Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Bakalárska práca

2011 **Diana Kalinová**

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Počítačová kriminalita v Slovenskej republike

Vypracoval: Diana Kalinová
Vedúci práce: Mgr. Ing. Tomáš Sigmund, Ph.D.
Rok vypracovania: 2011

Čestné prehlásenie:

Prehlasujem, že som bakalársku prácu napísala samostatne a v súlade s normou ČSN ISO 690. Všetky zdroje, ktoré boli použité pre účel písania práce, sú uvedené v zozname bibliografických odkazov.

V Prahe dňa 09.05.2011 Podpis: .....

Poďakovanie:

Chcela by som sa poďakovať menovite Mgr. Ing. Tomášovi Sigmundovi, Ph.D., vedúcemu mojej bakalárskej práce, za cenné rady, pripomienky a usmerňovanie pri písaní práce.

Ďalej by som sa rada poďakovala za pomoc a morálnu podporu Alexandrovi Molnárovi, Márii Slovákovej a mojej rodine.

Abstrakt

Bakalárska práca sa zameriava na počítačovú kriminalitu v Slovenskej republike, ako nový druh kriminality, spojený s počítačmi a modernými technológiami a zároveň ako problém, ktorý je potrebné riešiť. Vysvetľuje pojem počítačovej kriminality, jej rozdelenie a problémy, ktoré sú s ňou spojené. Snaží sa priblížiť vybrané druhy tejto kriminality, ich fungovanie v praxi a používané nástroje. V krátkosti zobrazuje históriu počítačových zločinov.

Ďalšia časť zmieňuje najzávažnejšie prípady, ktoré sa odohrali v dejinách slovenskej počítačovej kriminality. Vymenúva a popisuje inštitúcie, zákony a preventívne programy, ktoré sa na Slovensku zaoberajú touto problematikou. Hlavnou časťou práce je nájdenie legislatívnych úprav v zahraničí, ktoré by mali byť pre Slovensko kladným i záporným príkladom. Na základe všetkých získaných informácií uvedených v práci, zhodnotiť situáciu v Slovenskej republike a navrhnúť jej možné riešenie.

Abstract

The Bachelor thesis focuses on cyber crime in the Slovak republic, as a new kind of criminality that is associated with computers and modern technologies as well as a problem, which must be addressed. It explains the concept of cyber crime, its divisions and problems that are associated whit it. It seeks to bring selected types of crime, how they work in practice and used instruments. It briefly reflects the history of computer crime.

The next part of the Bachelor mentions in chronological order the most serious cases, which occurred in the history of Slovak cyber crime. It appoints and describes the institutions, laws and prevention programs, which dealing with this issue in Slovakia. The main part of Bachelor thesis is the search for foreign legislative changes, which should be positive and negative examples for Slovakia. On the basis of all obtained information listed in the thesis, assess the situation in the Slovak republic and propose possible solution.

Obsah

Zoznam skratiek

ARP	Address Resolution Protocol, sieťový protokol určujúci fyzickú adresu z inej známej adresy
BBS	Bulletin Board System, systém umožňujúci pripojenie do siete pomocou počítača a telefónnej linky
CD	Compact Disc, kompaktný disk
ČR	Česká republika
DNS	Domain Name Server, Systém doménových mien
DoS	Denial of Service, útoky spôsobujúce zneprístupnenie služby
DVD	Dissociated Vertical Deviation, digitálny optický nosič
ENIAC	Electronic Numerical Integrator and Computer, prvý elektronický počítač
EÚ	Európska únia
EXE	Execute, spustiteľný súbor
FBI	Federal Bureau of Investigation, Federálny vyšetrovací úrad
FTP	File Transfer Protocol, protokol na prenos súborov v sieti
HTML	HyperText Markup Language, značkovací jazyk pre tvorbu webových stránok
IBM	International Business Machines, firma vyrábajúca počítačový softvér a hardvér
IP	Internet Protocol, internetový protokol
IQ	Intelligence quotient, inteligenčný kvocient
ISO	International Organization for Standardization, Medzinárodná organizácia pre štandardizáciu, archívny formát súboru, obraz disku
MAC	Media Access Control, identifikátor pre sieťové zariadenie
MITM	Man in the Middle, útok, pri ktorom je útočník vystupuje ako prostredník
MMS	Multimedia Message service, multimediálna správa
NBÚ	Národný Bezpečnostný úrad
PC	Personal computer, osobný počítač
PIN	Personal Identification Number, osobné identifikačné číslo
P2P	Peer-to-peer, počítačové siete slúžia na výmenu súborov
RAW	raw, neupravovaný formát súboru
SME	názov slovenského denníka
SMS	Short Message Service, krátka textová správa
SMTP	Simple Mail Transfer Protocol, protokol na prenos emailov
SR	Slovenská republiky
TA3	prvá súkromná spravodajská televízna stanica na Slovensku
TOC	Table of Contents, spôsob ochrany nosičov, prostredníctvom neplatných sektorov
URL	Uniform Resource Locator, jednotný zdrojový lokátor, používaný na internete
USA	United State of America, Spojené štáty americké
USB	Universal Serial Bus, univerzálna sériová zbernica
ZIP	skomprimovaný, archívny formát súboru

Úvod

Počítačová kriminality je pomerne novým fenoménom, s ktorým zápasia všetky krajiny na svete. Často sa o nej dozvedáme z médií, prostredníctvom článkov a reportáži. Mnoho ľudí si napriek tomu nevie ani len predstaviť, aký obšírny je tento problém.

Problematike kybernetickej kriminality sa v Českej republike a na Slovenku venujú odborníci medzi inými i Václav Jirovský a Michal Matějka. Prvý z menovaných pôsobí na ČVUT v Prahe a je vedúcim Ústavu bezpečnostných technológií a inžinierstva. Michal Matějka zasa vyštudoval komerčné právo na VŠE v Prahe a. Práve knihy týchto dvoch odborníkov, Kybernetická kriminalita (Jirovský, 2007) a Počítačová kriminalita (Matějka, 2002), budú jednými z oporných bodov pri písaní práce. V oblasti Phishingu práca vychádza z knihy špecialistu na bezpečnosť a phishing Lance Jamesa (James, 2007). Pre informácie o softvérom pirátstve, bude podkladom kniha (Craig, 2005) Paula Craiga, ktorý skutočne prenikol do pirátskej skupiny.

Cieľom práce je popísať súčasnú situáciu na Slovensku v oblasti počítačovej kriminality a následne navrhnúť možné riešenia problémov.

Aby som dosiahla splnenie cieľa, budem si klásť nasledovné otázky:

1. **Aká je súčasná situácia ohľadne vybraných druhov počítačovej kriminality a celkovo na Slovensku?** To znamená prípady, ktoré sa na Slovensku udiali, situáciu legislatívy, inštitúcií a prevencie.
2. **Čo ju spôsobuje?**
3. **Ako situáciu riešiť?**

Otázky zodpoviem a navrhnem možné riešenie situácie.

Pre pochopenie je najprv predstavený pojem počítačovej kriminality a problémy, ktoré sú s ňou spojené. Následne sú vybrané rôzne členenia a pre rozsiahlosť tematiky, konkrétne druhy kybernality, ktoré sa ale navzájom prelínajú. Bude predstavená krátka história a prevádzanie týchto činov, aby bolo možné ich pochopiť a riešiť.

V práci je vykreslená celková situácia v SR. Vymenované najznámejšie prípady, ktoré sa udiali, ich riešenie, prípadne tresty udelené súdom za tieto činy. Inštitúcie, ktoré v krajine bojujú proti páchaniu a preventívne programy, ktoré sa snažia o vzdelávanie obyvateľov v tejto oblasti.

Inšpiráciou pre návrh riešenia, budú rôzne zákony a návrhy zákonov, z iných krajín, ktoré či už boli platné alebo iba navrhované. Budeme sa zaoberať konkrétnymi vybranými druhmi počítačovej kriminality a k ním budú vyhľadané relevantné i odpudzujúce príklady, ktoré by malo Slovensko brať v úvahu pri prijímaní novej legislatívy.

V závere sa bude nachádzať v krátkosti zhrnuté navrhované riešenie situácie na Slovensku.

1 Definícia počítačovej kriminality

Pojem počítačová kriminalita je v zahraničí známy pod názvami ako cybercrime, IT crime, computer crime, či High-Tech crime. Na Slovensku neexistovalo žiadne stanovené rozdelenie trestných činov, ktoré sú počítačovou kriminalitou, až kým Slovensko ako člen Európskej únie, v roku 2007 ratifikovalo, Dohovor o počítačovej kriminalite.

Definícií počítačovej kriminality je mnoho, pre účel spracovania práce boli vybrané tri. Prvá sa nachádza na oficiálnych stránkach Ministerstva vnútra Slovenskej republiky (Ministerstvo vnútra SR, bez dátumu) v nasledovnom znení: *„Pod pojmom počítačová kriminalita alebo High-Tech Crime sa skrýva využívanie informačných technológií, najmä počítačov na páchanie trestnej činnosti.“*

Druhou je definícia zo Štatútu Komisie expertov pre zločin v kyberpriestore (Matějka, 2002, s. 5, preklad autor). *„Trestný čin namierený buďto proti integrite, dostupnosti alebo utajeniu počítačových systémov alebo trestný čin v tradičnom zmysle, pri ktorom sú použité moderné informačné či telekomunikačné technológie.“*

Ďalšiu z definícií počítačovej kriminality vyslovil vo svojej knihe Kybernetická kriminalita Václav Jirovský (2007, s. 19, preklad autor). *„Kybernetickou kriminalitou, alebo kybernalitou, rozumieme takú činnosť, ktorou je porušovaný zákon alebo je v rozpore s morálnymi pravidlami spoločnosti. Táto kriminalita môže byť namierená priamo proti počítačom, ich hardwaru, softwaru, dátam, sieťam apod., alebo v nej vystupuje počítač iba ako nástroj pre páchanie trestného činu, prípadne počítačová sieť a k nej pripojené zariadenia sú prostredím, v ňom sa takáto činnosť odohráva.“*

Najzrozumiteľnejšou je posledná definícia Jirovského, ktorá vysvetľuje počítačovú kriminalitu jednoducho ale výstižne, porozumejú jej i do problematiky nezasvätení ľudia.

Pre účely tejto bakalárskej práce budú za počítačovú kriminalitu považované všetky nelegálne činnosti prevádzané s pomocou počítača i proti počítaču, ktoré sú páchané so zlým úmyslom, prípadne za účelom nadobudnutia finančného zisku alebo citlivých údajov, dát.

2 Problémy spojené s počítačovou kriminalitou

Riešenie počítačovej kriminality je veľmi zložité, pretože sa spája s viacerými problémami (Jirovský, 2007, s. 19–31), vyskytujúcimi sa vo všetkých krajinách. Pre účel pochopenia počítačovej kriminality a navrhnutia riešení vzniká potreba oboznámenia sa s nasledovnými problémami spojenými s počítačovou kriminalitou:

1. Problém hrozby

Hrozbou je zmena informácie, informačného systému či jeho parametrov. Konkrétnym prevedením hrozby je útok. Útoky sú rôzneho rozsahu a trvania, spôsobujú malé i veľké škody, napr. stratu dôležitých dát alebo ich zneužitie.

Informačné systémy by mali byť pred útokmi chránené. Ochrana môže mať svoje slabé miesta, ktoré môže útočník zneužiť, preto je potrebné vytvoriť bezpečnostnú stratégiu. Správne vyjadriť hodnotu majetku, ktorý je potrebné ochrániť i riziká útoku.

2. Legislatívny problém

V platných zákonoch krajín na celom svete nie sú vymenované všetky nové zločiny počítačovej kriminality a použitie analógie je možné len v niektorých prípadoch. Ďalším problémom je nedostatok zákonov v tejto oblasti, z dôvodu ťažkej definície zločinov počítačovej kriminality a ich dokazovaniu.

Proces prijímania zákonov je zdĺhavý. V dobe prijatia je už zákon neaktuálny, preto by sa mala zvýšiť kvalita navrhovanej legislatívy. Opravou chýb a novelizáciami sa zbytočne legislatívny proces komplikuje.

Zákony by mali chrániť obyvateľov a firmy, preto sú pri vytváraní poradcami odborníci, ktorí sa problematike venujú. Neraz podľahnú záujmovým skupinám a tak zákon neplní svoju pôvodnú funkciu.

3. Problém polície a justície

Hlavným problémom polície je zlyhávanie klasických metód vyšetrovania a nedostatok kvalifikovaných pracovníkov, ktorí sú schopní odhaliť a v priebehu niekoľkých minút zaistiť miznúce stopy počítačového zločinu a nestále rozvíjať svoje znalosti v oblasti kyberpriestoru.

Zločiny počítačovej kriminality sú ťažko odhaliteľné a dokázateľné. Sudcovia nemajú potrebné znalosti, používajú pomoc znalcov na informačné technológie, ktorých je nedostatok. Dôkazy zmiznú bez možnosti zaistenia, kvôli zdĺhavým postupom. Mnoho počítačových zločincov ostáva na slobode.

4. Spoločenský problém

Počítačové zločiny sú spoločnosťou chápané miernejšie ako klasické. Dôvodom je násilie spájané s podstatou klasického zločinu a neúspešnosť polície pri riešení počítačových zločinov. Páchatelia pritom dosahujú vyšší zisk s nižším rizikom zadržania a odsúdenia.

Užívatelia si pri práci s informačnými a komunikačnými technológiami neuvedomujú potrebu bezpečnosti. Riešením je zvyšovanie počítačovej gramotnosti.

5. Problém chápania bezpečnosti

Ľudia príliš dôverujú počítačom. Veria v pravdivosť emailov šíriacich škodlivý softvér z dôvodu nedostatočných znalostí. Nepriznajú si, že práve ich nedostatočná obozretnosť ponúkla možnosť počítačovým kriminálnikom.

V oblasti šifrovania a bezpečnosti zlyhávajú i odborníci, vytvárajúci neprelomiteľné matematické šifry, bez ohľadu na implementáciu a hardvér. Pôsobením teoreticky nepredvídaných podmienok v praxi, sú šifry zdolateľné.

Každý z problémov je veľmi zložitý a ťažko riešiteľný sám o sebe. Je dôležité tieto problémy riešiť, pretože ak nebudú riešené, nikdy nebude dostatočným spôsobom riešená ani počítačová kriminalita.

3 Delenie počítačovej kriminality

Na počítačovú kriminalitu môžeme nazerať z rôznych hľadísk. Každé hľadisko ponúka iný pohľad, podľa ktorého môžeme konkrétny prejav počítačovej kriminality prehľadnejšie zaradiť. Rozdelenie do skupín je v mnohých prípadoch veľmi zložité, pretože konkrétny prejav počítačovej kriminality môže patriť zároveň do viacerých skupín. Z dôvodu prehľadnosti uvádzam viacero možností členenia.

3.1 Počítačová kriminalita z pohľadu legislatívy

Slovensko je členom Európskej únie. Ratifikáciou Dohovoru o počítačovej kriminalite (Rada Európy, 2001) sme prijali členenie trestných činov počítačovej kriminality vytvorené Radou Európy v tomto dokumente. Dohovorom sa trestné činy klasifikujú do nasledovných skupín:

1. **Trestné činnosti proti dôvernosti, celistvosti a funkčnosti počítačových údajov a systémov**

   Do tejto skupiny patria nasledovné trestné činy, ktoré sa musia vyznačovať úmyselnosťou:

   a. **Nezákonný prístup** – za trestný čin nezákonného prístupu sa považuje porušenie bezpečnostných opatrení s nečestným úmyslom. Za nečestný úmysel sa pokladá napríklad úmyselné získanie počítačových údajov.
   b. **Nezákonné odpočúvanie** – je neoprávnené odpočúvanie s nečistým úmyslom voči počítačovým systémom, prostredníctvom technických prostriedkov neverejných prenosov počítačových údajov.
   c. **Zasahovanie do údajov** – sa považuje neoprávnené úmyselné poškodenie, vymazanie, modifikácia a zneprístupnenie počítačových údajov, ktoré spôsobilo značnú škodu.
   d. **Zasahovanie do systému** – úmyselný trestný čin, spôsobený závažnými neoprávnenými meraniami funkčnosti systému prostredníctvom práce s počítačovými údajmi.
   e. **Zneužitie zariadení** – úmyselná výroba, predaj, obstarávanie a údržba zariadení, počítačových programov, počítačových hesiel, kódov a údajov za účelom spáchania trestného činu.

2. **Počítačové trestné činy**

   Počítačovými trestnými činmi sú:

   a. **Falšovanie spojené s počítačom** – neoprávnené vloženie, pozmenenie, vymazanie a zneprístupnenie počítačových údajov s nečestným úmyslom, tak aby boli tieto modifikované údaje považované za autentické.

   b. **Podvod spojený s počítačom** – je úmyselným a neoprávneným vložením, pozmenením, vymazaním, zneprístupnením údajov a zasahovanie do počítačového systému s nečestným úmyslom, za účelom spôsobenia straty inej osobe.

