kriminální policie a vyšetřování s celorepublikově vymezenou působností zodpovídá v rámci celé Policie ČR za řešení problematiky počítačové kriminality a kriminality páchané za pomoci počítačů.

Tedy tohle oddělení je odpovědné za:

- útoky na data
- zneužití elektronických platebních systémů
- šíření nelegálního software prostřednictvím Internetu

- ostatní formy využití informačních technologií k páchání trestné činnosti (*dětská pornografie, extremismus, vydírání, vyhrožování…)*
- Porušování autorského práva v oblasti programového vybavení ve smyslu ustanovení § 152 trestního zákona versus občansko-právní aspekty

Největší podíl trestné činnosti, kterou se toto oddělení zabývá je tzv. nadlimitní užívání software nad rámec autorského zákona – tedy nelegální užívání software pro výdělečnou činnost, podnikání apod.
Největším problémem oddělení jsou chybějící experti na IT+kriminalitu, kteří by pracovali pro Policii ČR. (36)

V rámci prevence lze s úspěchem využít tzv. **softwarového auditu**. Cílem softwarového auditu je legalizace veškerého software ve firmě. Hlavním krokem je úplná inventarizace softwaru a hardwaru. Při této činnosti je každý počítač podrobně rozebrán a veškerý nainstalovaný software je zaznamenám a porovnán s účetními doklady a dalšími doklady. V případě neshody legálního nabytí software, navrhne licenční specialista nejvhodnější způsob zlegalizování. Po legalizace veškerého softwaru, je firmě vystaveno osvědčení o softwarovém auditu.

6 Kauzy a trestné činy související s kriminalitou na internetu

6.1 Odsouzení k povinnosti nahradit škodu přesahující milión korun

„Krajský soud v Brně uložil obžalovanému R. D. povinnost uhradit poškozeným škodu, na jejíž náhradu uplatnili nárok v trestním řízení, a to v celkové výši 1 061 730,- Kč. Z toho poškozeným filmovým distributorům ve výši 719 440,- Kč a poškozené společnosti Cenega Czech, s.r.o. specializující se na herní software ve výši 342 290,- Kč.
Odsouzený se dopustil trestného činu porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 152 odst. 1 a 2 písm. b) trestního zákona a trestného činu poškození a zneužití záznamu na nosiči informací podle § 257a odst. 1 písm. a) trestního zákona tím, že v roce 2003 šířil prostřednictvím stránek www.cdr.pegasoft.cz vypálené kopie filmů na CD-R, přičemž bylo zajištěno celkem 843 disků s kopiemi filmů.

Kromě povinnosti k náhradě škody, byl obžalovaný za spáchání výše uvedených trestných činů odsouzen k trestu odnětí svobody v trvání 2 let s podmíněným odkladem výkonu trestu na zkušební dobu 2 roky.“ (31)

6.2 Filmový pirát způsobil škodu za 52 miliónů

„Šestadvacetiletého muže z Rýmařova na Bruntálsku, který pomocí internetu nabízel nelegální kopie filmů včetně úplných novinek, obvinila policie z trestného činu porušování autorských práv. Škoda, kterou měl způsobit, je vyčíslena na 52 miliónů korun."Je to zatím největší případ porušování autorských práv, jaký policie na Bruntálsku odhalila,“ uvedla mluvčí policie Pavla Tušková. Dodala, že muž v období od února do září 2008 nabízel po internetu více než 600 filmů různých žánrů, a to za 35 korun za jedno DVD."Nabídku filmů aktualizoval podle momentálních novinek na trhu. Filmy nabízel v DVD kvalitě na nosičích DVD-R. Zájemcům zasílal seznam a komunikoval přes e-mailovou adresu. Filmy prodával přes poštu a to na dobírku, bez obalů a popsané fixou,“ řekla Tušková.

Policie zjistila zatím několik desítek zákazníků z celé republiky, kteří si od obviněného koupili 138 filmů. "Policisté u obviněného zajistili dalších 456 nosičů a také notebook s externím harddiskem,“ dodala mluvčí. Obviněný muž se podle ní hájí tím, že si chtěl vylepšit svou nedobrou finanční situaci. "Nyní mu hrozí trest odnětí svobody až na dva roky,“ řekla Tušková.“ (19)

6.3 Kauza s The Pirate Bay

The Pirate Bay (*česky:* ***pirátská zátoka***) je švédská webová stránka indexující BitTorrenty. Tato největší světová torrentová databáze a 106. nejpopulárnější stránka dle serveru Alexa.com, je převážně financována z reklamy zobrazující se při vyhledávání. V listopadu 2003 byl spuštěný první server Anti-copyrightovou společností Piratbyrån, ale pak byl již provozován jednotlivci.

Jelikož tento server nepřímo nabízí nelegální software, tak byl předmětem mnoha různých soudních sporů a se stal trnem v oku velkým mediálním společnostem jako např. Warner Bros, Sony Music Entertainment, EMI a dalších. Aby se provozovatelé vyhnuli těmto sporům, rozhodli se koupit v roce 2007 vlastní ostrov v mezinárodních vodách, kde neplatí autorský zákon. Měli zájem o bývalou námořní

plošinu Sealand, ale zarazila je vysoká cena 750 milionů EUR, na kterou chtěli získat peníze pomocí sbírky. (42)

„Dne 17. dubna 2009 došlo k průlomovému rozhodnutí v jedné z nejsledovanějších kauz týkajících se používání P2P sítí a speciálně torrentů. Provozovatelé nejznámějšího torrentového trackeru/vyhledávače **The Pirate Bay** byli uznáni vinnými z napomáhání zpřístupňování autorsky chráněných děl…

Všichni čtyři obvinění (Peter Sunde alias „brokep“, Fredrik Neij alias „TiAMO“, Gottfrid Svartholm alias „Anakata“ i Carl Lundström) dostali každý jeden rok vězení. Soud uznal, že obžalovaní fungovali jako tým, že si byli vědomi, že prostřednictvím The Pirate Bay si uživatelé vyměňují autorsky chráněný obsah a fungováním TPB jim to usnadňovali. Zamítl však vyčíslené horentní sumy přesahující miliardu dolarů, sám stanovil škodu ve výši 30 miliónů švédských korun (v přepočtu 3,62 miliónu dolarů / skoro 74 miliónů Kč / 2,7 miliónu €). Na tuto škodu by se měli všichni čtyři obvinění složit.“ (26)

Tento rozsudek nad The Pirate Bay, zatím není oficiální, jelikož dne 23. dubna 2009 byl soudce Tomas Norström**,** který vedl soudní proces proti TPB nařčen ze zaujatosti a je velice pravděpodobné, že celý proces bude anulován a měl by se opakovat.