3. **Trestné činy súvisiace s obsahom**

   a. **Trestné činy súvisiace s detskou pornografiou** – úmyselná výroba, distribúcia, ponúkanie, sprístupnenie, prenos, obstarávanie a uchovávanie detskej pornografie za pomoci počítačového systému.

4. **Trestné činy súvisiace s porušením autorských a príbuzných práv**

   Považujú sa za úmyselné trestné činy porušenia autorských a morálnych práv, v obchodnom meradle, prostredníctvom počítačového systému.

3.2 Počítačová kriminalita podľa role počítača

Počítač, podľa Štatútu Komisie expertov Rady Európy pre zločin v kyberpriestore, môže pri páchaní počítačovej kriminality vystupovať rôznym spôsobom (Madliak a Mesároš, 2009, s. 202–205). Z tohto pohľadu môžeme počítačovú kriminalitu rozdeliť na:

1) **Priamu –** zahŕňa nasledovné trestné proti počítačom a iným komunikačným zariadeniam:
   a) útok na počítač, komunikačné zariadenie, program a údaje,
   b) neoprávnené použitie softvéru, tvorba a rozširovanie jeho kópii,
   c) neoprávnené použitie počítača, komunikačného zariadenia,
   d) neoprávnený prístup k údajom, získanie utajovaných skutočností a informácií o osobách,
   e) krádež počítača, programu, údajov, komunikačného zariadenia,
   f) modifikácia programu, údajov

g) šírenie poplašných správ.

2) **Nepriamu –** predstavuje nasledovné trestné činy spáchané za pomoci počítača:
   a) zneužívanie počítačov na inú trestnú činnosť,
   b) bankové krádeže a finančné machinácie spáchané s pomocou počítača.

3.3 Počítačová kriminalita podľa typu konania

Počítačová kriminalita môže byť členená z pohľadu typu konania. Je rozdelená podľa používania pred a po vzniku moderných technológií (Madliak a Mesároš, 2009, s. 199).

Z hľadiska typu konania môžeme počítačovú kriminalitu rozčleniť na:

1) **Tradičnú** – trestné činy, ktoré boli páchané i pred vznikom nových technológií a počítač ponúkol iba novú možnosť páchať klasické trestné činy ako napr. krádež či špionáž iným spôsobom.
2) **Novú** – tieto typy konania vznikli a prišli až so vznikom moderných technológií.

Spomínané členenia následne aplikujeme u jednotlivých vybraných druhov kriminality.

4 Vybrané druhy počítačovej kriminality

Za počítačovú kriminalitu môžeme považovať mnoho nelegálnych činností. Pre rozsiahlosť problematiky je potrebné vybrať iba niektoré. Na základe prvého indexu na svete zaoberajúceho sa počítačovou kriminalitou vytvoreného spoločnosťou Symantec pod názvom Norton Cyber Crime Index (Norton, bez dátumu) boli vybrané nasledovné druhy počítačovej kriminality: hacking, spam, phishing a malware. Tento index je dostupný na webových stránkach spoločnosti, kde každodenne informuje užívateľov internetu o možných hrozbách a zločinoch počítačovej kriminality.

Posledným druhom počítačovej kriminality, ktorá bola vybraná je softvérové pirátstvo. Podľa Siedmej výročnej štúdii BSA o softvérovom pirátstve (2010, s. 12) sa za rok 2008 a 2009 na Slovensku používalo 43% softvéru nelegálne. I keď škody spôsobené pirátmi sa pohybovali okolo 45,2 miliónov eur, týmto percentuálnym podielom sa Slovenská republika zaradila medzi 30 krajín s najnižšou mierou softvérového pirátstva na svete.

U vybraných druhov počítačovej kriminality si vysvetlíme ich fungovanie, vymenujeme a popíšeme nástroje vykonávania a postup páchateľov.

4.1 Hacking

Pojmy hacking a hackeri si väčšina ľudí spája s ich dnešným negatívnym významom a počítačovou kriminalitou najmä vďaka médiám. Pôvodne pojem hacker označoval počítačových odborníkov, programátorov, ktorí sú veľmi zanietenými vo svojej oblasti.

Skutočný hacker sa vyznačuje nasledovnými charakteristikami (Jargon File: New Hackers Dictrionary, bez dátumu):

1. Detailne skúma programovateľné systémy a neustále rozširuje svoje znalosti.
2. Programuje s nadšením.
3. Vie oceniť hack (riešenie problému).
4. Programuje rýchlo a dobre.
5. Expert na program, ktorý používa.
6. Expert na určitú oblasť.
7. Rieši problémy kreatívne a obchádza obmedzenia.
8. Kriminálnici získavajúci citlivé údaje sú crackeri nie hackeri.

Pojmom hacker by sa mali označovať iba pôvodný hackeri, snažiaci sa nachádzať chyby a upozorňovať na nich, zlepšovať systémy, konať dobro. Zločinci, napádajúci systémy, predovšetkým s vidinou zisku by sa mali nazývať crackermi.

V spoločnosti a médiách sa pre počítačových útočníkov používa názov hacker nie cracker. Z tohto dôvodu bude v práci slovo hacker synonymom zločinca a nebude do úvahy braný pôvodný význam slova.

Hacking patrí k novej, priamej počítačovej kriminalite a trestným činom proti dôvernosti, celistvosti a funkčnosti údajov a systému.

4.1.1 Typy hackerov

Z pohľadu kriminality je najlepším rozdelením hackerov delenie podľa klobúkov (Jirovský, 2007, s. 54–55). Delenie, v ktorom sa berie do úvahy legálnosť činnosti hackera. Obsahuje nasledovné tri typy hackerov:

- **White Hat (biely klobúk)** – hacker, snažiaci sa napádať systémy a odhaľovať bezpečnostné trhliny. Objavené slabiny systému nezneužíva. Určitým spôsobom upovedomí majiteľa alebo správcu systému o chybách a ten ich má následne možnosť opraviť. Hacking je jeho záľubou a peniaze zarába ako zamestnanec skutočnej firmy.
- **Black Hat (čierny klobúk)** – označovaný ako hacker alebo cracker, svoje znalosti používa pre zlé a nelegálne činnosti. Hľadá chyby, narúša bezpečnosť, útočí na systémy, kradne, ničí dáta a získava údaje od konkurencie. Vždy so zlým úmyslom, kvôli vidine finančného zisku alebo z dôvodu získania výhody. Pracuje pre kriminálnikov prípadne kriminálne skupiny.
- **Grey Hat (šedý klobúk)** – nachádza sa na hranici medzi čiernym a bielym klobúkom, zväčša sa presúva z jednej skupiny do druhej. Napáda systémy aby upozorňoval na chyby ale nerobí to so zlým úmyslom. Zisťovaním chýb dáva možnosť útočiť iným.

4.1.2 Nástroje hackerov

Jednotlivé nástroje hackerov vysvetľujú ako útočníci pracujú a vykonávajú nelegálne činnosti. Prehľadne môžeme nástroje hackerov rozdeliť do nasledovných hlavných skupín podľa účelu (Jirovský, 2007, s. 59–68):

- **Password cracker (lámač hesiel)** – ľahko použiteľný nástroj, vytváraný na prekonávanie ochrany proti kopírovaniu. Prelamuje staticky zakódované sériové číslo, prostredníctvom kombinovania rôznych možných znakov. Existujú dva základné druhy lámačov hesiel (Jirovský, 2007, s. 62)., ktoré používajú:
  - slovníkové útoky – fungujú prostredníctvom postupného zadávania všetkých slov obsiahnutých v slovníku vytvorenom hackerom,
  - útoky hrubou silou – používajú sa pri vyhľadávaní hesiel, ktoré sú náhodnými kombináciami veľkých a malých písmen a čísel.
- **Backdoor (zadné dvierka)** – program vytvorený hackerom, umožňujúci vzdialene riadiť napadnutý systém bez autentizácie užívateľa. Využíva bezpečnostnú dieru napadnutého systému. Snaží sa v systéme ukrývať. Komunikuje prostredníctvom bežne používaných služieb na portoch, služieb na portoch s vysokým číslom alebo interaktívnymi nástrojmi komunikácie. Napr. sa môže vydávať za webový prehliadač. Takto získané počítače neskôr slúžia pre ďalšie útoky. Program môže byť inštalovaný samostatne, ale väčšinou je súčasťou iného škodlivého softvéru.
- **Skener** – prostredníctvom skenerov sú získavané základné údaje o užívateľovom počítači, o jeho operačnom systéme, verzii systému. Pomáha hackerovi pripraviť sa na útok, zistiť bezpečnostné trhliny a využiť ich k útoku. Skener získava informácie prostredníctvom otvorených portov počítača a bežiacich služieb. Existujú rôzne skenery, zameriavajúce na všetky porty alebo na obmedzený počet portov.
- **Sniffer** – nástroj, slúžiaci na zachytávanie sieťovej komunikácie. Týmto spôsobom útočník získava a analyzuje dáta. Cez prepnutie sieťovej karty do promiskuitného režimu sleduje všetko, čo prichádza a odchádza z počítača. Zložitosť sniffera sa pohybuje od snifferov, používajúcich príkazový riadok až po programy so zložitým grafickým rozhraním. V rukách správcu siete je užitočným nástrojom na diagnostiku. So zlým úmyslom ho môžu zneužiť i úplní začiatočníci.
- **Rootkit** – upravený systémový program, zakrývajúci činnosť hackera a svoju prítomnosť v počítači, ktorý sa usadí priamo v operačnom systéme. Veľmi dobre skrýva škodlivý kód pred bezpečnostnými programami a tvári sa akoby celý systém fungoval v poriadku čo najdlhšiu dobu. Novšie rootkity modifikujú

operačný systém i jadro operačného systému. Môže sa šíriť za pomoci spamu, P2P aplikácií, trójskych koňov alebo komerčných aplikácií. Rootkity zväčša používajú hackeri s vynikajúcimi znalosťami systému, aby mohli zdrojové kódy upravovať pre vlastné potreby.

- **DoS nástroje (Denial of Service nástroje)** – metóda zahltenia systému, ktorá spôsobí nemožnosť prístupu k službe, počítaču alebo sieti legálnemu užívateľovi. Útočník používa exploit – program, vytvorený a určený pre útok. DoS útoky môžeme rozdeliť nasledovne (DoS útoky: úvod, Haller, 2006):
  - záplavové (DoS Flood) – zahlcujú linku užívateľa prostredníctvom veľkého množstva dát, líšia sa od seba použitým protokolom,
  - využívajúce chybu a vyčerpanie systémových prostriedkov – pri útokoch sú využívané chyby v softvéri alebo hardvéri, najskôr útočník analyzuje svoju obeť alebo vyhľadáva nové chyby,
  - využívajúce bezpečnostné opatrenia – útoky využívajú rôzne bezpečnostné opatrenia ako napr. uzamkýnanie účtu po určitom počte pokusov,
  - využívajúce MITM útoky – dátový tok je presmerovaný tak, aby prechádzal cez útočníkov počítač,
  - distribuované (DDoS) – záplavový útok, pri ktorom sa spolu s útočníkom na útoku podieľa viacero počítačov,
  - nechcené (Unintentional DoS) – základnou vlastnosťou je neúmyselnosť,
  - odrážajúce a zosilňujúce – odrážajúcimi útokmi zahlcuje útočník linku obete pomocou iných počítačov a útočník je ťažko odhaliteľný. Zosilňujúcimi útokmi sa množstvo dát od útočníka cestou k obeti zväčší.
- **Trójsky kôň** – malý program zamaskovaný do zdrojového kódu iného programu, ktorý chce užívateľ používať. Slúžia k rôznym účelom, napr. sú schopné zachytávať heslá alebo monitorovať počítač. Užívateľ ho spúšťa neúmyselne, pretože sa vydáva za legálnu súčasť používaného programu. Šíri sa prostredníctvom súborov stiahnutých z internetu alebo emailom. Znižuje výkon počítača. Podľa účelu sa rozdeľujú na (Thigpen, 2004):
  - Backdoor.Trojan – otvára zadné dvierka.
  - Downloader – sťahuje do napadnutého počítača malware.
  - Infostealer – kradne informácie.

- **Nástroje prieskumu siete** – s ich pomocou môže útočník získať užitočné údaje. Prostredníctvom obyčajného webového prehliadača, prezeraním stránky a zdrojového kódu stránky je možné získať mnoho drobných informácií. K týmto nástrojom patria programy ako ping alebo tracert, doplnené o grafické rozhranie.
- **Debugger** – nástroj slúžiaci programátorom na odstraňovanie chýb a ladenie programov. Používa sa najmä pri programoch, ktorých kód má niekoľko tisíc riadkov. Debugger je schopný označiť chybu i riadok, na ktorom sa nachádza. Je používaný na krokovanie kódu, pomocou ktorého útočník nachádza chyby. Do týchto miest vkladá vlastný kód. Využívaný je i crackermi na hľadanie ochranných programov a ich pochopenie. Na základe týchto zistení je vytvorený generátor kľúčov.

4.1.3 Spôsob ochrany proti hackerom

Užívatelia sa musia starať o bezpečnosť svojho počítača. Hackeri sú totiž presvedčení o svojom konaní, ich zlý úmysel a túžbu po zisku zväčša nezmení ani nebezpečenstvo uväznenia. Dnes sú útoky, s pomocou hackerských nástrojov čoraz častejšie a jednoduchšie. Hackeri našli nový spôsob zárobku. Po vytvorení ponúkajú vlastné hackerské nástroje na predaj a prostredníctvom týchto nástrojov dokážu škodiť i úplní začiatočníci.

Ako sa teda týmto nástrojom brániť? Užívatelia by mali pravidelne aktualizovať svoje programy a operačný systém. Aktualizácie slúžia ako záplaty na odstránenie zistených chýb. Útočník musí vynaložiť veľké úsilie hľadaním nových bezpečnostných trhlín. Ďalším spôsobom obrany je zmena pôvodných nastavení, zablokovanie niektorých portov a funkcií programov, aby nebolo možné ich zneužiť, prípadne ich používanie obmedziť a zakúpiť si kvalitný bezpečnostný program, ktorý bude chrániť počítač ako napr. antivírusový softvér alebo firewall.

4.2 Softvérové pirátstvo

Softvérového pirátstva sa dopúšťajú ľudia bez ohľadu na vek, vzdelanie či rodinné pomery, často nevedome. Nelegálne šírenie filmov, hudby, softvéru je pirátstvom a vlastne sa jedná o krádež softvéru. Porušovaniu zákona napomáhajú digitálne kópie originálu, nie sú horšej kvality ako originál.

V knihe Prevencia kriminality (Madliak a Mesároš, 2009, s. 203) je použitá nasledovná definícia: *„Neoprávnené použitie počítačových programov a nelegálna tvorba a rozširovanie kópií programov (softvérová kriminalita, resp. počítačové pirátstvo): ide o jeden z najrozšírenejších a najznámejších spôsobov, ktoré je možné kvalifikovať ako trestný čin porušovania autorského práva.“*

Pirátstvo je novým, priamym konaním kybernetickej kriminality a trestným činom porušovania autorských práv.

Piráti označujú pirátstvo ako súpera, konkurenta legálneho softvéru. Porušujú svojím konaním zákony a spôsobujú veľké finančné škody. Dôvody pirátov sú charakteristickým znakom, ktoré ich od seba odlišujú (Craig, 2005):

- ✓ Pohnútkami prvej skupiny je snaha prekonať ostatných, pirátstvo sa stáva ich závislosťou.
- ✓ Druhá skupina sa pirátstvom zaoberá iba z finančných dôvodov, zdá sa im to ako ľahká možnosť rýchleho zárobku.

Pre priblíženie porušovania autorských práv si vysvetlíme jednu z novších foriem počítačového pirátstva, Warez.

Warez sú organizované skupiny pirátov, ktoré šíria nelegálne softvér ochraňovaný autorskými právami. Skupiny pozostávajú z nasledovných hlavných členov: dodávateľ, líder, cracker, carder. Líder sa stará o fungovanie celej skupiny. Riadi skupinu, usmerňuje všetkých členov a vyhľadáva nových. Warezové skupiny sa chcú porušovaním autorských práv zviditeľniť.

4.2.1 Dodávatelia

Dodávatelia sa snažia získať programy skôr, ako sa dostanú do obchodov, aby všetkým dokázali, že práve oni sú najlepší. Riskujú slobodu s cieľom získať uznanie a popularitu v skupine, nie sú ale žiadnymi amatérmi a pracujú podľa pravidiel. Skupiny získavajú softvér nasledovnými spôsobmi (Craig, 2005, s. 37–60) :

- **Insider** – zamestnanec softvérovej firmy má zväčša v predstihu bezplatný prístup k softvéru firmy, u ktorej pracuje.
- **Zamestnanci spoločností vyrábajúcich média CD, DVD** – dodávateľ ich motivuje vysokou čiastkou, aby počas balenia ukradli CD, DVD so softvérom.

- **FTP Snooping** – monitorovanie adresárov na firemnom FTP serveri, kde firmy umiestňujú dôverné informácie.
- **Podvody s kreditnými kartami** – dodávatelia platia za tovar ukradnutými kreditnými kartami. Spôsob priťahuje veľkú pozornosť, najmä pri drahých nákupoch.
- **Hacking** – je zriedkavo využívaný, ale jednoduchý. Na rozdiel od iných útokov, firma si väčšinou vôbec nevšimne, že bola napadnutá hackerom.
- **Sociálne inžinierstvo** – vydavatelia časopisov majú prístup k softvéru zvyčajne skôr z dôvodu propagácie, prostredníctvom recenzie. Prípadne dodávatelia kontaktujú priamo firmu vytvárajúcu softvér, napr. z dôvodu záujmu o kúpu ich softvéru a zaslanie demo CD.
- **Legitímny maloobchod** – dodávatelia vyhľadajú dátumy, krajiny a v nich obchody, kde bude softvér uvedený ako prvý. Zaplatia, aby dostali softvér najskôr ako je možné a následne prelomia ochranu.
- **Preobjednávky** – pri preobjednávkach dostávajú zákazníci softvér o niekoľko dní skôr ako sa objaví v obchodoch.

Softvéroví piráti sú pre získanie softvéru schopní čohokoľvek, dokonca na páchanie trestných činov navádzajú iné osoby.

4.2.2 Crackeri

Crackeri sú hackeri prevádzajúci nelegálne činnosti. Cracker v pirátskej skupine sa špecializuje na obchádzanie všetkých ochrán softvéru proti kopírovaniu. Spoločnosti investujú do obrany veľké čiastky, pretože piráti im spôsobujú finančné straty. Sú veľmi inteligentnými odborníkmi, schopnými prelomiť i najkomplikovanejší systém obrany. Všetky ochrany musia prekonať vo veľmi krátkom čase a zdolať svojich súperov z iných skupín.

Crackovať nevedia ani niektorí vynikajúci programátori. Je to veľmi zložitý proces, spôsobujúci závislosť a veľkú psychickú záťaž. Práve z tohto dôvodu by mohli byť crackeri slabým článkom pirátskej skupiny a svojou závislosťou a psychickou vyťaženosťou napomôcť k vypátraniu skupiny.

4.2.3 Spôsoby ochrany proti kopírovaniu

Spoločnosti, v snahe brániť svoje práva, vytvárajú mnoho zložitých spôsobov ochrany proti softvérovým pirátom. Môžeme ich rozdeliť do nasledovných skupín (Craig, 2005, s. 70–94):

Sériové čísla – obsahujú mnoho informácií, slúžia na identifikáciu licencie. Rozdeľujú sa do nasledovných druhov:

- **Staticky zakódované** – obsahuje zakódované údaje o užívateľovi, verzii a kuse. Spôsob ako prostredníctvom sériového čísla sledovať držiteľa licencie. Pri získaní sériového čísla crakerom je jedinou možnosťou obrany napísanie čísla na čiernu listinu. Prípadne programátori nelegálne získané sériové číslo ošetria v ďalšej verzii škodlivým kódom.
    - Kľúče zamknuté v node – chránia pred silnejšími útokmi, kľúč obsahuje konkrétne údaje o hostiteľskom počítači napr. MAC adresu, teda každý z týchto kľúčov funguje iba na jednom počítači.
    - CD kľúče – softvér je voľne dostupný po určitú dobu a po uplynutí času je uzamknutý. Pre ďalšie použitie si musí klient zakúpiť licenciu. Následne dostane kľúč, ktorý aplikáciu znovu otvorí. CD kľúče neobsahujú žiadne fyzické údaje o užívateľovi a sú získavané hrubou silou.
    - Algoritmické CD kľúče – sú založené na algoritmoch a matematických vzorcoch. Do kľúča je zakomponovaný druh výrobku, miesto zakúpenia a predajné číslo. Slúži predovšetkým k sledovaniu užívateľov.
    - Metódy ochrany CD nosičov:
        - **Záznam TOC** (Table of Contents) jedna z metód proti kopírovaniu používajúcich poškodený alebo neplatný obsah disku. Ochrana nosičov spočíva v nemožnosti ich prečítania a neplatných sektoroch.
        - **RAW napaľovačky** dokážu skopírovať i média s TOC ochranou, všetky neplatné sektory budú i nanovo napálenom nosiči.
        - **Iná hustota sektoru** a iné meranie reakčného času u doma skopírovaných médií.

- **Komerčné ochranné aplikácie vkladané do .exe súboru**, ktoré zaručujú, že hra zo skopírovaného média nefunguje, navyše crackerom znemožňuje používať debugger.
- Pokiaľ je na počítači nainštalovaný softvér na napaľovanie ako na napr. Nero, softvér sa nedá nainštalovať.

- U starších hier sa používal ako ochrana príliš veľký rozsah hry za pomoci zbytočných programov. Hra sa načítala len v prípade pôvodnej veľkosti.
- Dongle kľúče - ochrana pomocou licenčného kódu na externom zariadení, napr. na USB.

Spôsoby ochrany sa neustále zlepšujú, sú zložitejšie a ich prekonávanie trvá dlhšie. Pirátom sa zatiaľ podarilo každú z ochrán prelomiť. Úspech spoločností chrániacich autorské práva, spočíva v tom, že i keď sú ochrany prekonané, niektoré z nich dokáže prelomiť iba zopár pirátov na svete a trvá im to dlhú dobu.

4.2.4 Spôsoby prelamovania ochrany

Crackeri používajú na prekonávanie ochrany sériových čísel nasledovné spôsoby (Craig, 2005, s. 74–76):

1. **Zmenu zdrojového kódu softvéru** – softvér po manipulácii prijme akékoľvek sériové číslo, správne sériové číslo označí za nelegálne a nesprávne za legálne, prípadne cracker vytvorí malý program Patch, slúžiaci na zmenu kódu softvéru.
2. **Vytváranie legálnych licencií** – spôsob je častejšie používaný, nezasahuje do kódu a licencie, sú zväčša použiteľné v nových verziách softvéru. Craker vytvorí generátor licenčných kľúčov, schopný vytvárať legálne licenčné kľúče.

Odborníci, vytvárajúci ochrany proti kopírovaniu, poznajú niektoré z techník používaných na prelomenie ochrany. Následne budujú nové bezpečnostné programy, ktoré sú proti týmto technikám odolné.

4.2.5 Carder

Z hľadiska fungovania pirátskej skupiny je carder dôležitou osobou, zabezpečujúcou dostatok finančných prostriedkov.

Carding je zneužívanie platobných kariet. Spôsob, pri ktorom útočník získa číslo karty a iné osobné údaje majiteľa účtu, prípadne priamo platobnú kartu. V začiatkoch cardingu sa používali najrôznejšie spôsoby získavania od krádeže samotných kariet, až po hľadanie výpisov v odpadkových košoch. Dnes je carding oveľa sofistikovanejší. Údaje o kartách útočníci získavajú pri nákupoch na internete a z databáz.

Prostredníctvom získaných platobných kariet skupina hradí svoje výdaje. Čím viac veľkých výdavkov skupiny je uhrádzaných prostredníctvom kradnutých kariet, tým viac stôp za sebou skupina zanecháva.

4.2.6 Distribúcia

Predtým, než pirátska skupina zverejní program, musí byť získaný, prelomí sa ochrana, je otestovaný a zabalený, následne distribuovaný. Musí spĺňať určité podmienky, aby sa mohol nachádzať na najbezpečnejších stránkach, napr. veľkosť, kvalitu, názov. Koordinátor zabezpečuje súlad softvéru s pravidlami webových stránok a kuriér čo najrýchlejšie uverejnenie.

Existujú webové stránky, na ktorých pirátske skupiny softvér zverejňujú. Čím má stránka lepšie hodnotenie, tým ťažšie je stať sa jej užívateľov. Najlepšie stránky ponúkajú vysokú bezpečnosť, nič neinzerujú, nelákajú pozornosť, kontrolujú súbory pomocou antivírusových programov a odstraňujú zlé súbory. Stránky s nízkym hodnotením sú často odhalené políciou.

Webové stránky pre uverejňovanie pirátskych programov, môžeme rozdeliť do nasledovných druhov (Craig, 2005, s. 113 – 124):

- **ISO stránky** – stránky, na ktoré sa nahrávajú pirátske programy ako ISO obrazy CD a DVD,
- **0 dňové stránky** – obsahujú súbory upravené pomocou programov WinRar a WinZip, ktoré sa väčšinou sťahujú pár hodín,
- **Music Exclusive** – hudobné pirátske stránky,
- **Súkromné stránky a skládky** – stránky vytvorené samotnými skupinami, obsahujúce mnoho cenných informácií,
- **Site Bots a Clever Pirate** – inteligentné stránky, ktoré upozorňujú užívateľov na posledné zverejnené programy.

Tieto stránky uvádzajú pirátsky softvér na scénu, z nich sú šírené do súkromných adresárov a súkromných skupín a následne ku koncovým užívateľom. Softvér pirátskych skupín neobsahuje vírusy, práve preto nie sú na distribúciu používané P2P siete, na ktorých sa nachádza škodlivý a falošný softvér. Trestná činnosť softvérových pirátov spočíva v porušovaní autorských práv, ale nie šírení škodlivého softvéru.

4.3 Malware

Pojem malware pochádza z anglického výrazu malicious software, čo v preklade znamená škodlivý softvér. Prvoradým účelom tohto softvéru je škodiť počítačovému systému. Šíri sa rôznymi spôsobmi, či už prostredníctvom emailov, internetu alebo programov. Patrí medzi novú, priamu počítačovú kriminalitu. Podľa jeho obsahuje ho možné zaradiť k trestným činom proti dôvernosti, celistvosti a funkčnosti ale i k počítačovým trestným činom.

4.3.1 Rozdelenie malwaru

Podľa určitých charakteristických vlastnostní a použitia môžeme malware rozdeliť do nasledovných skupín (Vírusy, Zodpovedne.sk, 2008):

- **Vírusy**

  Vírus je škodlivý program, podmnožina malwaru, niekedy je nesprávne považovať ho za zástupcu všetkých škodlivých programov. Keď sa dostane do počítača, je schopný nainfikovať iný softvér. Sám sa pripája k legálnemu softvéru. Rozsah škôd vírusu je rozličný, vírus môže spôsobiť drobné škody ale i mať veľké devastačné následky. Ich fungovanie môže byť naviazané na určitý časový údaj. Prenáša sa ako súčasť softvéru, dokumentov, obrázkov, emailov alebo prostredníctvom digitálnych médií. V súčasnosti sa veľmi rozmohlo i napádanie mobilných telefónov prostredníctvom vírusov.

  Najčastejšími druhmi vírusov sú (Vírusy, Zodpovedne.sk, 2008):

  - **BOOTovacie** – vírusy šíriace sa cez BOOTovací sektor diskov. Počítač sa môže nakaziť pri reštartovaní alebo zapínaní.
  - **Súborové** – vírus je zapísaný do spúšťacieho programu, prepísaním časti kódu programu. Spúšťa sa iba spolu s programom.

- **Multipartitné** – vírusy, ktoré sú kombináciou BOOTovacích a súborových vírusov.
- **Neviditeľné** – veľmi dobre sa ukrývajú pred užívateľmi, sú schopné sa sami odvíriť, aby nevzbudili pozornosť a následne znovu zavíriť.
- **Polymorfné** – najťažšie identifikovateľné vírusy. Sú schopné sami meniť časť svojho kódu.

- **Červy**

  Pracujú samostatne, bez ďalšieho softvéru a sami sa kopírujú. Modifikujú operačný systém a šíria sa najmä prostredníctvom bezpečnostných dier alebo sociálneho inžinierstva. Ak sú červy správne nastavené, vedia vykonávať viacero činností, ak nie, môžu spôsobiť iba spomalenie systému a zmätok. Používajú sa na inštaláciu zadných dvierok

  Typy červov (Vírusy, Zodpovedne.sk, 2008):

  - **Internetové** – rozširujú sa pomocou vlastnej počítačovej siete. Po aktivácii sa snažia nakaziť každý počítač, s ktorým prídu do styku. Vyhľadáva bezpečnostné trhliny a snažia sa cez ne do systému preniknúť.
  - **Emailové** – sú súčasťou spustiteľnej prílohy emailu. Po otvorení sa snaží získať všetky emailové adresy užívateľa a rozosielať sa ďalej jeho známym.

- **Trójske kone**

  Sú podobné ako vírusy. Nie sú schopné sa rozmnožovať, sú súčasťou určitého užitočného programu. Tvári sa akoby prebiehal legálny program, za ktorým sa ukýva ale v skutočnosti robí svoje vlastné činnosti, ako napr. ničenie dát.

- **Dialery**

  Programy presmerovávajúce telefónne spojenie na linky s vysokou tarifikáciou s následkom vysokých účtov za telefon. Program dokáže zmeniť nastavenia systému pripojenia, nasmeruje pripojenie tak, aby prechádzalo cez ním určené číslo. Nemajú vplyv na počítače so širokopásmovým internetom. Týmto spôsobom boli spoplatňované niektoré stránky s nevhodným obsahom.

- **Spyware**

  Škodlivé programy, zhromažďujúce citlivé údaje o užívateľovi, ktoré následne posielajú ich útočníkovi. Hlavnou činnosťou spywaru je špehovanie. Spyware

získava informácie o operačnom systéme, technických parametroch počítača, navštevovaných stránkach a pod. Informácie získava rozličnými spôsobmi, napr. sleduje všetky stlačené klávesy na užívateľovom počítači. Na ich šírenie sa využívajú trójske kone.

Dobre sa zamaskujú pomocou iných aplikácií a názvov súborov. Vedia obchádzať antivírusový softvér. Vydržia sa skrývať dlho, pretože sa netvária vôbec podozrivo, ale spôsobujú spomalenie počítača.

- **Adware (Advertising-supported software)**

  Program slúžiaci ako počítačová reklama. Po inštalácii alebo používaním zobrazuje na monitore reklamu. Je upravovaný tak, aby monitoroval činnosť užívateľa (napr. sleduje, aké stránky užívateľ navštívil) ale nezachytával osobné údaje. Následne podľa monitoringu zobrazuje reklamy, ktoré by mohli užívateľa zaujať. Kvôli tejto funkcii je často zamieňaný za Spyware, ktorý ale nielen monitoruje užívateľa, ale získava i citlivé údaje bez jeho vedomia.

- **Spam**

  Nevyžiadaná elektronická pošta zasielaná hromadne. Väčšinou posielaná z komerčných dôvodov. Otravný spôsob zasielania reklamy prostredníctvom emailov, SMS alebo MMS. Častokrát obsahuje spam i iný škodlivý softvér, ktorý po otvorení správy napadne užívateľov počítač. Podrobnejšie informácie o spame sú uvedené v nasledujúcej kapitole.

- **PopUp a Hijackery**

  PopUp sú agresívne programy, otvárajú okná webového prehliadača, ktoré sú zväčša reklamou alebo otvárajú užívateľovi stránky s nevhodným obsahom. V prípade Hijackeru sa jedná o škodlivý softvér, ktorý upravuje užívateľove nastavenia webového prehliadača a bez jeho pokynov otvára okná prehliadača. Nasmeruje ho na stránky so zakázaným obsahom. Na týchto stránkach väčšinou na užívateľa číha ďalší malware napádajúci jeho počítač.

- **Hoax**

  Existoval už dávno predtým, než vznikli počítače a bol zasielaný papierovou formou, no jeho šíreniu výrazne pomohol vznik internetu. Hoax v dnešnej podobe poplašných správ sa prvýkrát objavil v roku 1988.

  Jedná sa o poplašnú správu a reťazové listy šíriace sa prostredníctvom emailov, SMS, MMS a cez instant messaging. Rozposielajú ho bežní užívatelia z dôvodu

nevedomosti. Práve naopak, myslia si, že spravia dobrý skutok, alebo im posielanie správ prospeje. Autori Hoaxov sa týmto spôsobom zabávajú na ľuďoch. Hlavnými znakmi Hoaxu sú (HOAX, Zodpovedne.sk, 2008):

- **naliehavosť správy, popis nebezpečenstva,**
- **ničivé dôsledky,**
- **snaha o dôveryhodnosť,**
- **prosba alebo apelovanie na ďalšie posielanie správy**.

Najčastejšími druhmi Hoaxov sú (HOAX, Zodpovedne.sk, 2008):

- varovania pred útokmi, vírusmi,
- popis nebezpečenstva,
- prosby o pomoc,
- fámy,
- petície a výzvy,
- podvodné emaily, ako napr. Nigérijské listy,
- ponuky rýchleho zbohatnutia,
- reťazové listy,
- vtipné správy.

- **Phishing**

  Zasielanie podvodných emailov za účelom vylákania citlivých údajov od užívateľa a ich následné zneužitie. Phishing sa považuje aj za druh spamu.