Soudce Tomas Norström je členem následujících spolků:

- **SFU (Swedish Association of Copyright)**: Tomas Norström je členem diskuzního fóra pořádajícího semináře a diskuze a vydalo též „Nordic Intellectual Property Law Review“.

- **.SE (The Internet Infrastructure Foundation):** Tomas Norström pracuje pro „nadaci internetové infrastruktury“, která dohlíží nad švédskými doménami `.se` a je poradcem v rozepřích ohledně doménových jmen.

- **SFIR (Swedish Association for the Protection of Intellectual Property)**: Tomas Norström sedí v radě této asociace, mezi jejíž cíle patří i posilování autorských práv. (40)

7 Dotazníkový průzkum

Účelem tohoto anonymního dotazníkového průzkumu bylo zjistit povědomí lidí o internetové kriminalitě a jejich chování na internetu, v závislosti na věku, vzdělání a počítačové gramotnosti. Dotazníku se účastnilo 151 respondentů různých věkových kategorií, vzdělání a pohlaví. Tento dotazník byl realizován za pomoci internetového webu www.vyplnto.cz , který je na tento online průzkum speciálně zaměřen.

Věk, pohlaví a dosažené vzdělání

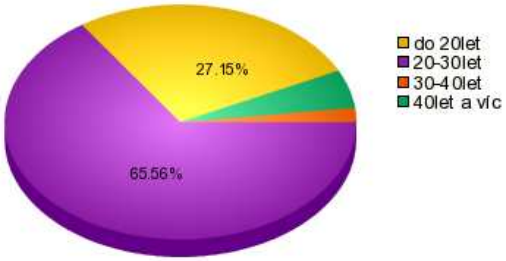
Na dotazník odpovědělo 151 respondentů, z toho bylo 84 (55.63%) žen a 67 (44.37%) mužů, ve věkových kategoriích:

do 20let - 41 (27.15%);

20-30let – 99 (65.56%);

30-40let – 3 (1.99%);

40let a víc – 8 (5.3%)



Graf č. 1 Věk

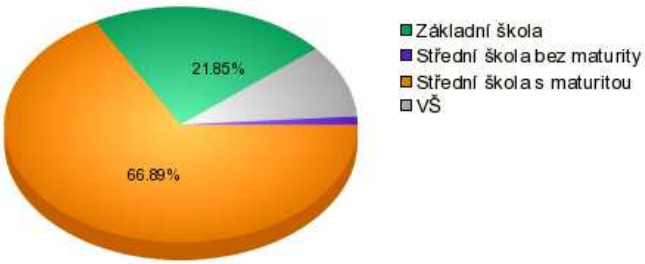
Dosažené vzdělání respondentů bylo následující:

Základní škola - 33 (21.85%);

Střední škola bez maturity - 2 (1.32%);

Střední škola s maturitou - 101 (66.89%)

VŠ - 15 (9.93%)



Graf č. 2 Dosažené vzdělání

Počítačová gramotnost

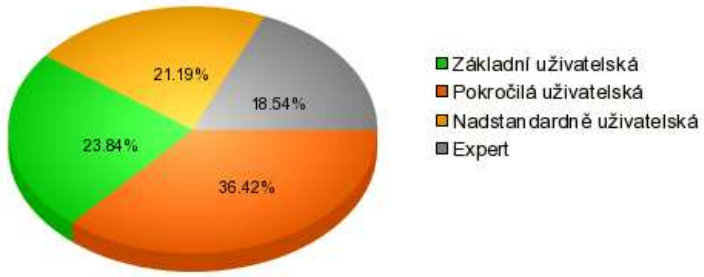
Jelikož se průzkum týká internetové kriminality, tak mě zajímalo, jakou mají respondenti počítačovou gramotnost, abych si dokázal představit orientaci v počítačovém prostředí. Roztřídil jsem je do následujících kategorií:

Základní uživatelská - s počítačem pracuji, ale software a hardware sám radši neinstaluji - **36** (23.84%)

Pokročilá uživatelská - s počítačem pracuji a dokážu si software sám nainstalovat – 55 (36.42%)

Nadstandardně uživatelská - s počítačem pracuji a dokážu si SW i HW sám nainstalovat **- 32** (21.19%)

Expert - s počítačem nejen pracuji, ale dokážu vše okolo SW a HW sám nainstalovat a nastavit - **28** (18.54%)



Graf č.3 Počítačová gramotnost

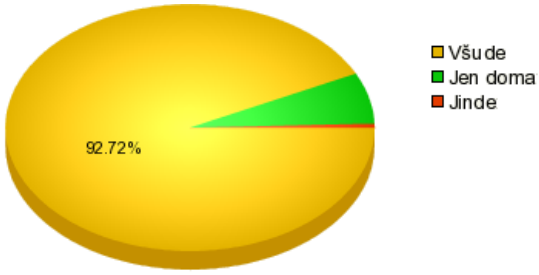
Vzhledem k výsledkům je možno říci, že průzkum byl prováděn z větší části u těch, kteří s počítači pracují a dokážou si software sami nainstalovat, a s hardware si také poradí. Tedy z těchto výsledků můžu usoudit, že tento dotazníkový průzkum zaměřený na internetovou kriminalitu bude objektivní.

Možnosti a četnost připojení

Vzhledem k různým možnostem připojení jsem se respondentů ptal, kde a jak často mají možnost připojit se k internetu. Z nabídnutých možností připojení doma, v práci, ve škole, jinde nebo všechny tyto možnosti, respondenti odpověděli takto:

Všude (doma a v práci, doma a ve škole, všechny možnosti) **– 140** (92.72%)

Jen doma – 10 (6.62%) **Jinde - 1** (0.66%)

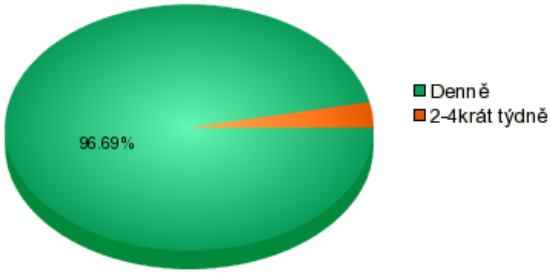


Graf č. 4 Možnosti připojení

V otázce na četnost připojení jsem nabízel možnosti odpovědí: denně, 2-4x týdně a několikrát za měsíc.