- **Phraming**

  Vytváranie podvodných stránok, napodobňujúcich skutočné stránky nejakej inštitúcie s cieľom získania citlivých údajov. Stránka je takmer dokonalou napodobeninou, a tak si mnoho užívateľov vôbec nevšimne rozdiel oproti skutočnej stránke inštitúcie, je teda zameraný na chybu užívateľa. Najčastejšie sú takto vytvárané stránky bánk, za účelom získať údaje užívateľa a následne finančné prostriedky z jeho účtu. Pri podozrení na pharming je potrebné všimnúť si, či je stránka so zabezpečeným protokolom a kto podpísal bezpečnostný certifikát.

- **Spoofing**

  Spoofing je metódou zakrývania totožnosti útočníka. Útočník pri spoofingu mení svoju IP adresu, email alebo sa stáva prostredníkom komunikácie.

4.3.2 Spôsob ochrany proti malwaru

Ochrana proti malwaru spočíva predovšetkým v prevencii a zodpovednosti užívateľov. Dôležité je používanie menej známych programov a operačného systému, ktoré nie sú častými cieľmi útokov, zabezpečenie počítača prostredníctvom firewallu, anti-spywaru a antivírusových programov. Užívatelia by sa mali vyhýbať nebezpečným stránkam, sťahovaniu a zdieľaniu súborov, čítaniu neznámych a podozrivých emailov, inštalovať všetky dostupné aktualizácie a zálohovať dáta.

4.4 Spam

„Spam je nevyžiadaná reklamná pošta, alebo iné nevyžiadané oznámenie, spravidla komerčného charakteru zasielané hromadne mnohým príjemcom.“ (Adámek, 2009, s. 16, preklad autor).

Ministerstvo financií SR v rámci informatizácie spoločnosti uvádza nasledovnú definíciu spamu (Bíro, 2008): *„Vo všeobecnosti sa pojmom spam označuje nevyžiadaná elektronická pošta. Ide o e-mail, ktorý si príjemca vopred nevyžiadal a vo väčšine prípadov obsahuje marketingové a komerčné prvky. Takýmto spôsobom fyzické i právnické osoby ponúkajú služby a tovar, alebo sprostredkovanie takejto služby alebo tovaru. V širšom zmysle sa pod pojmom nevyžiadaná elektronická správa označuje elektronická pošta vrátane SMS (short message service), MMS (multimedia message service), faksimilnej správy a inej elektronicky posielanej správy, ktorá bola odoslaná príjemcovi bez jeho predchádzajúceho súhlasu.“*

Spam by sme teda mohli definovať nasledujúcimi charakteristickými prvkami:

- automatickosť zasielania,
- veľký počet príjemcov,
- nevyžiadanosť,
- nemožnosť zrušiť odber správ
- nelegálnosť.

4.4.1 Formy spamu

Za spam sú považované nasledovné formy emailov (Grendár, Kocák a Špitalský, 2011 ,s. 11–16) :

- **Obchodné ponuky obsahujúce odkaz na webovú** stránku – jedná sa o reklamné emaily na rôzne druhy tovarov a služieb, ktoré sú nevyžiadané.
- **Scam** – známy aj pod názvom nigérijské listy. Scam sa pokúša podviesť užívateľov, emailami obsahujúcimi výherné oznámenia a obchodné ponuky. Prostredníctvom ponúk a oznámení sú získané citlivé údaje, ktoré sú neskôr zneužité.
- **Kontaktné emaily** – emaily sú posielané s cieľom nadviazať s užívateľom kontakt, pre následné zasielanie spamu alebo scamu.
- **Verifikačné emaily** – emaily, ktoré obsahujú odkaz na webovú stránku. Kliknutím na odkaz užívateľ neúmyselne potvrdí aktívnosť adresy pre zasielanie spamu.
- **Phising** – emaily, tváriace sa veľmi dôveryhodne, posielané za účelom získania citlivých údajov užívateľa.
- **Malware** – email, obsahujúci škodlivý softvér.
- **Nekomerčný spam** – politické alebo náboženské emaily, prípadne poplašné a reťazové správy.

Najčastejšie používanými sú obchodné emaily, ktoré sú reklamou od spoločností, ktoré nemajú súhlas na zasielanie reklamných emailov. Dôvodom pre zasielanie obchodných spamov je získavanie zákazníkov. Firmy prostredníctvom spamu dokážu získať niekoľkých zákazníkov.

4.4.2 Rozosielanie spamu

Pre rozosielanie spamu sa používajú anonymné emaily, aby nebolo možné vypátrať pôvodcu. Jedným z hlavných cieľov odosielateľov spamu je vytvoriť kvalitný zoznam s najväčším počtom emailových adries, na ktoré je možné spam odoslať. Ďalším cieľom je vytvorenie emailu, ktorý je schopný prejsť cez filtre, zachytávajúce spam a schopný zaujať oslovenú osobu. Ako je možné tento filter prekonať? Každý údaj v emaile je hodnotený určitým číslom, napr. záhlavie, obsah. Emaily sú upravené tak, aby podľa filtrov boli údaje dôveryhodné a nedosahovali hodnoty, podľa ktorých je spam zachytený.

Pre šírenie spamu sú používané nástroje hromadnej pošty, ktoré sú schopné naraz odoslať milióny emailov s rovnakými vlastnosťami rôznym ľudom. Odosielatelia

spamu majú ako všetci ľudia zaužívané určité zvyky, medzi ktoré patrí i používanie rovnakých nástrojov pre šírenie spamu. Najviac používanými sú nástroje vytvorené samotným odosielateľom, no niektorí vyžívajú i drahé zakúpené nástroje.

4.4.3 Spôsob ochrany proti spamu

Určitý spôsob ochrany spočíva znovu v opatrnosti užívateľov, ktorí by nemali často zverejňovať svoj email. Prípadne by si pre účely registrácií a zverejňovania mali vytvoriť iný email. Ďalším krokom k bezpečnosti je používanie kvalitného emailového klienta, antispamového filtru a neotváranie podozrivých emailov.

Spam je možné filtrovať pomocou niektorých charakteristických vlastnostní a práve prostredníctvom týchto vlastností je rozborom možné identifikovať profil skupiny odosielateľov spamu alebo konkrétneho odosielateľa. K charakteristickým prvkom pre identifikáciu patria (James, 2005, s. 25) :

- identifikácia nástroja pre hromadnú poštu,
- podskupiny vlastností,
- metóda rozosielania spamu.

4.5 Phishing

Phishing sa vyčlenil ako druh spamu, presnejšie patrí do kategórie scamu. Odosielatelia phishingových emailov sa prostredníctvom zdanlivo pravého emailu od dôveryhodnej inštitúcie prípadne firmy pokúšajú zistiť citlivé údaje. Pravú podstatu phishingu vyjadruje odvodenie od anglického slova fishing, čiže rybárčenie. Podvodník odošle množstvo phishingových emailov na všetky adresy vopred pripraveného zoznamu a čaká na svoj úlovok, na chvíľu, kedy jeden z príjemcov emailu uverí jeho správe a on získa prihlasovacie meno, heslo, prístupové práva a iné údaje. Phishing patrí k počítačovým trestným činom, medzi nepriamu a novú počítačovú kriminalitu.

U phishingovej skupiny sa získané dáta ukladajú na serveri typu base camps, ktorý slúži ako centrála komunikácie a distribúcie phisingovej skupiny a na serveri typu anonymných stránok. Najväčšia možnosť získať údaje prostredníctvom phishingového emailu je podľa výskumov do 48 hodín od odoslania emailu. Phisheri falšujú emaily za účelom krádeže. Šikovnejšie skupiny používajú na krádeže malware zachytávajúci údaje vyplnené do formulárov.

Veľmi výstižnou je definícia jedného z najväčších svetových odborníkov v oblasti počítačovej bezpečnosti Lance Jamesa, ktorý phishing definoval nasledovne (2005, s. 28, preklad autor): *„...primitívna metóda, ako spôsob odosielania falšovaného emailu príjemcovi, ktorý klamlivým spôsobom napodobňuje legálnu inštitúciu s úmyslom vyzvedať od príjemcu dôverné informácie ako číslo platobnej karty alebo heslo k bankovému účtu. Takýto email väčšinou navádza užívateľa, aby navštívil nejaké webové stránky a zadal tu tieto dôverné informácie.“*

Phishing pri presmerovaní užívateľa na falošné webové stránky inštitúcií a firiem používa klamanie oka prostredníctvom fuzzy domains. Využíva, že bežný užívateľ si nevšimne nepatrne modifikovanú URL adresu inštitúcie, za ktorú sa phisher vydáva. Ďalší trik je zameraný na sémantiku URL adries. Časť URL adresy je prevedená do iného kódovania, aby bol užívateľ zmätený.

Dnes je však úspešnejšou formou phishingu phishingový email, spojený s key-logovým malwerom, ktorý zaznamenáva používanie tlačítok klávesnice. Obeťou sa stáva viacero užívateľov, ponúka väčší objem zistených dát ale nevýhodou je, že získané informácie nemusia byť pre phishera potrebné a využiteľné. Proti phishingovému malweru je možné brániť sa aktualizáciami antivírových programov. Phishingový malware je viac vhodný pre získanie informácií k jednoduchším systémom, naopak phishingový email pre získanie citlivých informácií k zložitejším systémom.

Phishing prebieha veľmi rýchlo, preto je ťažké nájsť jeho páchateľov. Falošné stránky inštitúcií migrujú medzi servermi a sú aktívne počas krátkej doby. Všetky stopy, ktoré phisher zanechá sú v dobe zaisťovania stôp a vyšetrovania už neaktuálne.

4.5.1 Základný postup pri phishingu

Nasledovné metódy útokov sú iba jednou z možných variant používaných skutočnými útočníkmi, ale ponúkajú možnosť pochopiť fungovanie phishingu. Všetky typy phishingových útokov môžeme považovať za MITM. Medzi základné postupy pri phishingu patria (James, 2005, s. 43–74):

1. **Útok metódou falošnej identity**

Najjednoduchšia z metód, ktorá využíva na prilákanie obetí falošnú stránku konkrétnej inštitúcie s vzhľadom veľmi podobným originálnej webovej stránke.

Pri metóde falošnej identity útočník najprv odzrkadlí skutočnú stránku inštitúcie, neskôr ju modifikuje, tak aby získavala údaje. Stránka môže byť prepojená s originálnou webovou stránkou, z dôvodu úspory času a zobrazovania všetkých obrázkov a odkazov z originálnej stránky. Stránka je umiestnená na server a všetky získané údaje sú odosielané do anonymnej emailovej schránky vytvorenej útočníkom.

Jednou z techník, ktorá je pri metóde falošnej identity používaná je MITM – Man in the Midlle. Útočník je sprostredkovateľom, odpočúva skutočnú komunikáciu medzi užívateľom a skutočnou webovou stránkou. Najprv klienta presmeruje na svoj server, získa údaje a následne presmeruje a prihlási užívateľa na skutočnú webovú stránku. Útok je prevádzaný prostredníctvom:

- **oklamania ARP** – útočník presvedčí klienta, že je hlavným smerovačom, bránou pre prístup na internet,
- **oklamania DNS** – DNS server je nútený odoslať klientovi IP adresu falošnej webovej stránky, a tak klient nenavštívi originálnu stránku inštitúcie ale falošnú,
- **vychýlenia URL alebo HTML** – užívateľ je presmerovaný na phishingový server,
- **trójskeho koňa** – útočník prostredníctvom škodlivého softvéru ovláda webový prehliadač užívateľa.

Jedným z najdôležitejších krokov získania obete je vytvorenie dôveryhodného emailu, ktorý je formálny a používa nátlak na užívateľa. Doplnený je odkazom na falošnú stránku, ktorú je potrebné navštíviť.

2. Útok metódou presmerovania

Phisher používa email, ktorého vzhľad je totožný so vzhľadom niektorej zo známych webových stránok ako napr. eBay, s presmerujúcim odkazom ponúkajúci prihlásenie. Prostredníctvom prihlásenia sú získané prihlasovacie údaje osoby a následne je osoba presmerovaná alebo dokonca prihlásená na skutočnú webovú stránku spoločnosti.

Útočník potrebuje iba presmerovací skript na serveri a údaje od užívateľa sú získané priamo zadaním do emailu. Sofistikovanejšia metóda používaná skôr hackermi, pri ktorej je posielaný phishingový email ako vestník či email oboznamujúci s výhodami pri nákupe v elektronických obchodoch a aukciách.

Pri metóde je dôležitý email, v ktorom je možné sa prihlásiť a jeho súčasťou je zachytávací a presmerovací skript. Pomocou presmerovacieho odkazu a jednej z techník MITM útočník získa prihlasovacie údaje.

3. Útok metódou vyskakovacích okien

Pomerne neúčinná metóda útoku, ktorej zabraňujú prehliadače webových stránok blokovaním vyskakovcích okien. Metóda sa prvýkrát vyskytla v roku 2003 a vyznačuje sa nízkou návratnosťou. Server útočníka presmeruje užívateľa na novú stránku a zobrazí mu vyskakovacie okno s formulárom, do ktorého má užívateľ vpísať prihlasovacie údaje, ktoré budú odcudzené.

Na mieste je otázka ako vlastne phishingové skupiny dokážu sfalšovať email? Využívajú, že pri návrhu SMTP protokolu nebol kladený dôraz na bezpečnosť. V SMTP protokole je možné zmeniť niektoré položky záhlavia, iné sú naopak nemenné ako napr. IP adresa, podľa ktorej je možné odhaliť, odkiaľ bol email odoslaný. Navyše väčšina emailov obsahuje špecifické údaje v záhlaví, ktoré email obsahuje práve pre prípad, že je nevyžiadanou poštou a s ich pomocou je možné odhaliť odosielateľa. Phishingové emaily tieto údaje určite neobsahujú. Skúsený odborník tak jediným pohľadom odhalí falošný email. Phishing sa prevádza i za pomoci cudzích open relay a proxy serverov, aby phisheri skryli svoju IP adresu. Najnovšie využívajú phisheri i bezdrôtové pripojenia reštaurácií či iných podnikov – war driving.

4.5.2 Spôsoby ochrany proti phishingu

Proti phishingu sú na trhu dostupné rôzne antiphishingové programy, nie je však isté že po zakúpení takéhoto softvéru sa mu vyhnete a budete chránení. Mnoho dodávateľov totiž nechápe podstatu phishingu a pristúpili k budovaniu antiphishingového softvéru z dôvodov vidiny ľahkého zárobku.

Užívateľ sa môže chrániť podobne ako v prípade spamu, používaním kvalitného emailového klienta, antispamového filtra a nečítania podozrivých emailov.

5 História počítačovej kriminality vo svete

Rozdelenie počítačovej kriminality a konkrétne prípady do roku 2001 sú použité z knihy. Udalosti od roku 2001 do 2008 pochádzajú z webových stránok (Wavefront Consulting Group, bez dátumu). Počítačová kriminalita (Matějka, 2002, s. 17 – 42). Prípady od roku 2008 po súčasnosť boli vybrané.

5.1 Obdobie do roku 1981

Počítačová kriminalita vznikla dávno pred prvým počítačom, v roku 1801 vo Francúzsku, s prípadom týkajúcim sa automatizovaného tkáčskeho stroja. Nasledovali výstrelky v telefónnych ústredniach a v 20. storočí zneužívanie telefónov.

Prvý elektronický počítač ENIAC z roku 1946, ešte nebol podnetom pre počítačové zločiny z dôvodu finančnej i priestorovej náročnosti. Programy fungujúce na týchto počítačoch boli plné chýb. Prvýkrát sa objavuje pojem hacker, odvodený zo slova hack, ktoré predstavovalo optimalizačné zásahy do programov a hacker bol programátor, ktorý analyzoval a optimalizoval programy.

Pojmy ako phreaker, hacker a creaker sa začali počas vojny vo Vietname spájať s prienikom do systému prostredníctvom siete. Protivojnové hnutie Yippie vďaka manipulácii s telefónnymi systémami často používalo telefón zadarmo. Neskôr začal phreaking, zneužívanie telefónnych sieti, slúžiť ku krytiu nelegálnych činností.

Začiatkom 60. rokov prichádzajú kotúčové magnetofóny, možnosť kopírovania a významné porušovanie autorských práv.

V 70. rokoch začala vznikať prvá sieť počítačov Arpanet, bez dôrazu na bezpečnosť. Odborníci nepredpokladali rozmach sietí až do dnešnej podoby. V roku 1971 sa preslávil John Draper, ktorý používal na oklamanie telefónneho automatu píšťalku z cereálií Cap ´n´ Crunch. Rokom 1978 a vynálezom Bulletin Board System, získal každý majiteľ počítača a zároveň telefónnej linky možnosť pripojiť sa do siete.

V tomto období nastal i prvý zákrok proti hackerom, zatýkaním phreakerov a hackerov prostredníctvom FBI, jedným z nich bol i Kevin Mitnick. Obdobie je charakteristické počítačovými trestnými činmi bez vidiny zisku.

5.2 Obdobie rokov 1981 – 1994

12. 8. 1981 začína ďalšia etapa počítačovej kriminality a to uvedením počítača IBM PC. Bol prvým cenovo dostupným osobným počítačom a zvýšil sa i počet pripojených do systému BBS.