Denně - 146 (96.69%)

2-4krát týdně – 5 (3.31%)



Graf č. 5 Četnost připojení

Výsledek těchto otázek jen potvrzuje expanzi internetové technologie, víc než 92% respondentů má možnost připojení k internetu dá se říci všude, tedy na pracovišti, doma, ve škole i jiných veřejně dostupných přístupových bodů. Co se týká četnosti připojení, tak výsledek také potvrzuje, že internet je součástí našeho každodenního života, jelikož více než 96% respondentů odpovědělo, že je připojeno k internetu denně.

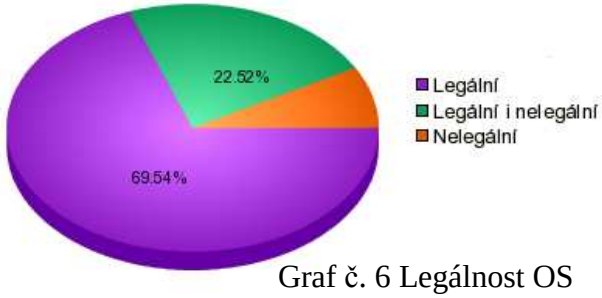
Legálnost operačního systému a softwaru

V dalších otázkách jsem se respondentů ptal na legálnost operačních systémů a softwaru, nainstalovaném na počítači. Operační systém mám:

Legální (vlastním licenci – koupená, případně volně dostupný OS) **- 105** (69.54%)

Nelegální (nevlastním licenci – stáhnutý z internetu) **- 12** (7.95%)

Legální i nelegální - 34 (22.52%)



Graf č. 6 Legálnost OS

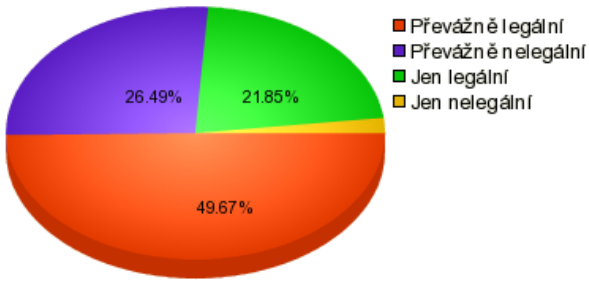
Software na počítači mám:

Převážně legální – 75 (49.67%)

Převážně nelegální - 40 (26.49%)

Jen legální – 33 (21.85%)

Jen nelegální - 3 (1.99%)



Graf č. 7 Legálnost software

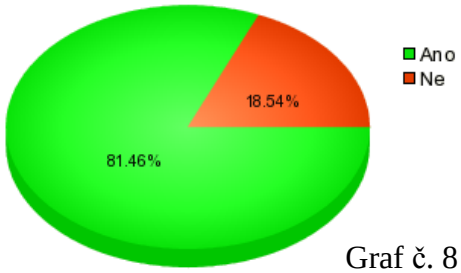
Výsledky otázek věnující se legálnosti systému a softwaru svědčí o tom, že většina respondentů má nainstalovaný legální OS, je možno tvrdit, že to je asi z důvodu, prodeje notebooku s OS či zlevňování cen OS. Důvodem také může být používání volně dostupných OS, jako je například Linux. Co se týče legálnosti softwaru na počítačích respondentu, tak převážná většina (přes 81%) odpovědělo, že má nainstalovaný legální nebo převážně legální software. Důvodem může být dostupnost open source software, tedy volně licenčně dostupných.

Stahování a sdílení filmů, hudby a softwaru

V otázce, kdy jsem se ptal respondentů, jestli stahují hudbu a filmy z internetu, odpovídali následovně:

Ano – 123 (81.46%)

Ne - 28 (18.54%)



Graf č. 8 Stahování hudby a filmů

Následovala otázka týkající se způsobu stahování a dalšího využití.

Legálně (po zaplacení ceny či autorských poplatků z oficiálních serverů) - **7** (4.64%)

Nelegálně, ale pro svoji potřebu – 111 (73.51%)

Nelegálně, pro další sdílení – 7 (4.64%)

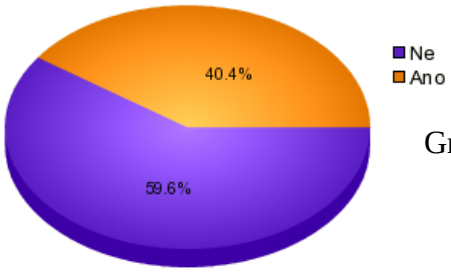
Nestahuju – 26 (17.22%)

Graf č. 9 Legálnost stahování a využití

Poslední otázkou, týkající se hudby, filmů a software byla, jestli ji respondent sdílí.

Ne – 90 (59.6%)

Ano - 61 (40.4%)



Graf č. 10 Sdílení dat

Výsledky okruhu otázek, týkající se stahování a sdílení hudby na jednu stranu nejsou překvapivé, ale z druhé strany si zas odporují. Většina respondentů odpověděla, že hudbu a filmy z internetu stahuje, taky proč ne, není to nelegální, ale co se týče dalšího sdílení, tak více než 40% dotazovaných odpovědělo, že data podléhající autorskému právu sdílí. Zajímavé je, že když jsem se ptal na využití stahovaných dat, tak jen 7 respondentů odpovědělo, že sdílí uvedené data, a většina (73,51%) odpověděla, že data využívá jen pro svou potřebu.

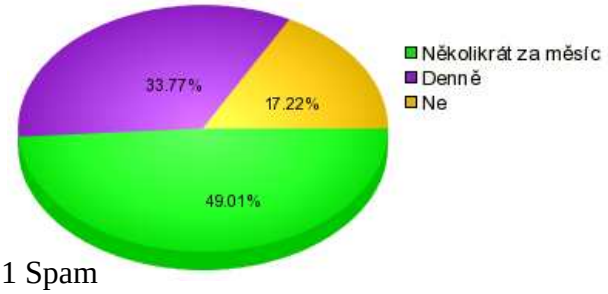
Nevyžádaná pošta, internetové podvody

Každý snad víme co je to spam, tak se jedna otázka dotazníku týkala této nevyžádané pošty, a tomu jak často respondentům chodí na své emailové adresy.