Cieľom zločinov sa stáva finančné obohatenie. V USA nastal boj proti hackerom s federálnym zákonom o počítačovom podvode a zneužití počítača, vydanom v 1986.

15. 1. 1990 spadla celoštátna telefónna sieť diaľkových hovorov v USA, obvinení boli neprávom hackeri. FBI začala operáciu Sundevil a zatýkala počítačových nadšencov nie zločincov. Hackeri sa cítili obmedzovaní, niektorým boli odnímané počítače. Situácia bola podnetom pre vznik Nadácie elektronického pohraničia, založenej Johnom Barlowom a Michaelom Kaporom. 12. 8. 1981 začína ďalšia etapa počítačovej kriminality a to uvedením počítača IBM PC. Bol prvým cenovo dostupným osobným počítačom a zvýšil sa i počet pripojených do systému BBS.

Cieľom zločinov sa stáva finančné obohatenie. V USA nastal boj proti hackerom s federálnym zákonom o počítačovom podvode a zneužití počítača, vydanom v 1986.

15. 1. 1990 spadla celoštátna telefónna sieť diaľkových hovorov v USA, obvinení boli neprávom hackeri. FBI začala operáciu Sundevil a zatýkala počítačových nadšencov nie zločincov. Hackeri sa cítili obmedzovaní, niektorým boli odnímané počítače. Situácia bola podnetom pre vznik Nadácie elektronického pohraničia, založenej Johnom Barlowom a Michaelom Kaporom.

5.3 Obdobie od roku 1994

V 90. rokoch sa počítače začali masovo šíriť osobné počítače i operačný systém Windows spoločnosti Microsoft. Internet sa v domácnostiach a kriminálnikov nadšencov vystriedali kriminálnici profesionáli. Dôležitým medzníkom je lúpež banky Citibank. Počas roka 1992 sa začal objavovať Warez.

Prvá zmienka o phishingu sa objavuje v roku 1995 v USA, kedy sa prvýkrát objavujú programy podporujúce phishing. Obeťami sa stali užívatelia America Online, kde phisher vydávajúci sa za administrátora America Online získaval prihlasovacie údaje užívateľov i údaje o ich platobných kartách.

V roku 1995 argentínsky hacker zistil heslá pre prístup do vládnych počítačov USA. Páchateľ bol zadržaný. O rok neskôr zamestnanec spoločnosti Intel skopíroval topografiu čipu Intel a odoslal ju konkurencii, ktorá ale páchateľa oznámila a súd ho odsúdil na 33 mesiacov nepodmienečne. V tomto roku bol prijatý i zákon Community Decency Act, ktorý obsahoval kontroverzné definície obscénneho a neslušného obsahu.

Ochranu autorských práv v súvislosti s informačnými a komunikačnými technológiami v USA upravil zákon Digital Millenium Copyright Act, prijatý v 1998. Absurdnými výkladmi kontroverzne obmedzoval užívateľa duševných práv.

Ďalším výrazným medzníkom bol rok 1999 a začiatok šírenia vírových hrozieb. Vírus s názvom Melissa. V roku 2000 ju nasledoval vírus v podobe milostného vyznania I love you. Prichádzajú série útokov proti svetoznámym portálom i elektronickým obchodom tzv. DoS útoky. Bol zostrojený i program na dekódovanie DVD. Objavuje sa i nová hrozba, program Napster, pre zdieľanie hudby v sieťach P2P, kde boli za dáta zodpovední užívatelia. Spoplatňovanie viedlo k jeho zániku.

V roku 2001 sa stali webové stránky spoločnosti Microsoft obeťou útoku, ktoré zneprístupnili stránky spoločnosti pre klientov na 2 dni. Šírila sa vlna vírusov prostredníctvom infikovaných príloh sľubujúcich fotky Anny Kurnikovovej. EÚ prijala Dohovor o počítačovej kriminalite.

Prvý phishing zameraný na internetové bankovníctvo a finančné inštitúcie sa objavuje až o osem rokov neskôr a to v roku 2003. Prostredníctvom červa bol v roku 2003 napadnutý bezpečnostný systém jadrovej elektrárne v Ohiu. V roku 2004 USA prijalo zákon, ktorý postihuje šíriteľov spamu. O rok neskôr získali hackeri údaje o účtoch niekoľkých amerických univerzít.

V 2006 hackeri napadli viacero vládnych počítačov v USA. Viac ako 1,5 milióna Američanov sa stalo obeťou krádeže identity. O rok neskôr bola Čína obvinená z hackerskych útokov sietí iných národov a predtým zo špionáže amerického vojenského systému. Obeťou hackerov sa stali i portál E-Bay, MySpace a Facebook. Kuriozitou o rok neskôr je i presmerovanie návštevníkov webovej stránky Baraca Obamu na stránky Hillary Clintonovej. V Kanade sa objavil návrh zákona proti kyberšikane.

Grécki hackeri v roku 2008 prenikli do jedného z počítačov urýchľovača častíc Európskej organizácie pre jadrový výskum aby poukázali na bezpečnostné trhliny. Smrť

speváka Michaela Jacksona, v roku 2009 využívajú počítačoví zločinci na rozosielanie spamu, prostredníctvom emailov i sociálnych sietí. Hackeri čoraz častejšie začali napádať sociálne siete, kradnúť heslá, fotky ale i šíriť vírusy za pomoci sociálnych sietí.

O rok neskôr hackeri získali prístup na serveri Európskej vesmírnej agentúry a ukradli citlivé údaje ako heslá. V roku 2011 boli pre účely šírenia spamu zneužitá kráľovská svadba. Počítačoví zločinci vytvorili i viacero falošných stránok týkajúcich sa Majstrovstiev sveta v hokeji 2011. Stránky sú v slovenskom a českom jazyku a rozširujú malware.

Počítačová kriminalita sa stále viac rozširuje. Zisky kriminálnikov v oblasti moderných technológií sa z roka na rok rozrastajú. Zločinci sa snažia využiť každú príležitosť, ktorá sa im naskytne. Nechávajú najímať podsvetím, stávajú sa členmi organizovaných skupín. Je potrebné posilniť boj proti počítačovej kriminalite bez obmedzovania základných ľudských práv a slobôd.

6 Situácia v Slovenskej republike

6.1 História počítačovej kriminality na Slovensku

V dostupnej literatúre sa nepodarilo nájsť opísanú históriu počítačovej kriminality na Slovensku. Spracovanie celej histórie by bolo nesmierne zložité a nad rámec tejto práce. Práve z tohto dôvodu sú v tejto kapitole vyhľadané a v časovom slede uvedené a stručné popísané najzávažnejšie prípady počítačovej kriminality v Slovenskej republike.

6.1.1 Konkrétne prípady počítačovej kriminality na Slovensku

- **One_Half**
  One_Half bol slovenský ničivý vírus z roku 1994. Jedná sa o polymorfný vírus, ktorý sa rozširoval v Európe a USA pod názvom Slovak Bomber. Napádal disk a šifroval dáta v prípade, že bol odstránený, dáta sa už nepodarilo rozšifrovať.
- **Prvá pomoc BSA**
  V novembri 1999 bol na Slovensku prvýkrát odsúdený softvérový pirát. Pri zadržaní páchateľa pomáhala Polícii SR BSA. Súd mu zabavil všetko vybavenie, ktoré používal na porušovanie autorských práv ako CD napaľovačky, všetky kópie a dostal pokutu 35 000 Sk. Ak by čiastku neuhradil, šiel by do väzenia.
- **Binary Division**
  Skupina slovenských hackerov pod názvom Binary Division v decembri 2000 napadla webové stránky Ministerstva vnútra ČR a Polície ČR. Obe stránky nezobrazovali informácie od inštitúcií ale výtvory hackerov. Útok bol vyvrcholením niekoľkých mesiacov napádania českých a slovenských webových stránok. Skupina napadla webové stránky politických strán Komunistickej strany Čiech a Moravy a Hnutia za demokratické Slovensko. Všetky stránky boli po napadnutí zmenené útočníkmi a obsahovali ich texty. Ukážky útokov tejto skupiny si môžete prehliadnuť v prílohách 1 a 2.
- **Útok na Inzine.sk**
  V roku 2001 sa stali obeťou hackerov internetový magazín Inzine.sk. Hacker, ktorý napadol internetový magazín sa podpísal ako Ježiško. Dôvodom napadnutia bolo, že stránka útočníka už dlhší čas rozčuľovala. Podľa jeho slov si splnil vianočné prianie. Celý text vytvorený útočníkom sa nachádza v prílohe 3.
- **Prvý uväznený pirát**

Na Slovensku bol prvý raz nepodmienečne odsúdený počítačový pirát v roku 2004. Súd udelil trest odňatia slobody na 10 mesiacov. Škoda spôsobená vlastníkom autorských práv týmto konaním bola približne vo výške 185 000 Sk. Jednalo sa o prípad prevádzkovateľa počítačovej herne, ktorý mal na počítačoch nainštalovaný nelegálny softvér, najmä hry.

- **Útok na NBÚ**

  Jednou z najväčších káuz počítačovej kriminality, ktorá mala i dlhú súdnu dohru bolo napadnutie Národného bezpečnostného úradu. V roku 2006 sa dvaja mladíci dostali na slabo zabezpečené servery NBÚ za pomoci jednoduchého prístupového hesla nbusr123, ktoré bolo uhádnuté za pomoci trójskeho koňa.

  Útočníci nezískali utajované údaje ale moc nad systémom, mohli jednať v mene najvyšších osôb z NBÚ napr. zasielaním emailov. Útok prebehol z desiatich IP adries, z toho jedna patrila serveru Stredného odborného učilišťa v Michalovciach. Ako jeden z páchateľov bol zadržaný administrátor školského servera. Argumentoval, že je administrátorom servera a preto nemá dôvod ho napádať. Druhý obvinený odmietol vypovedať pred súdom, cítil sa nevinný.

  Kvôli vytváraniu znaleckých posudkov trvalo vyšetrovanie kauzy až tri roky. Slovenskej polícii pomáhala s prípadom i FBI. Sám prokurátor, ktorý vzniesol obžalobu priznal, že útok bol preventívnym opatrením, ktoré upozornilo na veľké bezpečnostné medzery. Pre nedostatok dôkazov boli v októbri roku 2010 útočníci oslobodení, zatiaľ čo rok predtým boli odsúdení na ročný podmienečný trest odňatia slobody. Podľa verdiktu súdu nebolo dokázané, že skutok sa stal. Obvinení celý čas tvrdili, že sú nevinní a spoznali sa až na súde.

- **DoS útoky na Slovensku**

  Internetový portál slovenského denníka SME sa počas novembra 2007 stal obeťou útokov, ktoré spôsobili niekoľkohodinové výpadky.

  Na začiatku roka 2008 neznámi hackeri napadli i portál slovenskej televízie TA3. Portál TA3 sa stal terčom zahraničných hackerov, prostredníctvom DoS útokov, za účelom spôsobiť škody a znemožniť prístup užívateľom. IP adresy používané pre útok pochádzali z celého sveta od Európy až po Južnú Ameriku a Áziu.

- **Phishing na Slovensku**

  S marcom 2008 sa začal Slovenskom šíriť phishingový email. Údajne bol odosielaných Slovenskou sporiteľnou. Email obsahoval odkaz, po kliknutí naň

boli vyžadované údaje ako meno, priezvisko, číslo karty, PIN a iné údaje. Objavilo sa viacero variant emailu. Prvá verzia emailu bola v anglickom jazyku s odkazom na falošné stránky Slovenskej sporiteľne. O pár dní neskôr sa začal šíriť email v slovenskom jazyku. Oznamoval klientom blokáciu internetového bankovníctva a jeho potrebné obnovenie. Spomínané emaily sú súčasťou prílohy.

mesiac neskôr boli zaznamenané ďalšie podvodné emaily zamerané na klientov Dexia banky. Tieto emaily kvalitou značne zaostávali. Text bol nevydarene preložený do českého jazyka. Ak ste však klikli na odkaz falošnej webovej stránky, vyzerala veľmi dôveryhodne, problémom boli iba zavádzajúce názvy kolónok. Phishingové emaily a stránka sa nachádzajú v prílohách 4 – 6.

- **Hackeri a voľby**

  V roku 2009 bol napadnutý i web kandidátky na post prezidenta Zuzany Martinákovej. Neznámy hacker zmenil obsah na stránke a informoval o jej odstúpení. Tejto správe uverila dokonca i Tlačová agentúra SR. O pár dní neskôr bola napadnutá i stránka prezidenta Ivana Gašparoviča. Ukážky napadnutých stránok sú prílohami 7 a 8.

- **Igigi**

  S rokom 2009 prichádza postrach slovenských a českých webových stránok, vtedy ešte takmer neznámy hacker s prezývkou Igigi. Napadol viacero známych stránok, keďže sa väčšina portálov snažila jeho tvrdenia o napadnutí vyvrátiť alebo dokonca ututlať, hacker vytvoril blog, na ktorom zverejňoval čiastočné záznamy zo stránok a databáz, dokonca zašifrované heslá ako dôkazy svojich činov. Igigi je typickým príkladom gray hat hackerov.

  Prvou obeťou sa stala Československá filmová databáza, ďalšou obeťou boli stránka projektu výstavby nízkopodlažných bytových jednotiek pod názvom Račany, generátor českých eshopov Shoptet.cz a Rozzlobenimuzi.com. Igigi sa ale neuspokojil iba s pozornosťou slovenských, českých médií a obyvateľov. Napadol Rockyou.com odkiaľ získal 32 miliónov hesiel, čo je možné považovať za jeden z najväčších útokov na svete. Ďalej pokračoval stránkami: Orange.sk, Svetsluchatek.cz, Zoner.cz, Svadobneobrucky.com, Union.sk, Denik.cz, Atlas.sk, Aaaauto.cz, Games.tiscali.cz, Auto.cz a mnoho iných stránok.

  Rozruch ale opäť spôsobil prienikom na Azet.sk. Na začiatku roka 2010 zaútočil na portál Azet.sk odkiaľ získal zašifrované dáta z databáze portálu. Medzi

dátami boli údaje ako mená, emailové adresy, telefónne čísla, správy či dokonca fotografie a následne zverejnil ukážky dát s názvami databáz. Azet.sk dlho popieral prienik útočníka, hovoril, že žiadne dôležité údaje nezískal. Následne Igigi zverejnil heslá užívateľov.

Dodnes nikto netuší, kto je Igigi, mnohí sa však domnievajú, že pochádza zo Slovenska, najmä z dôvodu že pri zverejňovaní údajov prieniku na Denik.cz uviedol názov Denik.cz.

- **Červ Zimuse a útok na Apache**
  Na začiatku roka 2010 spoločnosť Eset varovala pred červom Zimunse. Bol vytvorený na Slovensku pre účel napadnutia počítačov motocyklového klubu na Liptove. Červ sa rozšíril zo Slovenska do celého sveta, napadol počítače USA, Thajsku, Španielsku, Taliansku či Česku. Rozširuje sa pomocou IQ test programu alebo ako samorozbaľovací balíček ZIP. Podobá sa na vírus One_Half.

  V apríli 2010 a sa uskutočnil útok na servery organizácie Apache Software Foundation. Hacker, ktorý servery napadol je údajne zo Slovenska, pretože útok bol spáchaný pod užívateľským menom Robert Fico a používal systémový nick hranol.

- **Rok 2011**
  Spoločnosť Slovak Telekom v januári tohto roku upozornila svojich klientov na phishingové emaily a SMS, ktorým sa majú vyvarovať. Útočníci sa pokúšali získať prihlasovacie mená a heslá.

6.1.2 Zhodnotenie

Zločinci na Slovensku nie sú až takí zákerní ako vo svete. Síce sa vyskytli prípady, ako vírus One_Half alebo červ Zimunse, ktoré napáchali množstvo škody na celom svete, no ani Zimunse nemal preniknúť do zahraničia.

Slovenskí hackeri, až na Igigiho, nespôsobujú veľké škody. Skôr sa pokúšajú takouto formou vyjadriť svoj politický, odborný alebo iný názor, prípadne sa snažia poukázať na bezpečnostné chyby. Veľké škody nechcel páchať ani Igigi, dôkazom toho je i ten fakt, že údaje, ktoré zverejňoval, boli nejakým spôsobom upravené, aby ich nemohol niekto iný zneužiť. Zverejňoval iba čiastočné výpisy databáz alebo výpisy niekoľkých zašifrovaných hesiel. Oznamoval skôr informácie, ktoré získal diagnostikou

ukradnutých dát ako napr. najčastejšie sa opakujúce heslá. Po jeho útokoch ostali bezpečnostné trhliny, ktoré mohli zneužiť iní útočníci.

Na Slovensku pôsobí viacero „dobrých“ hackerov, ktorí sa snažia zisťovať bezpečnostné trhliny a pomáhať spoločnostiam, rôznymi varovaniami a oznámeniami o chybách. Väčšina týchto spoločností nemá vôbec záujem zistené chyby opraviť, radšej sa obraňujú v médiách.