Několikrát za měsíc – 74 (49.01%)

Denně - 51 (33.77%)

Ne – 26 (17.22%)



Graf č. 11 Spam

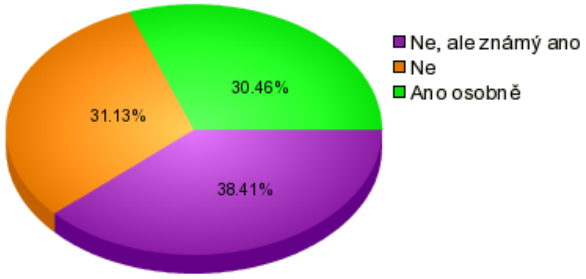
Výsledky této otázky mě nikterak nepřekvapují, dle statistik je přes 90% veškeré emailové komunikace spam, a z tohoto průzkumu vyšlo, že třetina dotázaných dostává spamy denně a skoro polovina několikrát do měsíce.

Další otázkou byla, jestli se respondent setkal na internetu s nějakým podvodem.

Ne, ale známý ano – 58 (38.41%)

Ano osobně – 46 (30.46%)

Ne – 47 (31.13%)



Graf č. 12 Podvod na internetu

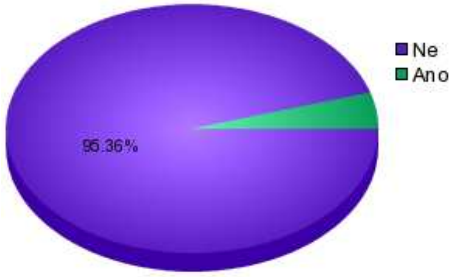
Výsledkem je dle mého názoru jasná odpověď, internet je stvořený pro různé podvody, a dotazník to jen dokázal, více než 30% respondentů odpovědělo, že se s nějakým internetovým podvodem setkalo osobně a dalších 38% odpovědělo, že znají někoho, kdo byl obětí nějakého internetového podvodu. Zbytek tedy asi 31% dotázaných se zatím s žádným podvodem nesetkalo, z vlastních zkušeností můžu jen říci, co zatím není, může být.

Vydírání a vyhrožování na internetu

Na otázku, zdali dotázanému někdo přes internet vyhrožoval, či se stal obětí vydírání, odpověděli respondenti následovně:

Ne – 144 (95.36%)

Ano – 7 (4.64%)



Graf č. 13 Vydírání a vyhrožování

Více než 95% dotázaných odpovědělo, že se nestali obětí vydírání nebo vyhrožování přes internet, v potaz musíme také brát, že většina odpovídajících byla do 30let věku, tedy je možné, že se s tímto velice rafinovaným způsobem vydírání nebo vyhrožování setkají až později. Jelikož, jak už jsem psal, pachatelé na internetu se vyhledávají jen stěží.

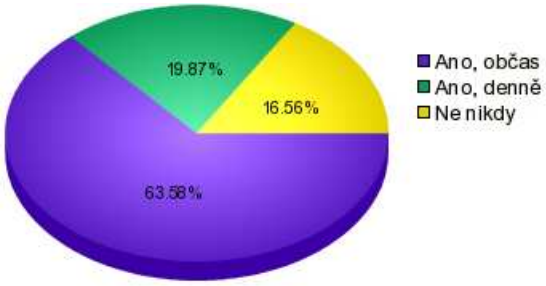
Pornografie

Dalším velice ožehavým tématem na internetu je šíření pornografie, toho se týkala jedna otázka dotazníku. Přesněji to byla otázka, zdali se účastníci průzkumu setkali s pornografií na internetu:

Ano, občas – 96 (63.58%)

Ano, denně – 30 (19.87%)

Ne nikdy – 25 (16.56%)



Graf č. 14 Pornografie na internetu

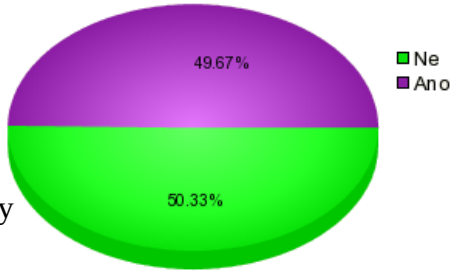
Jak už jsem psal, pornografie je velice častým tématem na internetu a tomu také odpovídají výsledky průzkumu. Skoro 20% dotázaných se s pornografií setkává denně, přes 63% se s ní občas na internetu setkávají. Není to nic překvapivého, jelikož vyskakující „pop-up“ okna a odkazy na stránky tohoto druhu jsou skoro všude. Pouhých necelých 17% odpovídajících, se s pornografií nesetkalo vůbec.

Internetové seznamky

V dnešní uspěchané době se říká, že není čas na klasické seznámení, ale objevil se tady nový druh seznámení, kterého využívá stále více lidí. Jedna otázka v dotazníku se týkala toho, zdali respondent se s někým seznámil přes internet či jestli využívá služeb internetových seznamek.

Ne – 76 (50.33%)

Ano – 75 (49.67%)



Graf č. 15 Internetové seznamky

Z těchto výsledků a z věku respondentů lze usoudit, že tento druh seznamování v dnešní době není nic neobvyklého, polovina dotázaných odpověděla, že se s někým přes internet seznámila, či dokonce že služeb internetových seznamek využívá. Ale položme si otázku, je takové to seznamování bezpečné? Přeci jen musíte být důvěřivý, abyste si s někým začali psát na internetu, na druhém konci může být úplně někdo jiný, než za koho se vydává. Tady je riziko, hlavně pro mladé a nezkušené uživatelé internetu, jimiž jsou převážně děti.

Bezpečnost hesel

Hlavní příčinou toho, že se různí hackeři a pachatelé trestných činností dostanou k velice citlivým údajům je také to, že uživatelé nesprávně volí hesla do svých internetových aplikací. Jednou z otázek dotazníku byla, jestli respondenti volí dostatečně silná hesla, tedy kombinace číslic a písmen velkých i malých v dostatečné délce.

Ne, jelikož jsou složité na zapamatování - 20 (13.25%)

Ano, ale jen někdy – 80 (52.98%)

Ano vždy – 43 (28.48%) **Ne nikdy – 8** (5.3%)

Graf č. 16 Bezpečnost hesel

Z výsledků je vidět, že pouhých 28.48% dotázaných volí svá hesla bezpečně vždy, tedy mají strach ze zneužití jejich dat, dále pak necelých 53% volí svá hesla dostatečně silná jen někdy, předpokládám, že to budou hesla týkající se internetového bankovnictví a další velmi důležitých aplikací. Asi 13% dotázaných, svá hesla nevolí silná, jelikož jim to přijde složité na zapamatování, ale to až se jim do aplikací někdo dostane a zneužije jejich data, si poté zapamatují velice dobře. Zbylých 5.3% respondentů hesla nikdy nevolí dostatečně silná, asi si stále myslí, že internet je velice bezpečné místo.

Dle různých zdrojů z internetu se dovíme, že hacker heslo o 4 znacích malé abecedy zlomí za 0.2s, o 8 znacích za 2,5h, ale když se jedná o všechny symboly ASCII tabulky, tak heslo o délce 8 znaků, tak mu to potrvá prolomit 91 let. Nestojí to za to? Data jsou to nejdůležitější, co v počítači máme.

Bezpečnost internetu

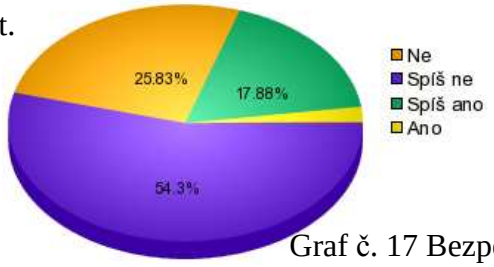
Poslední otázku, kterou jsem dotázaným položil, se týkala jejich názoru na bezpečnost internetu, tedy jestli si myslí, zdali je internet bezpečné místo, z hlediska zneužití údajů, fotografií, a nelegálního šíření dat.

Ne – 39 (25.83%)

Spíš ne – 82 (54.3%)

Spíš ano – 27 (17.88%)

Ano – 3 (1.99%)



Graf č. 17 Bezpečnost internetu

Myslím si, že odpovědi dají za vše, pouze 2% respondentů si myslí, že je internet bezpečné místo, naopak celkem asi 80% dotázaných si myslí, že internet není, či spíš není bezpečné místo, nezbývá mi nic jiného, než s nimi souhlasit. Internet je dobrý sluha, ale špatný pán, když někdo zneužije toho, že dokáže svými schopnosti z Vás dostat potřebné údaje a ani o tom nebudete vědět, poté je internet opravdu nebezpečné místo.

8 Navrhovaná řešení na zlepšení stávající situace

Boj proti počítačové kriminalitě musíme rozdělit na dvě základní složky, **prevence a represe**. Bez dostatečně rozsáhlé prevence, nelze ani s počítačovou kriminalitou bojovat. Když „poškozený“ (nemá-li na PC žádnou preventivní ochranu) nezjistí, že se mu do jeho počítače někdo “naboural“, tak nemá důvod něco takového řešit, a tudíž ani policie či jiné orgány nemají snahu tuto kriminální činnost řešit.

Co se vzájemného poměru těchto složek týká, je jasné, že právě prevence zaujímá imaginární vůdčí postavení, jelikož působení represe je kvůli velkému množství komplikací při vyšetřování těchto počítačových zločinu velmi omezené.

Prevenci se rozumí, různá zabezpečení, která zkomplikují útočníkovi dostat se na Váš počítač, či dostat se k jiným datům takto chráněným. Takto praktikovaná prevence se nazývá **technologická prevence**. Hlavními body této „ochrany“ našeho počítače, je jistě mít zapnuté bezpečnostní prvky, jako jsou antivirové programy, antispyware, firewall, proxy server, zapnutý rezidentní štít a další takto zaměřené preventivní programy. K těmto programům je nutné podotknout, že nestačí jen ho mít na počítači nainstalovaný, ale také důležitým prvkem je udržovat tyto programy s aktualizované a s nejnovější databází proti škodlivému softwaru. Máme-li takto udržované programy na svém počítači, je velká pravděpodobnost, že jsme dostatečně chránění před nebezpečným vlivem vnějšího prostředí. Co se týče emailových zpráv, tak je velice důležité, neotevírat poštu s neznámou přílohou, případně emaily, které nám vůbec nedávají smysl vymazat. Filtrování emailové pošty je taky jeden ze základních preventivních prvků, správně nastaveným filtrem nepronikne až 100% spamu. Dalším preventivním krokem k ochraně našeho počítače, je stahování pravidelných aktualizací systémů od výrobce, i když už se stalo, že „záplaty“ od Microsoftu způsobili více škod než užitku.

Dalším velice důležitým prvkem prevence je dostatečné povědomí uživatelů pohybujících se na internetu. Toto povědomí by se mělo hlavně týkat bezpečnostních rizik na internetu, uživatelé by měli používat dostatečně silná přihlašovací hesla, doporučuje se mít heslo o minimální délce 6-8 znaků složené ze všech znaku ASCII tabulky, takto vybrané heslo trvá hackerovi dlouho, než dokáže prolomit a když se bude ještě pravidelně měnit, tak je takřka nemožné, aby se do vašich aplikací někdo dostal.

Dále by se povědomí uživatelů mělo týkat netikety, tedy chování na internetu a také různých podvodů, které na ně na internetu číhají: phishing, pharming, spamy, hoaxy apod.

Tato prevence se netýká jen uživatelů internetů jako samotných osob, ale vztahuje se také na společnosti a v neposlední řadě se týká i příslušníků policie. Každá společnost, když bude vědět, jaké rizika obnáší mít na svém počítači nelegální software, si zajisté rozmyslí, jestli takto bude jednat či nikoliv, tady lze užít již zmiňovaný „**softwarový audit**“, který firmám zaručí, že jejich software je legální a tím i ušetří problémy spojené s prošetřováním. Pravidla týkající se zabezpečení firemních dat, jsou obdobná, jak už jsem zmiňoval u uživatelů internetu.

Dalším důležitým prvkem je tzv. **psychologická prevence**, tedy šíření povědomí o nemorálnosti a společenské nepřijatelnosti protiprávních činů souvisejících s tímto druhem kriminality. Tato část prevence se týká hlavně stahování a sdílení audiovizuálních děl, hudby a softwaru podléhajícímu autorskému zákonu. Díky anonymitě internetu, si člověk řekne, že se na něho nemůže přijít, ale neuvědomuje si, že se dopouští trestného činu srovnatelného s krádeží. Z velké části, se takto kopírovaná díla šíří dále jen proto, že cena originálů je často nad ekonomické možnosti uživatele. Tedy tady bych apeloval na výrobce softwaru a producenty hudby a filmů, snížením cen těchto produktů se jistě také sníží počet nelegálně šířených dat, jelikož, komu bude stát za to, vystavovat se policejnému stíhání za „pár drobných“.