V boji proti hackerom zatiaľ Polícia SR a slovenské súdy nezaznamenali veľké úspechy. Jediným známym prípadom zadržaných hackerov je prípad napadnutia NBÚ. Údajní páchatelia boli zadržaní, tvrdili, že sú nevinní a súd im skutok nedokázal. Kto teda NBÚ napadol? Otázka s odstupom času bude už len ťažko zodpovedaná, vzhľadom k tomu, že elektronické stopy zmiznú za niekoľko sekúnd.

Najviac škody spôsobujú softvérový piráti, ktorí porušujú autorské práva najmä významných spoločností ako napr. Microsoft. V oblasti softvérového pirátstva sa darí i Polícii SR. Zachytení páchatelia sú zväčša odsúdení, či už na peňažný trest alebo trest odňatia slobody.

Phishing nie je na Slovensku práve častou formou počítačovej kriminality. Najmä z toho dôvodu, že slovenský jazyk je pre páchateľov veľmi zložitý. Aby bol takýto email účinný, mal by byť v rodnom jazyku, mnohým Slovákom je i dnes angličtina veľmi vzdialená. Podvodníci sa síce pokúsili o niekoľko takýchto podvodov, avšak iba s veľmi úbohým výsledkom.

Slovensko je síce malou krajinou, nie však počtom a kvalitou počítačových kriminálnikov. Zločinci sú podľa týchto prípadov pár krokov pred políciou i justíciou.

6.2 Zákony

Pre objasnenie situácie na Slovensku, sú v tejto kapitole opísané platné zákony, ktoré sa týkajú vybraných druhov počítačovej kriminality. Pre lepšiu orientáciu sú zo zákonov vybrané konkrétne odseky, ktoré sa k problematike vzťahujú.

6.2.1 § 247 Trestného zákona č. 300/2005 Z. z.

Paragraf 247 nesie názov Poškodenie a zneužitie záznamu na nosiči informácií. Je označovaný ako slovenský paragraf proti hackerom. Úplné znenie paragrafu sa nachádza v prílohe 9.

Prvý odsek hovorí o úmyselnom neoprávnenom získavaní informácií ich následnom zneužití, zničení. Zahŕňa i neoprávnené zasahovanie do počítača a funkčnosti počítačového systému za účelom podvodu. Druhý odsek pojednáva o neoprávnenom sledovaní elektronickej komunikácie alebo počítačového systému, zaobstaraní či poskytnutí prístupu k počítaču alebo programom, za účelom neoprávneného zásahu do počítača. Osoba, vykonávajúca niektorý z týchto činov si môže odpykať trest šesť mesiacov až tri roky väzenia.

Ak spomínané činy spôsobia značnú škodu môže páchateľovi súd udeliť trest jedného až piatich rokov väzenia. Škoda veľkého rozsahu alebo členstvo v skupine, môže páchateľa predchádzajúcich trestných činov stáť tri až osem rokov väzenia.

6.2.2 Autorský zákon č. 618/2003 Z. z.

Zákon upravuje ochranu autorských práv. Jeho porušovanie môže byť riešené občianskoprávnym konaním a trestnoprávnym konaním.

V občianskoprávnom konaní je osoba súdená podľa Občianskeho zákonníka č. 40/1964 Z. z.. Vinník musí vrátiť všetky nelegálne kópie a tak isto ich zmazať z počítača. Má povinnosť uhradiť škody, ktoré spôsobil svojim konaním a odovzdať všetky prostriedky, ktoré získal používaním nelegálnych kópií diela. Prípadne, môže dostať k náhrade i trovy konania.

V trestnoprávnom konaní je porušovateľ autorských práv súdený podľa Trestného zákona č. 300/2005 Z. z.. Konkrétne sa problematikou zaoberá § 283, ktorý nájdete v úplnom znení ako prílohou 10. Trest, za porušovanie autorských práv, môže súd udeliť až na dva roky, prípadne ak páchateľ spôsoby väčšiu škodu, závažnejším spôsobom konania, z osobitného motívu alebo prostredníctvom počítačového systému, hrozí mu šesť mesiacov až tri roky odňatia slobody. Za značné škody sa trest pohybuje od jedného roka až na päť rokov. V prípadne pôsobenia v skupine alebo spôsobenia veľkej škody môže byť páchateľ odsúdený na tria až osem rokov.

6.2.3 § 3 odsek 7 Zákona č. 147 /2001 Z. z. o reklame

Paragraf tri sa zaoberá všeobecnými podmienkami, ktoré musí spĺňať reklama. Odsek sedem je jedno z legislatívnych opatrení proti spamu. Hovorí, že odosielateľ musí mať pre účely zasielania reklamy formou emailov, telefaxu alebo automatického telefonického volacieho systému súhlas adresáta vopred. Podľa § 11, odseku 3 c) môže

porušovateľ tohto odseku dostať pokutu do výšky 2 000 000 Sk. Dozor vykonáva Slovenská obchodná inšpekcia. Tretí paragraf tohto zákona je prílohou 11 .

6.2.4 § 65 odsek 2 Zákona č. 610/2003 Z. z. o elektronických komunikáciách

Odsek zdôrazňuje potrebu súhlasu prijímateľa na posielanie marketingových správ formou SMS, emailov či faxov. Prijímateľ má právo na zrušenie súhlasu, preto musí správa obsahovať názov a adresu firmy, aby vedel prijímateľ zaslať žiadosť o zrušenie. Dohľad nad zákonom vykonáva Telekomunikačný úrad. Sankcia sa podľa odseku 5 e) pohybuje do výšky 1 000 000 Sk. Znenie celého paragrafu sa nachádza v prílohe 12.

6.2.5 § 4 odsek 6 Zákona č. 22/2004 Z. z. o elektronickom obchode

Podľa odseku šesť nesmie internetový obchod bez súhlasu zasielať zákazníkovi emaily. Dohľad vykonáva Slovenská obchodná inšpekcia. Paragraf je prílohou 13.

6.2.6 Zhodnotenie

Slovenské zákony dostatočne nepokrývajú oblasť kyberkriminality. Legislatíva nedostatočne pokrýva napr. problematiku spamu, za ktorý považuje iba nevyžiadanú elektronickú komunikáciu. Nepokrýva oblasť emailov šíriacich škodlivý softvér, či zbierania emailových adries. Taktiež sa nezaoberá ani phishingom a podvodmi páchanými prostredníctvom elektronickej komunikácie. Nezahŕňa trestanie šírenia škodlivého softvéru a jeho tvorby. Úspešné zahraničné zákony by mohli byť príkladom pri pokrývaní tejto oblasti.

6.3 Návrhy zákonov a zákony, riešiace počítačovú kriminalitu v iných krajinách

V tejto kapitole uvedieme niektoré zaujímavé návrhy zákonov a zákony, ktoré boli zostavené v iných krajinách na riešenie problému počítačovej kriminality. Sú dobrými i zápornými príkladmi, ktorým by sa mal slovenský legislatívny systém inšpirovať alebo vyhýbať.

6.3.1 Riešenie hackingu

6.3.1.1 Veľká Británia

V roku 2006 vznikol vo Veľkej Británii návrh na doplnenie Zákona o počítačovej kriminalite, tzv. Computer Misuse Act. Návrh bol zameraný na zakázanie hackerskych nástrojov. Zákon je zaujímavý tým, že pod jeho charakteristiku hackerskych nástrojov, spadajú i niektoré legálne programy. Tak by sa mohlo stať, že bude odsúdený človek, ktorý program používa na legálnu prácu a nie zločin. Zakazuje vytvorenie, vlastnenie a šírenie hackerských nástrojov.

Tento návrh zákona nie je jediný kontroverzný z britskej dielne. V roku 2009 sa objavuje zákon, ktorý bol schválený Radou ministrov EÚ. Polícii by týmto zákonom vzniklo právo vzdialene prehľadávať počítače útočníkov. Bolo by to možné i bez súdneho príkazu. V utajení môžu preniknúť do počítača a prehľadať disky. Do počítačov chcú vstupovať spôsobmi, ktoré používajú hackeri.

6.3.1.2 Zhodnotenie zákona

Zaujímavé zákony, ktoré ale svojou platnosťou prinesú viac komplikácií ako pomoci v boji proti kybernalite.

Po zverejnení návrhu vo VB uvažovala o podobnom zákone i SR. Ministerstvo vnútra SR ho ale vyhodnotilo ako neefektívny spôsob boja proti hackerom, ktorý sťaží a skomplikuje prácu všetkým administrátorom. Pod zákon totiž spadajú programy na obnovu hesiel alebo monitorovanie siete. Dokonca je možné, že by zákon spôsobil väčšie škody. Zatiaľ čo Ministerstvo financií, ktoré má na starosti informatizáciu na Slovensku podobný zákon chcelo prijať. Nakoniec sa v slovenských zákonoch podobné paragrafy neobjavili, dúfajme, že sa ani neobjavia.

Druhý návrh je veľmi amorálny. Človek má nárok na súkromie. Navyše zákon môže byť zneužitý, a tak je potrebné ho prísne regulovať. Užívatelia na Slovensku by neboli veľmi spokojní, ak by bol takýto zákon prijatý. Najmä z dôvodu rôznych prípadov, kedy verejní činitelia zneužívali svoje právomoci. Návrh je zlým príkladom postoja polície, nemala by sa znižovať na úroveň zločincov. Dáva tým nesprávny vzor napríklad teenagerom, ktorí sa pokúšajú hackovať. Môže jednoducho privodiť stav, kedy si užívatelia povedia: „Môžem to robiť tiež, aj polícia to robí.“ Zábavný je spôsob prevedenia, ktorým to chcú prevádzať. Vlastnými technikami útočníkov. Útočníci musia

byť dosť obozretní, pri tom čo robia, je otázne, či by podľahli tak jednoduchej pasci, ktorú sami vytvorili.

6.3.1.3 USA

Hackerom je každý, kto neoprávnene získa prístup k počítaču a informáciám. Ak skutkom získal viac ako 5 000 USD ročne, ak rozosiela niečo, čím je možné poškodiť počítače alebo používa získané informácie na vydieranie.

Zaujímavá je výška trestu za tieto skutky, ktorá môže v prípade najvyššieho trestu dosiahnuť 20 rokov pre recidivistu. Hackeri pokúšajúci sa útokmi zarobiť, môžu dostať trest až 5 rokov a 10 rokov za veľké škody. Pokuta je udelená podľa závažnosti činu.

6.3.1.4 Zhodnotenie zákona

Vyššie tresty, ktoré sú v USA, sú dobrým nápadom. Najmä z toho dôvodu, trestné činy v podobnej oblasti na Slovensku, nie sú zväčša páchané so zlým úmyslom a spôsobením veľkej škody, prípadne nie až takým ako vo svete. Skôr sa slovenskí hackeri pokúšajú sami sebe a iným dokazovať, ako sú dobrí. Prípadne poukazujú na chyby a vyjadrujú svoj názor. Myslím si, že takíto hackeri by si dvakrát rozmysleli páchanie podobných trestných činov, ak by im za opakované chytenie hrozilo 20 rokov. Možno to znie ako obhajoba hackerov, ale zatiaľ sa na Slovensku nestalo, aby náš hacker napadol napr. jadrovú elektráreň a žiadal za to výkupné. No možno je iba otázkou času, kedy sa slovenskí hackeri nechajú na podobné útoky najímať podsvetím.

6.3.1.5 Návrh pre Slovensko

V tejto oblasti je návrhom pre Slovensko, skôr sprísnenie trestov. Sme malou krajinou, ktorú by podobné výstrelky ako v Británii vyšli veľmi draho a zároveň by nemali žiaden pozitívny efekt. Bol by to zákon, ktorý by nemal kto prevádzať. Nemáme totiž špecializovanú jednotku, ktorá by mala podobné schopnosti a dokázala by napádať počítače útočníkov a ešte bez toho, aby na to prišli.

6.3.2 Riešenie softvérového pirátstva

6.3.2.1 Francúzsko

Prvým príkladom zaujímavého zákona riešiaceho problém softvérového pirátstva je kontroverzný zákon vo Francúzsku, ktorý bol platný v roku 2009. Platnosť zákona umožňovala, odpájať počítačových pirátov od internetu.

Hlavnou myšlienkou zákona je uplatnenie pravidla trikrát a dosť v oblasti počítačového pirátstva a porušovania autorských práv. Osoby, dopúšťajúce sa tohto zločinu, sú prvý a druhýkrát upozornené emailom na svoje nelegálne konanie, od poskytovateľa internetového pripojenia. V prípade, že po varovaní neprestanú vykonávať činnosti, ktorými porušujú autorské práva a spoločnosti, ktoré ich vlastnia majú podozrenie, môžu byť piráti odpojení od internetu až na dobu 12 mesiacov. Dohľad nad zákonom vykonával orgán HADOPI - Úrad pre distribúciu diel a ochranu práv na internete.

6.3.2.2 Zhodnotenie zákona

Zákon je pre Slovensko nevhodným príkladom protipirátskej legislatívy z viacerých dôvodov.

Prvým nedostatkom bolo potláčanie prezumpcie neviny. Osoba mohla byť odpojená od internetového pripojenia bez rozhodnutia súdu. V prípade, že úrad získal podozrenie, osoba bola okamžite odpojená bez toho, aby jej úrad pred súdom dokázal sťahovanie a používanie nelegálneho softvéru, filmov či hudby, chránených autorskými právami.

Ďalším veľmi závažným nedostatkom bolo porušovanie ľudských práv a osobných slobôd. Zákon sa dostal do kolízie s legislatívou Európskej únie. Internet je zdrojom mnohých informácií, ktoré sú pre náš každodenný život nevyhnutné a každá osoba má právo na prístup k týmto informáciám.

Zlou stránkou zákona je i jeho dopad na obyčajných užívateľov. Takýto zákon neodstraší pirátov, ktorí si stále hľadajú spôsob ako obchádzať zákon a spôsobujú väčšinu škôd spoločnostiam, chrániacim autorské práva. Skôr vystraší obyčajných užívateľov, ktorí sa zväčša dopúšťajú drobných porušení a najmä nevedome. Menej skúsení užívatelia sa môžu dokonca báť návštevy internetu, z dôvodu, že nevedome a nechcene, nejakým spôsobom porušia autorské práva.

6.3.2.3 Švédsko

Švédsko je ďalšou z krajín, ktorá prijala veľmi kontroverzný zákon. Po prijatí zákona sú poskytovatelia internetových služieb povinní odovzdávať informácie o svojich zákazníkoch, porušujúcich autorské práva, majiteľom autorských práv. Zákon vznikol ako reakcia na európsku smernicu s názvom IPRED.

Na kontroverzný zákon poskytovatelia internetového pripojenia vo Švédsku reagovali ochranou svojich zákazníkov tak, že prestali zhromažďovať údaje o svojich klientoch, ich IP adresách a navštevovaných stránkach.

6.3.2.4 Zhodnotenie zákona

Zákon je veľmi nevydareným príkladom zákona z pohľadu Švédska. Nie z dôvodu, že by hlavná myšlienka zákona bola zlá. Problém v prípade zákona bol predpoklad, že poskytovatelia internetového pripojenia budú o svojich klientoch zaznamenávať údaje i bez zákona, ktorý by im túto povinnosť predkladal.

Namiesto pomoci v chytaní páchateľov skomplikoval zákon život švédskej polícii. Keďže poskytovatelia internetového pripojenia neuchovávajú tieto potrebné údaje o zákazníkoch, polícia nemá možnosť vypátrať ani páchateľov veľkých trestných činov.

6.3.2.5 Návrh pre Slovenskú republiku

Najvhodnejším zákonom pre Slovenskú republiku by bol podobný zákon ako vo Švédsku. Síce zákon v tejto krajine neplní svoju úlohu tak ako má, na Slovensku by s niektorými úpravami mohol fungovať správne.

Slovenská republika má v Zákone č. 610/2003 o elektronických komunikáciách ošetrené uchovávanie údajov o elektronickej komunikácii. Poskytovatelia internetových služieb sú povinní uchovávať údaje o elektronickej komunikácii po dobu 6 mesiacov, ak sa jedná o komunikáciu, počas pripojenia k internetu, internetovú elektronickú poštu a telefonovanie prostredníctvom internetu. Na požiadanie je poskytovateľ povinný tieto údaje vydať orgánom SR.

Práve v tom by spočívala navrhnutá modifikácia zákona. Mnohí ľudia nedôverujú spoločnostiam, ktoré vlastnia autorské práva. Snažia sa totiž uchrániť svoj majetok za každú cenu. Z pohľadu bežných užívateľov by sa mohla naskytnúť i otázka dôvernosti údajov. Údaje, ktoré je povinný poskytovateľ internetového pripojenia

uchovávať, sú viazané telekomunikačným tajomstvom a môžu byť vydané iba orgánom SR. Tým sa obmedzuje moc, ktorá bola daná firmám vo Švédsku. Spoločnosti by museli o údaje potrebné na chytenie páchateľa žiadať od kompetentných orgánov, ktoré by uznali, či je vhodné ich vydanie iným osobám. Prípadne by začali konať orgány a snažili sa páchateľa zachytiť.