Do dalšího boje proti počítačové kriminalitě bych zařadil činnost společností, nabízejících své služby na internetu, k ochraně svých aplikací. Myslím tím převážně bankovní instituce, které jsou častým terčem internetových podvodů. Klienti již rozsáhlého internetového bankovnictví, často jsou obětí phishingu, tedy podvodných emailů, když už se ale stanou obětí, a pachatel dostane přihlašovací údaje, je důležité mu zkomplikovat transakce na účtech. Tedy zvýšením zabezpečení např. certifikátem, který má uživatel jen na svém počítači, zasíláním autorizačních SMS či použitím autentizačního kalkulátoru.

9 Závěr

S rychlým nárůstem vývoje informačních technologií a hlavně možnosti využití internetu, se rozmáhá nový druh kriminality, označována jako internetová či počítačová kriminalita. Do takové trestné činnosti můžeme zařadit různé podvody, šíření poplašných či falešných zpráv, nelegální stahování a sdílení autorsky chráněných děl a v neposlední řadě cílené útoky pachatelů na „nevinné“ uživatele internetu, pomocí škodlivého softwaru označovaného jako malware.

Díky převážné anonymitě, kterou internet svým uživatelům nabízí, se kriminalita rozšířila i mezi normální uživatele, ať už cíleně či nevědomě. Tito uživatelé se dopouštějí převážně nelegálního stahování a sdílení warezu, důvodem takového konání může být neinformovanost či úmyslné jednání. Zároveň tito uživatelé se stávají obětí různých podvodných útoků vychytralých nepoctivců, kteří se chtějí na neznalosti jiných přiživit a získat tak od nich citlivé údaje, či data, které mohou nějak zpeněžit, příkladem takového útoku je Phishing nebo Pharming.

Proti nelegálnímu počínání, se zaměřením na potlačování nelegálního stahování a sdílení warezu, se snaží bojovat různé instituce a orgány, v našem případě Business Software Alliance (BSA), Česká protipirátská unie (ČPU), Mezinárodní federace hudebního průmyslu (IFPI) a v neposlední řadě Policie ČR.

Policie ale zaujímá v boji proti počítačové kriminalitě vedoucí roli, jelikož všechny další organizace s ní musí spolupracovat, aby pachatele potrestaly. Zřízením speciálního oddělení informační kriminality, udělala policie velký krok směrem proti tomuto trestnému počínání, ale bohužel stále mají nedostatek specialistů.

V boji s kyberkriminalitou je důležitá prevence, mezi které patří prevence technologická, především softwarové zabezpečení proti útokům, a dále pak prevence psychologická, která se snaží u lidí vzbudit pocit, že to co na internetu páchají, není zrovna morální a legální. Je důležité u lidí zvyšovat povědomí ohledně možných útoků.

Na základě dotazníku jsem zjistil, že internetová kriminalita se dotýká převážné většiny uživatelů a to bez rozdílů věku a pohlaví. Tito uživatelé, ale stále nedostatečně zabezpečují svá data nebo nepoužívají dost silná hesla, ale na druhou stranu dle odpovědí lze usoudit, že používají na svých počítačích převážně legální software.

Vzhledem k rychle se vyvíjejícím moderním technologiím se dá říci, že s tímto trendem budou postupovat i pachatelé trestných činu a bude je stále složitější dopadat,

jelikož bude stále lepší technologie k zamaskování stop. Pozitivem ale je, že povědomí lidí u těchto kriminálních činů roste a pro pachatele je stále složitější vymýšlet způsoby jak uživatele internetu oklamat. Nasazením speciálních oddělení v boji proti počítačové kriminalitě je krokem do budoucna. Co se týče nelegálního stahování autorských děl, tady by byla potřeba, aby producenti snížili ceny těchto produktů a ty by tak byly ekonomicky dostupnější pro většinu uživatelů a nebyla by je potřeba nelegálně stahovat či jinak šířit.

10 Seznam použitých zdrojů

10.1 Klasické zdroje

1) HLAVENKA,J a kolektiv. *Výkladový slovník výpočetní techniky a komunikací*. 3.vyd,Praha: Computer Press, c1997 , s.405. ISBN:80-7226-023-5

2) SMEJKAL,V. a SOKOL,T. *Počítačová kriminalita a její trestněprávní aspekty*. Softwarové noviny. 1993, č. 6

3) LÁTAL, I. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. Policista. 1998, č. 3.

10.2 Elektronické zdroje

4) BEDNÁŘ, Martin. *Historie vzniku internetu* [online]. 2007 [cit.2009-04-27]. Dostupný z WWW: < http://www.owebu.cz/internet/vypis.php?clanek=1083>

5) BSA. *O BSA a členech* [online]. [cit.2009-05-02]. Dostupný z WWW: <http://www.bsa.org/country/BSA%20and%20Members.aspx>

6) *Citibank 20060303 - phishingový útok na české klienty* [online]. [cit.2009-04-30]. Dostupný z WWW: <http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=522>

7) *Co je SPAM* [online]. [cit.2009-05-01]. Dostupný z WWW: <http://www.spamy.cz/co-je-spam/>

8) *Co je to HOAX* [online]. [cit.2009-05-01]. Dostupný z WWW: <http://www.hoax.cz/hoax/co-je-to-hoax>

9) *Co je to Phishing* [online]. [cit.2009-04-30]. Dostupný z WWW: <http://www.hoax.cz/phishing/co-je-to-phishing>

10) *Co je to pirátství a jaké tresty za něj hrozí* [online]. [cit.2009-05-02]. Dostupný z WWW: <http://www.cpufilm.cz/piracy.html>

11) *Čím HOAX škodí* [online]. [cit.2009-05-01]. Dostupný z WWW: <http://www.hoax.cz/hoax/cim-hoax-skodi> V příloze je typický příklad HOAX zprávy.

12) ČPU. *Kdo jsme a čím se zabýváme* [online]. [cit.2009-05-02]. Dostupný z WWW: <http://www.cpufilm.cz/kdo_jsme.html>

13) *Definice SPYWARE* [online]. 2005 [cit.2009-04-30]. Dostupný z WWW: <http://www.viry.cz/forum/viewtopic.php?f=24&t=2788>

14) *Domain Name System)* [online encyklopedie]. [cit.2009-04-27]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Domain_Name_System>

15) *File Transfer Protocol* [online encyklopedie]. [cit.2009-04-27]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/File_Transfer_Protocol>

16) *GÉANT2* [online]. 1996-2009 [cit.2009-04-27]. Dostupné z WWW: <http://www.cesnet.cz/provoz/geant.html >

17) *Hacker* [online encyklopedie]. [cit.2009-04-29]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Hacker>

18) HAUBEN, Michael. *Historie sítě ARPANET/Internet* [ebook]. 2001 [cit.2009-04-27].

19) HONUS,Aleš. *Filmový pirát způsobil škodu za 52 miliónů, tvrdí policie* [online]. 2009 [cit.2009-05-03]. Dostupné z WWW: <http://www.novinky.cz/krimi/163818-filmovy-pirat-zpusobil-skodu-za-52-milionu-tvrdi-policie.html>

20) IFPI. *IFPI's Mission* [online]. [cit.2009-05-02]. Přeloženo z AJ. Dostupné z WWW: <http://www.ifpi.org/content/section_about/index.html>

21) ILKOVÁ, Markéta. *Netiketa známá neznámá* [PDF dokument].[cit.2009-04-30] Inflow, 1/2008, s.4]

22) *Internet* [online encyklopedie]. [cit.2009-04-27]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Internet

23) *Internet u nás* [online]. [cit.2009-04.27]. Dostupné z WWW: <http://www.internet.estranky.cz/stranka/internet-u-nas>

24) *Internet2* [online]. 1996-2009 [cit.2009-04-27]. Dostupné z WWW: <http://www.cesnet.cz/provoz/internet2.html>

25) Jansa,L. *Cybersquatting a jeho podoby* [online], 2008 [cit.2009-05-02]. Dostupný z WWW: <http://www.pravoit.cz/view.php?nazevclanku=cybersquatting-a-jeho-podoby&cisloclanku=2008090003>

26) *Kauza The Pirate Bay na konci začátku: vinni, 1 rok vězení pro každého* [online]. 2009 [cit.2009-05-03]. Dostupný z WWW: <http://cdr.cz/a/26842>

27) *Klient(počítače)* [online encyklopedie]. [cit.2009-04-27]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Klient_(po%C4%8D%C3%ADta%C4%8De)>

28) MATOUŠKOVÁ, Ingrid. *Právo a počítačová kriminalita* [online]. 2006 [cit.2009-04-29]. Dostupný z WWW: <http://web.mvcr.cz/archiv2008/casopisy/policista/2006/01/pockrim.html>

29) MICROSOFT. Co je počítačový virus? [online]. [cit.2009-04-29]. Dostupný z WWW: <http://www.microsoft.com/cze/athome/security/viruses/intro_viruses_what.mspx>

30) MICROSOFT. Co je virus, červ a trojský kůň [online]. [cit.2009-04-30]. Dostupný z WWW: <http://www.microsoft.com/cze/athome/security/viruses/virus101.mspx#E2C>

31) *Odsouzení k povinnosti nahradit poškozeným škodu přesahující milión korun* [online]. 2008 [cit.2009-05-03]. Dostupné z WWW: <http://www.filmynejsouzadarmo.cz/cs/kauzy/>

32) PAUKERTOVÁ, Veronika. *Elektronická informační kriminalita* [online]. (diplomová práce). Praha: Univerzita Karlova v Praze, 2006. 114 s. Dostupný z WWW: <http://www.ikaros.cz/node/3554>

33) *Pharming* [online]. [cit.2009-04-30]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Pharming]

34) *"Pharming": když se phisheři vyvíjejí a usilují o nezjistitelnost* [online]. 2006 [cit.2009-04-30]. Dostupný z WWW: <http://www.symantec.com/cs/cz/norton/library/familyresource/article.jsp?aid=article1_08_06#ve>

35) *Počítačový virus* [online]. [cit.2009-04-29]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus#D.C5.AFvody_vzniku_vir.C5.AF>

36) Řanda, Vít. *Oddělení informační kriminality* [PowerPoint prezentace]. [cit.2009-05-02]

37) SATRAPA, Pavel. Internet2 má novou páteř [online]. 2007 [cit.2009-04-27]. Dostupné z WWW:<http://www.lupa.cz/clanky/internet2-ma-novou-pater>

38) *síť CESNET2* [online]. 1996-2009 [cit.2009-04-27]. Dostupné z WWW:< http://www.cesnet.cz/provoz/>

39) SMEJKAL, V. *Právo duševního vlastnictví* [dokument]. Zpravodaj ČSVZ 2/2000. str. 3

40) *Soudce v kauze The Pirate Bay nařčen ze zaujatosti* [online]. 2009 [cit.2009-05-03]. Dostupný z WWW: <http://cdr.cz/a/26878>

41) *TCP/IP* [online encyklopedie]. [cit.2009-04-27]. Dostupné z: <http://cs.wikipedia.org/wiki/TCP/IP>

42) *The Pirate Bay* [online encyklopedie]. [cit.2009-05-03]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/The_Pirate_Bay>