Zároveň by bolo dobrým riešením a preventívnym opatrením, ak by spoločnosti, vlastniace autorské práva, museli svoje diela chrániť určitým obranným mechanizmom proti kopírovaniu. Ak by tak neučinili mohli by im byť udelená pokuta, prípadne iný postih.

6.3.3 Riešenie malwaru

Malware je z vybraných druhov najhoršie riešiteľný. Niekoľko krajín prijalo zákon proti škodlivému, skôr sú to stručné odseky zákonov. No ani jeden z nich nezaznamenal významný úspech. Odborníci tvrdia, že táto oblasť nie je zákonom riešiteľná. Zatiaľ sa dá s týmto výrokom súhlasiť. Ak náhodou krajina príjme podobný zákon, odosielatelia škodlivého softvéru sa iba presťahujú do inej krajiny, odkiaľ začnú šíriť škodlivé programy znovu.

6.3.3.1 USA

Priekopníkom v tejto legislatívnej oblasti sú Spojené štáty. Jedná sa o zákon s názvom Spy Act, ktorý bol prijatý v roku 2004. Zákon hovorí, že programy nesmú počítač ovládať alebo modifikovať rôzne nastavenia. Za porušenie zákona hrozí pokuta 3 000 000 USD, prípadne väzenie. Zákon je primárne určený proti spywaru.

6.3.3.2 Zhodnotenie zákona

Ohodnotiť tento druh zákonov je veľmi zložité. Budú prechádzať ešte rôznymi zmenami, ktoré budú reakciami na stále nové nebezpečné programy. Možno ak všetky krajiny príjmu podobné zákony a ich odosielatelia nebudú môcť utekať do iných krajín. Ale budú nútený posielať malware pod hrozbou trestu alebo s tým prestať, tak možno podobný zákon zaznamená pozitívnejšie ohlasy.

6.3.3.3 Riešenie pre Slovensko

Pri tomto druhu počítačovej kriminality považujem za rozumnejšie preventívne opatrenia, spočívajúce v učení zodpovednosti a bezpečnosti slovenských užívateľov.

Legislatívnym opatrením proti škodlivému softvéru by mohol byť doplnený paragraf trestného zákonníka s vysvetlením pojmu, a určením peňažného trestu a väzenia. Zlým nápadom by bolo vytvárať, samostatné, siahodlhé zákony, ktoré by boli zbytočne drahé, ale nepriniesli by žiaden účinok.

6.3.4 Riešenie spamu

6.3.4.1 USA

V Spojených štátoch bol roku 2003 prijatý zákon pod názvom Can Spam Act. Spam je podľa zákona považovaný za nákladný, keďže používatelia elektronickej pošty sa musia voči nemu určitým spôsobom brániť, prípadne vynakladať úsilie na jeho odlišovanie a odstraňovanie. Často je spájané s nelegálnym obsahom, znižuje komfort elektronickej pošty.

Zákon spam opisuje ako zámerne zasielané emaily, častokrát zavádzajúce. Zaujímavosťou zákona je, že nezakazuje len zasielanie spamu ale aj zbieranie, získavanie a náhodné generovanie emailových adries. Teda trestným činom podľa zákona je, ak spameri, pre účely rozosielania nevyžiadanej pošty vyhľadávajú a zhromažďujú emailové adresy. Tieto emailové adresy sú získavané z webových stránok a rôznych diskusných fór. Za zločin sa považuje i skrývanie identity odosielateľa a úmyselná zmena údajov, ako napr. hlavičky emailu.

Emaily môžu byť zasielané, iba ak je poskytnutý súhlas adresáta, aby mohla byť získaná adresa presunutá do inej firmy, je potrebný ďalší súhlas. Komerčné emaily musia byť označené ako propagácia produktu, služby. Zákon ale spomína, že spam nie je používaný len ako propagácia ale i na rozosielanie škodlivého softvéru najmä rôznych trójskych koňov a červov.

Zákon uvádza tresty podľa závažnosti získaného zisku a spôsobených škôd. Páchateľom môže byť uložená pokuta, trest odňatia slobody či prepadnutie majetku nadobudnutého s pomocou páchania trestnej činnosti.

Po vzore amerického zákona sa vydalo i Nemecko. Už o rok neskôr, v roku 2004, bol predložený návrh antispamového zákona, ktorý spamerom ukladal nielen finančné tresty ale i tresty odňatia slobody. Taktiež upravoval ako trestný čin i zber emailových adries. Návrh zákona nebol prijatý.

6.3.4.2 Zhodnotenie zákona

Zákon je veľmi dobrým príkladom pre ostatné krajiny. Ošetroval ako prvý na svete niektoré dôležité skutočnosti. Zbieranie a získavanie adries je potrebné označiť za trestný čin a stíhať ho. Veľmi prínosné je i udeľovanie trestu odňatia slobody za spam. V mnohých krajinách sa ho totiž dopúšťajú firmy pri rozosielaní reklamy. Podľa zákona im hrozí pokuta, ak majú dostatočný zisk, tak ich to vôbec netrápi. Väzenie by mohlo byť lepšou motiváciou pre skoncovanie s rozosielaním spamu.

6.3.4.3 Návrh pre Slovensko

Na Slovensku je spam riešený prostredníctvom niekoľkých odsekov v rôznych zákonoch. Dohľad nad týmito zákonmi v dvoch prípadoch vykonáva Slovenská obchodná inšpekcia a Telekomunikačný úrad. Slovenskí občania sú zmätení, nevedia na koho sa v prípade oznámenia spamu majú obrátiť.

V prvom rade je potrebné vytvoriť kvalitný antispamový zákon, ktorý by sa mal zameriavať nielen na nevyžiadanú obchodnú komunikáciu. Mal by za spam považovať i masovo rozosielanú elektronickú poštu obsahujúcu rôzny škodlivý softvér.

Zavádzal by prísnejšie tresty. Z hľadiska finančných pokút sú terajšie tresty dostatočné, najvyššia možná čiastka je 2 000 000 Sk. Je potrebné tieto pokuty zjednotiť, pretože v každom zákone s a odlišujú.

Dôležitým krokom je ustanovenie dozorujúceho orgánu, ktorý by bol iba jeden. Riešil by všetky sťažnosti podávané ľuďmi. Prostredníctvom prevenčných projektov a inými spôsobmi, napr. prostredníctvom Internetu, by malo byť upozornené na aký orgán sa majú obyvatelia SR obrátiť, v prípade, že dostávajú spam.

Na stránkach orgánu by sa mal nachádzať jednoduchý nahlasovací formulár, ktorý by obsahoval všetky potrebné údaje na podanie oznámenia. V prípade, že by úrad udelil firmám pokutu, pôsobilo by to preventívne.

6.3.5 Riešenie phishingu

6.3.5.1 USA

Zákon HR 1731 vydaný v roku 2004. Zaoberá sa krádežou identity. Mnoho páchateľov sa i po prijatí tohto zákona v USA nepodarilo chytiť. Trest páchateľa krádeže identity bol 3 roky. Neskôr boli zákony v Spojených štátoch novelizované

a trest zvýšený na 5 rokov v súvislosti ak sa jedná o zneužitie identity v súvislosti s terorizmom. Phishing je metódou, pri ktorej je krádež identity získaná podvodom, takže páchateľ je obvinený nielen z krádeže identity, ale aj emailového podvodu a páchateľ si môže trest predĺžiť o 2 roky.

6.3.5.2 Zhodnotenie zákona

Spojené štáty majú s touto problematikou asi najväčšie skúsenosti zo všetkých krajín. Preto je ich riešenie problematiky prínosné. V tejto oblasti neočakávame prelomové riešenia. Mnoho krajín túto oblasť nemá vôbec ošetrenú.

6.3.5.3 Riešenia pre Slovensko

Riešenie problému je možné prostredníctvom prevencie, ktorá by naučila ľudí, ako si všimnúť phishingový podvod a vyvarovať sa mu. Zákony sú síce možným riešením najmä v podobe prísnejších trestov, no nedokážu zabrániť robiť chyby obyčajným ľudom. Dobrým nápadom je spojenie trestov za krádež identity a podvodu prostredníctvom emailu. Na Slovensku nie je phishing veľmi rozšírený a zväčša prichádza zo zahraničia, čo by znamenalo, že aj tak by nepodliehal slovenským zákonom.

6.4 Inštitúcie a združenia bojujúce proti počítačovej kriminalite na Slovensku

Nasledovné inštitúcie a združenia pôsobia na Slovensku najmä preventívnymi programami, zameriavanými na všetky vekové kategórie. Je veľmi dôležité vzdelávať, zvyšovať povedomie o moderných technológiách a zločinoch. Práve túto úlohu plnia Ministerstvo vnútra SR, Polícia SR ale najmä občianske združenie eSlovensko.

BSA a Polícia SR sú aktívne vo vyšetrovaní trestných činov, hľadaní páchateľov a pri dokazovaní ich viny pred súdom.

6.4.1 Ministerstvo vnútra SR a Polícia SR

Ministerstvo vnútra je poverené ochranou verejného poriadku a bezpečnosti majetku a osôb. Pod jeho správu patrí i Polícia SR. Obe inštitúcie sú štátne, majú povinnosť bojovať proti počítačovej kriminalite a zároveň ich zamestnanci majú právomoci verejného činiteľa.

Obe inštitúcie bojujú proti kriminalita aj prostredníctvom prevenčných programov. Za prevenciu považujú: *„vedecky zdôvodnené, cieľavedomé, zámerné, plánovité a koordinované pôsobenie na príčiny a podmienky kriminality s cieľom predísť im, odstrániť ich, alebo ich vhodnými formami a metódami pôsobenia aspoň sčasti eliminovať, prípadne ich negatívne prejavy obmedziť a súčasne podporovať vytváranie podmienok antikriminogénnych“*.

Konkrétne pre oblasť prevencie je zriadený odbor komunikácie a prevencie Polície SR. Odbor zabezpečuje mediálnu stratégiu Policajného zboru, informačný servis, organizuje tlačové besedy a stretnutia, rozpracováva koncepciu prevencie kriminality, v prevencii kriminality koordinuje útvary ministerstva celky polície.

Najväčším projektom, ktorý spolu vytvorilo Ministerstvo vnútra SR a Polícia SR na podporu prevencie počítačovej kriminality je Zodpovedne.sk. BSA spolupracuje s Políciou SR pri hľadaní softvérových pirátov, pretože ako združenie má obmedzené právomoci.

6.4.2 Telekomunikačný úrad

Telekomunikačný úrad sa zaoberá cenovou i národnou reguláciou elektronických komunikácií, rozvojom európskeho trhu a ochranou užívateľov. Úrad je štátnou inštitúciou a vedie ho predseda menovaný a odvolávaný NR SR. V súčasnej dobe je ním Ing. Ladislav Mikuš.

Financovanie úradu je plne pokryté prostriedkami získanými Zákonom o elektronických komunikáciách.

Úrad prevádza nasledovné činnosti dané zákonom:

- reguláciu elektronických komunikácií,
- zabezpečuje medzinárodné vzťahy v tejto oblasti,
- spolupracuje s Ministerstvom dopravy, pôšt a telekomunikácii SR a zabezpečuje informačné povinnosti NRSR a Európskej komisie,
- ochraňuje koncových užívateľov a poskytuje im potrebné informácie,
- podporuje rozvoj spoločného trhu ÉU,
- vydáva právne predpisy a vestník,
- vykonáva dohľad a ukladá sankcie.

Posledný bod je veľmi dôležitý, pretože ak sa stanete obeťou nevyžiadanej pošty, dohliadajúcim úradom na Slovensku, na ktorý je potrebné sa obrátiť, je Telekomunikačný úrad SR.

6.4.3 Business Software Alliance (BSA)

Neziskové profesijné združenie pôsobiace vo viac ako 80 krajinách na svete. Organizácia má centrálu vo Washingtone DC a pobočky v ďalších 11 mestách, medzi ktoré patrí napr. Brusel, Londýn, Mníchov, Tokio. Cieľom združenia je podporovať firmy zaoberajúce hardvérom a softvérom. BSA je súkromnou organizáciou, jej zamestnanci nemajú právomoc verejného činiteľa, práve preto spolupracuje pri zadržiavaní softvérových pirátov s Políciou SR.

Slovenská pobočka BSA bola založená v apríli 1997. Kvôli právnej forme BSA SR bola v roku 2007 zlikvidovaná. Aktivity združenia však pretrvávajú. Naďalej funguje webová stránka organizácie s informáciami a možnosťou nahlásenia používania nelegálneho softvéru.

BSA sa zaoberá podporou stabilného legislatívneho prostredia softvérového priemyslu, inovácie, rozvoja a konkurencieschopnosti trhu softvéru a technológií. Bojuje proti pirátstvu a za najúčinnejší spôsob dodržiavania autorských práv považuje o informovanie o dôsledkoch porušovania. Jej členmi sú spoločnosti ako Apple, Microsoft, Intel, Dell, Adobe a mnoho iných.

Politika verejného záujmu BSA sa zameriava na nasledovné priority, ktoré sú rozhodujúce pre softvérový priemysel:

- ochrana duševného vlastníctva,
- otváranie trhov bezbariérovému obchodovaniu,
- dátová bezpečnosť,
- rast príležitostí na rozvíjajúcich sa trhoch,
- softvérová inovácia a voľba,
- E-governement,
- pracovná sila a vzdelávanie.

Vymenované priority sú podporované výskumom, štúdiami, verejnými podujatiami a mediálnym pôsobením. BSA sa sústredí na podnety, ktoré sú nielen od

rôznych orgánov, organizácií ale i samotných užívateľov a prostredníctvom moderných technológií sa snaží odhaľovať pirátov.

Webová stránka združenia obsahuje možnosť ohlásiť softvérové pirátstvo. Ohlásenie je dôverné a možné prostredníctvom telefonátu alebo emailu. Ponúka i možnosť prezerania štatistík, prieskumov, aktivít združenia, rôzne varianty členstva a ich popis.

6.4.4 eSlovensko

eSlovensko je občianskym združením pre informatizáciu Slovenska. Podnetom pre vznik združenia bol nástup počítačov. Združenie vznikalo so snahou venovať sa rozvoju inovácií a nových technológií. Je súkromnou osobou, ktorá pôsobí v oblasti počítačovej kriminality iba preventívne.

V začiatkoch fungovania sa eSlovensko zameralo svojimi projektmi na robotechnológie a softvérové projekty. V roku 1991 bolo založené Inovačné centrum so sídlom v bratislavskej Mlynskej doline.

Od roku 2002 je eSlovensko mimovládnou, neziskovou organizáciou. Iniciuje, pripravuje a podieľa sa na mnohých projektoch v oblasti informatizácie a informačných a komunikačných technológií ako: eGovernement, eInklúzia, eTurizmus, eBezpečnosť, Zodpovedne.sk a Ovce.sk. Viacero projektov združenia je zameraných na používanie informačných technológií vo verejnej správe.

Organizácia má za sebou i podporu veľkých spoločností, medzi ktoré patri Eset, O2, Sanet, Microsoft či Slovak Telecom.

Združenie sa snaží vzdelávať slovenských občanov všetkých vekových kategórií a viesť ich k bezpečnému a zodpovednému používaniu moderných informačných technológií. Najmä vďaka iniciatíve a myšlienke organizácie vznikol projekt Ovce.sk, ktorý je slovenským vzdelávacím programom prevencie nebezpečenstva číhajúceho na internete. Projekt v súčasnosti rozšíril svoju pôsobnosť a stal sa medzinárodným.

6.5 Prevencia počítačovej kriminality na Slovensku

Veľmi dôležitým spôsobom boja proti počítačovej kriminalite je prevencia, v rámci ktorej sú občania oboznámení s nástrahami, ktoré na nich číhajú pri používaní informačných a komunikačných technológií. Preto je potrebné vytvárať projekty na

prevenciu, v rámci ktorých sa bude zvyšovať povedomie obyvateľov, aby sa kvôli nevedomosti nestávali terčom počítačovej kriminality. V tejto kapitole sú vymenované a popísané konkrétne projekty prevencie počítačovej kriminality na Slovensku.

6.5.1 Zodpovedne.sk

Slovensko je ako člen Európskej únie zapájaný do projektov prevencie. Jeden z týchto projektov nesie názov Zodpovedne.sk. a je súčasťou komunitárneho programu Safer Internet plus Európskej únie. Projekt je zastrešovaný Ministerstvom vnútra Slovenskej republiky, Políciou Slovenskej republiky, občianskym združením eSlovensko a jeho cieľom je zvýšiť povedomie detí, mládeže, rodičov i učiteľov tak, aby využívali internet zodpovedne, bezpečne a zbytočne sa nevystavovali nebezpečenstvu.

Spolu s projektom sa spája i poradenská linka pod názvom pomoc.sk, televízny program Cookie.sk a linka slúžiaca na nahlasovanie nezákonného obsahu na internete stopline.sk. Začiatok kampane projektu Zodpovedne.sk bol podporený i spotom v Slovenskej televízii.