10.3 Zdroje obrázků

Obr. 1: Mapa ARPANETu z prosince 1970

http://www.darpa.mil/Docs/Internet_Development_200807180909255.pdf ; str. 3

Obr. 2: Mapa ARPANETu z roku 1977

http://www.darpa.mil/Docs/Internet_Development_200807180909255.pdf ; str. 6

Obr. 3: Topologie CESNETu v polovině roku 1993

http://i.iinfo.cz/urs/b0213004-117119266971321.gif

Obr. 4: Mapa sítě Internet2 z roku 2007

http://regmedia.co.uk/2007/10/09/internet2usamap2.jpg

Obr. 5: Topologie sítě GÉANT2

http://www.cesnet.cz/provoz/img/geant.gif

Obr. 6: Topografie CESNET2 duben 2009

http://www.cesnet.cz/provoz/img/cesnet2-topo.gif

Obr. 7: Podvodný e-mail CITIBANK

http://www.hoax.cz/data/hoax/249.jpg

Obr. 8: Přesměrování z e-mailu na podvodnou stránku CITIBANK

http://www.hoax.cz/data/hoax/252.jpg

10.4 Zákony

Zákon č. 140/1961 Sb., trestní zákon

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

11 Přílohy

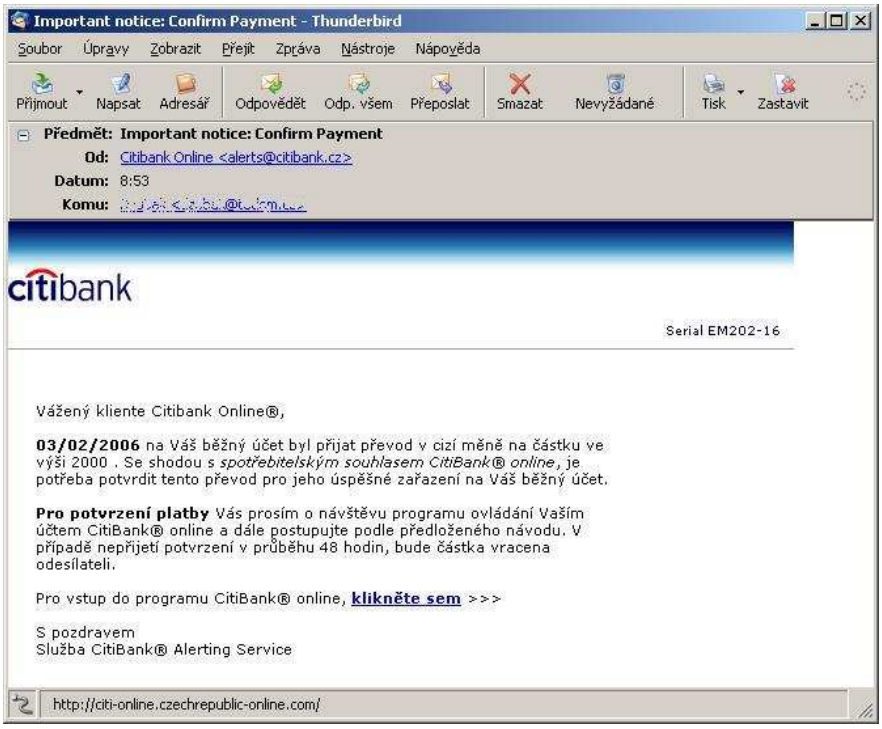
11.1 Phishingový útok na CITIBANK

Příloha 1: Znění podvodného emailu klientů CITIBANK:

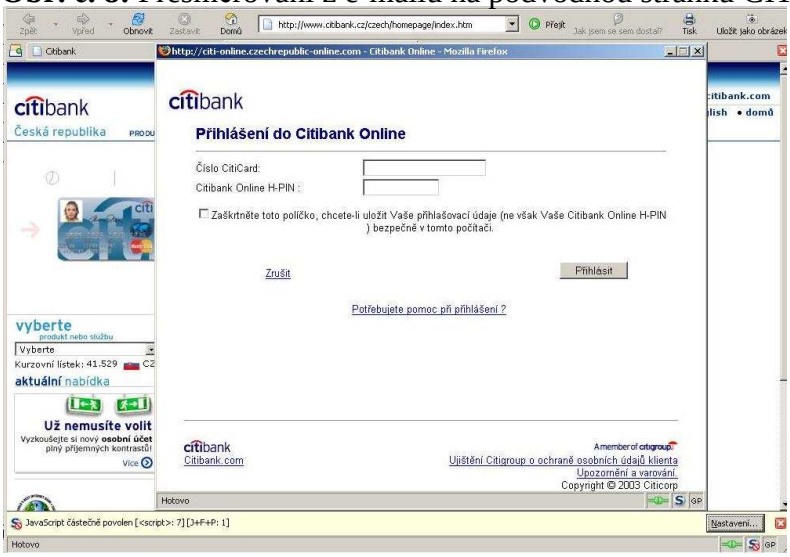
[cit.2009-05-01]. Dostupný z WWW: <http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=522>

„Vážený kliente Citibank Online®.
03/02/2006 na Váš běžný účet byl přijat převod v cizí měně na částku ve výši 2000 . Se shodou s spotřebitelským souhlasem CitiBank® online, je potřeba potvrdit tento převod pro jeho úspěšné zařazení na Váš běžný účet.
Pro potvrzení platby Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank® online a dále postupujte podle předloženého návodu. V případě nepřijetí potvrzení v průběhu 48 hodin, bude částka vracena odesílateli.
Pro vstup do programu CitiBank® online, klikněte sem >>>
S pozdravem
Služba CitiBank® Alerting Service“

Obr. č. 7: Podvodný e-mail CITIBANK



Obr. č. 8: Přesměrování z e-mailu na podvodnou stránku CITIBANK



11.2 Příklad Hoaxu

[cit.2009-05-01]. Dostupný z WWW: <http://www.hoax.cz/hoax/a-virtual-card-for-you/>

„Pozor: Nový virus

Objevil se nový virus, který Microsoft (www.microsoft.com) a McAfee (www.mcafee.com) klasifikují jako nejdestruktivnější dosud známý virus. Byl objeven včera (sobota 7.4.2001) u McAfee a dosud proti němu není spolehlivá ochrana. Tento virus zcela jednoduše zničí sektor 0 vašeho harddisku, kde jsou uloženy životně důležité informace pro správné fungování HD. Virus rozesílá sama sebe automaticky na všechny kontakty z vašeho seznamu s názvem "A VIRTUAL CARD FOR YOU". Když je očekávaná virtuální pohlednice otevřena, počítač "zamrzne" tak, že musí být restartován. Po stisku kláves CTRL+ALT+DEL nebo tlačítka reset virus zničí nulový sektor harddisku, což představuje zničení celého harddisku. Podle vysílání CNN (www.cnn.com) obdržel tento virus zaměstnanec Microsoft. Takže neotevírejte žádný mail s předmětem "A VIRTUAL CARD FOR YOU". Okamžitě po obdržení jej vymažte z pošty. Prosím, odešlete tento mail všem svým přátelům, každému ve vašem adresáři. Raději obdržím tento mail 25x než vůbec. Navíc: Intel oznámil, že se v poslední době objevil nový a velmi ničivý virus. Pokud obdržíte mail s názvem "AN INTERNET FLOWER FOR YOU", neotevírejte jej. Okamžitě jej vymažte! Tento virus odstraní z vašeho počítače všechny dynamické knihovny (soubory s příponou DLL). Poté nebudete moci počítač nastartovat. Pošlete tuto zprávu všem z vašeho adresáře kontaktů“