Projekt začal v auguste roku 2007, odvtedy poskytuje mnoho cenných rád pre všetky vekové kategórie občanov a v rámci projektu sa konajú i rôzne podujatia, školenia a stretnutia. Na projekt finančnými čiastkami prispeli Ministerstvo vnútra Slovenskej republiky, občianske združenie eSlovensko, Európska únia i sponzori komerčného sektora ako napr. spoločnosť Slovak Telekom, a. s.

Informuje o viacerých oblastiach ohrozenia na internete ako napr.: pedofília, pornografia, šikanovanie, poskytovanie osobných údajov a mnoho iných. Ďalej sa zaoberá prostriedkami ohrozenia ako napríklad spam, malware či sťahovanie.

Na stránkach projektu sa nachádza mnoho zaujímavých a náučných materiálov, videoklipov, príbehov i testov. Do Zodpovedne.sk sa zapojilo 50 informatikov pracujúcich v samospráve a 84 príslušníkov policajného zboru zameriavajúcich sa na prevenciu.

Prečo práve tento projekt? Hlavnú myšlienku vyjadruje už spomínaný spot vysielaný v Slovenskej televízii pod názvom Kde je Miro?, ktorý bol prevzatý z Nemecka v rámci programu Safer Internet plus. Spot upozorňuje rodičov na skutočnosť, že v reálnom živote kladú väčší dôraz na bezpečnosť svojich detí ako vo

svete virtuálnom. Ak by ich dieťa robilo to, čo robí na internete, keď si píše s neznámymi ľuďmi, zverejňuje svoje fotografie či osobné údaje v reálnom živote, rázne by zakročili ale mnohokrát ani netušia, že ich ratolesti sa ženú svojím nebezpečným konaním vo virtuálnom svete v ústrety zločinu.

6.5.2 Pomoc.sk

Pomoc.sk je slovenskou verziou združenej linky pomoci a rovnaké linky má väčšina členských štátov EÚ. Linka je súčasťou projektu Zodpovedne.sk a bola založená za účelom pomoci a poradenstva Slovenským občanom pri bezpečnom a zodpovednom používaní informačných a komunikačných technológií a internetu. K linke projektu Zodpovedne.sk bola pridružená i Linka detskej istoty od Unicefu, zlúčením vznikla linka Pomoc.sk.

Linka funguje v troch podobách a to ako:

- telefónna linka, ktorá je dostupná nonstop,
- live chat s operátorom, každý deň v dobe od 16:00 do 22:00 a
- konzultácií pomocou emailu.

6.5.3 Stopline.sk

Projekt Stopline.sk bojuje proti nezákonnému obsahu, zneužívaniu detí, rasizmu, xenofóbii a iným trestným činnom na Internete. Súčasťou projektu je vytvorenie a prevádzkovanie centra pre nahlasovanie nezákonného obsahu a činností na internete a členstvo centra v medzinárodnej siete INHOPE. Projekt je spolufinancovaný EÚ.

Hlavnými piliermi projektu sú: prístupnosť, nestrannosť, anonymita, efektivita, medzinárodná sieť, odbornosť a prevencia.

6.5.4 Cookie.sk

Cookie.sk je televízna relácia, ktorá pozostáva z deviatich 15 minútových častí. Moderuje ju Andrea Kerestešová, známa slovenská herečka a v každej časti účinkujú reálni mladí ľudia i počítačoví odborníci. Všetky časti boli odvysielané vo verejnoprávnych televíziách STV1 a STV2 a sú dostupné celkovo na piatich portáloch medzi ktorými sa nachádza i Youtube.com a Stream.cz.

6.5.5 Ovce.sk

Ovce.sk je ďalším z projektov na Slovensku s finančnou podporou Európskej únie v rámci programu Safer Internet. S hlavným podnetom pre vznik projektu prišlo občianske združenie eSlovensko. Na projekte sa podieľajú i DAFNE, Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Rada vlády SR pre prevenciu kriminality, Unicef, spoločnosť Slovak Telecom, detský časopis Maxík, portál Pokec a mnoho iných.

Projekt je zameraný na bezpečné a zodpovedné používanie informačných a komunikačných technológií a výchovu bezpečnejšieho pohybu v novom sociálnom prostredí vytvorenom modernými technológiami. Hlavnými cieľmi projektu je naučiť deti:

- kriticky myslieť pri používaní informačných a komunikačných technológií,
- chrániť sa pred hrozbami moderných technológií
- etike internetu.

Projekt bol vytvorený v hravej forme animovaného seriálu a komiksu a vo februári tohto roku bol rozšírený na medzinárodnú úroveň. Každá časť rozprávky sa spája s iným nebezpečenstvom číhajúcim prostredníctvom moderných technológií a nachádza sa na stránkach projektu v rôznych jazykoch i posunkovej reči. Hlavnými postavičkami sú pubertiak Jano, múdry Bača, Horár, ovečky a samozrejme nebezpečný vlk čakajúci na svoju príležitosť. Prvá časť bola uvedená 8. októbra 2009 a najnovšie diely by mali byť uvedené do konca roku 2011.

Webová stránka ponúka i množstvo materiálov na stiahnutie ako napr.: maľovanky, tapety, šetrič obrazovky, zvučka, zvonenie mobilu, príručku pre rodičov a učiteľov a mnohé iné materiály. Príručky pomáhajú pochopiť hlavnú náplň projektu ale i to, ako by mali rodičia postupovať pri pozeraní týchto rozprávok, aby bol projekt účinný. Projekt zaznamenal i viacero ocenení, jedným z prvých bola výhra 1. Miest na Slovensku v rámci Európskej ceny za prevenciu kriminality. Dabingom projekt podporili osobnosti ako: Jozef Vajda, Csongor Kassai, Rytmus, Rok Terkaj, Tamir Gostiša. Ukážky postavičiek, letáku a komiksu sa nachádzajú v prílohách 14 – 16.

6.6 Zhodnotenie situácie na Slovensku

Zo všetkých získaných informácií je možné zodpovedať otázky položené na začiatku práce.

Aká je súčasná situácia ohľadne vybraných druhov počítačovej kriminality a celkovo na Slovensku?

Zistiť momentálnu situáciu ohľadne kybernetickej kriminality na Slovensku je zložité. Dôkazom je i neúspešný pokus o získanie potrebných štatistických údajov počítačovej kriminality. Z dôvodu písania práce bola na Ministerstvo vnútra Slovenskej republiky i Štatistický úrad SR vznesená žiadosť o zaslanie štatistík počítačovej kriminality v SR. Ministerstvo žiadosť z dôvodu nedostupnosti informácií postúpilo Prezídiu policajného zboru.

Polícia SR má na svojich webových stránkach uvedených viacero štatistík kriminality, žiadna z nich ale konkrétne neodzrkadľuje stav počítačovej kriminality na Slovensku. Po následnej viacnásobnej komunikácii s Prezídiom a oboznámení s údajmi, ktoré sú požadované, boli od Prezídia zaslané štatistiky, ktoré ale vôbec nezodpovedali požadovaným informáciám a ani informáciám týkajúcim sa počítačovej kriminality.

Teda občan SR, ak aj prejaví záujem, nemá šancu sa dozvedieť aký je napr. podiel počítačovej kriminality na celkovej kriminalite na Slovensku, či celkovú úspešnosť riešenia prípadov v tejto oblasti. Azda jedinými prípadmi publikovania a dostupnosti informácií o počítačovej kriminalite sú správy BSA, v ktorých je uvedená miera softvérového pirátstva.

Ako sme už na začiatku spomínali, každá krajina sa spolu s počítačovou kriminalitou potýka i s problémami, ktoré prináša. Legislatívny problém nie je možné na Slovensku vyvrátiť. Prvým jeho výrazným dôkazom jeho existencie je ratifikácia Dohovoru o počítačovej kriminalite. Dohovor bol vytvorený v roku 2001 a SR sa stala členom EÚ v roku 2004, avšak dohovor bol ratifikovaný až o tri roky neskôr v roku 2007.

Problém polície a justície je na Slovensku znateľný. Polícia nemá dostatočný počet odborníkov, ktorí by boli schopní zaistiť dostatočne rýchlo a kvalitne stopy počítačových zločinov. Tieto stopy sú následne potrebné pri dokazovaní trestných činov pri súdnom procese. Nedostatok a nekvalita stôp znemožňujú potrestanie vinníkov.

Dôkazom je proces s hackermi NBÚ. Polícia určila údajných páchateľov, prokurátor vzniesol obžalobu. Slovenské orgány neboli schopné dodať dostatok dôkazov pre odsúdenie. Z tohto pohľadu považujem za problematickú situáciu Polície SR.

Problém spoločnosti a jej benevolentnejšieho prístupu k počítačovej kriminalite je i problém bezpečnosti. Ľudia príliš dôverujú počítačom a málo dbajú na bezpečnosť pri používaní počítača. Na Slovensku v posledných rokoch prebehlo viacero preventívnych projektov, ktoré položili základy bezpečne práce s počítačmi. Malo by byť v tejto oblasti viac projektov, ktoré by posilňovali základné vedomosti obyvateľov Slovenska o počítačovej bezpečnosti.

Problém hrozby je na Slovensku veľmi veľký. Na Slovensku bolo za posledné roky napadnutých mnoho spoločností. Hrozby prichádzajú zo Slovenska i zahraničia. Obeťami sa stali významné média ako denník Sme.sk, spravodajská televízia TA3, portál Azet.sk. Útočníci sa nevyhli ani takým inštitúciám ako sú banky. Menovite Slovenská sporiteľňa a Dexia banka.

Slovenská republika má niektoré zákony, paragrafy, ktoré ešte v niektorých krajinách nie sú prijaté ani dnes. Neprijíma v tejto oblasti zbytočné zákony, ktoré by komplikovali život. Neprijíma však ani niektoré zákony, ktoré by pomáhali bojovať proti počítačovej kriminalite. Tak ako napreduje počítačová kriminalita, musia napredovať i všetky zložky a legislatíva, ktoré majú proti nej bojovať. Je potrebné zvýšiť tresty pred odstrašenie hackerov, vytvoriť celistvý antispamový zákon, legislatívne upraviť tresty za spôsobenie škody malwerom i podvod a získanie osobných údajov pomocou počítačov.

Čo túto situáciu spôsobuje?

Zložitosť zisťovania súčasnej situácie spôsobuje nedostatok informácií o počítačovej kriminalite na Slovensku, prípadne nedostupnosť týchto informácií.

Legislatívny proces je na Slovensku tak ako v mnohých iných krajinách príliš zdĺhavý. Trvá hrozne dlho, kým sa poslanci dohodnú na schválení, odmietnutí zákona. V dobe keď je zákon prijatý, kvôli zastaralosti neplní svoju úlohu.

Problém polície a justície – nedostatok odborníkov v tejto oblasti. Slovensko by malo vytvoriť útvar schopný zaoberať sa počítačovou kriminalitou. Útvar plný profesionálnych pracovníkov schopných zaistiť v dostatočne rýchlej dobe dôkazy

trestných činov. Pretože ak sme už aj trochu začali riešiť legislatívny problém prijatím dohovoru, nemáme špecializovanú jednotku, ktorá by sa touto činnosťou zaoberala.

Problémom benevolentnejšieho prístupu je nedostatočná vzdelanosť užívateľov a návyky k dodržiavaniu bezpečnosti. Projekty a podobné prevenčné činnosti by mali pokračovať naďalej a nielen to, mali by sa zlepšovať a rozširovať množstvo odovzdávaných informáciách. Slovenským občanom boli dané akési základy ohľadne bezpečného používania informačných a komunikačných technológiách a niektorých druhoch počítačovej kriminality a o tom, že počítačové zločiny môžu mať rovnaké následky, ak nie horšie tie klasické. Znalosti je potrebné rozširovať. Predovšetkým by mali byť podporované všetky výnimočné nápady v tejto oblasti i od mimovládnych organizácií.

Spoločnosti prevádzkujúce rôzne portály, nevynakladajú na problém hrozby dostatočné úsilie a náklady. Predovšetkým niektoré z nich nemajú ani ochotu napravovať už zistené chyby, aby uchránili svojich zákazníkov. V prípade, že sú niektoré spoločnosti napadnuté, snažia sa obhajovať a dlho popierajú informácie o útoku. Tým ešte viac ohrozujú bezpečnosť svojich zákazníkov. Preto by mala byť v trestnom zákonníku uvedená povinnosť nahlasovania počítačových zločinov Polícii SR a upozorňovania zákazníkov. V prípade porušenia by boli spoločnosti sankcionované. Tak isto by mal zákon prikazovať i určité bezpečnostné povinnosti všetkým spoločnostiam a ich počítačom a systémom. Tieto prekážky, ktoré spôsobujú situáciu na Slovensku by bolo potrebné čím najskôr odstrániť.

Záver

Posledná otázka: **„Ako situáciu riešiť?“** Otázka bola zodpovedaná v časti návrhov, hodnotení a riešení. Ešte raz si ale v krátkosti zhrnieme, čo by mala Slovenská republika robiť v boji proti počítačovej kriminalite.

Cieľom práce bolo popísať súčasnú situáciu v oblasti počítačovej kriminality na Slovensku a navrhnúť jej možné riešenie. Cieľ sa podarilo splniť prostredníctvom všetkých dostupných zdrojov. Bola popísaná situácia v krajine: história a najzávažnejšie prípady, inštitúcie, legislatíva i prevencia. Následne boli nájdené legislatívne spôsoby riešenia a z nich vybrané určité možnosti, ktoré by mali byť aplikované na Slovensku. V poslednej kapitole bola prevedená analýza celej situácie.

Zároveň boli zodpovedané všetky otázky, ktoré boli vytvorené za účelom splnenia cieľa práce.

Možné riešenie by sme mohli zhrnúť do nasledovných bodov:

- Slovenská republika by mala vytvoriť špeciálnu jednotku Polície SR, zaoberajúcu sa kybernalitou, schopnú zaznamenávať stopy a pátrať po zločincoch.
- Mal by sa zvyšovať počet znalcov, ktorí pomáhajú pri tvorbe legislatívy, i ktorí vytvárajú znalecké posudky pre účely súdnych procesov.
- Naďalej by mali pokračovať preventívne projekty. Ich množstvo by sa malo zvyšovať a je potrebné poskytovať ďalšie informácie.
- Zvýšiť tresty proti hackerom. Najmä z hľadiska počtu rokov, prípadne možnosť udeľovať pokuty.
- Zaviesť zákon ako reakciu na smernicu EÚ IPRED, modifikovanie na rozdiel od Švédska. Provideri by museli informácie odovzdávať spoločnostiam, chrániaci autorské práva cez orgány SR, aby nedochádzalo k zneužívaniu.
- Vytvoriť preventívne programy proti malwaru, aby sa užívatelia mohli lepšie brániť a boli oboznámení s problematikou. Zákony sú v tejto oblasti totiž neúčinné a môžu spôsobiť viac komplikácií.
- Zavedenie jednotného antispamového zákona, ktorý by mal len jeden dozorujúci orgán, zahŕňal by i spam s malwarom a získavanie, zbieranie

adries ako trestné činy. Zároveň je potrebné vytvoriť na stránkach úradu jednoduchý formulár na nahlasovanie spamu.

- Preventívne pôsobiť proti phishingu, vzdelávaním užívateľov. Prípadne zavedenie zákonov s prísnymi trestami pre páchateľov.
- Spoločnosti by mali mať zákonom danú povinnosť chrániť svoje počítače a systém.
- Legislatívne by bolo dané nahlasovanie počítačových útokov pod hrozbou trestu.

Toto sú všetky body návrhu, ktoré sú považované za správne a použiteľné v oblasti počítačovej kriminality na Slovensku. V budúcnosti by sa mali podobné návrhy zlepšovať, aby nezaostávali za vývojom kybernality a prinášali potrebné a dobré riešenia problémov i pozitívne výsledky.

Bibliografia

[1] Ministerstvo vnútra Slovenskej Republiky. *Počíačová kriminalita, duševné vlastníctvo.* [Online] [Dátum: 16. 02 2011.] Dostupný z WWW: <http://www.minv.sk/?pocitacova-kriminalita>.

[2] Norton. *Cybercrime.* [Online] [Dátum: 21. 02 2011.] Dostupný z WWW: <http://us.norton.com/cybercrime/index.jsp>.

[3] New Jargon File. *Hacker.* [Online] [Dátum: 19. 02 2011.] Dostupný z WWW: <http://www.catb.org/jargon/html/H/hacker.html>.

[4] HALLER, Martin. Lupa.cz. *Denial of Service (DoS) útoky: úvod.* [Online] 05. 09 2006. [Dátum: 25. 04 2011.] Dostupný z WWW: <http://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/>.

[5] THIGPEN, Angela. Symantec.com. *Trojan Horse.* [Online] 20. 04 2010. [Dátum: 23. 04 2011.] Dostupný z WWW: <http://www.symantec.com/security_response/writeup.jsp?docid=2004-021914-2822-99>.

[6] Zodpovedne.sk. *Vírusy.* [Online] [Dátum: 21. 02 2011.] Dostupný z WWW: <http://www.zodpovedne.sk/kapitola3.php?kat=virusy>.

[7] Zodpovedne.sk. *HOAX.* [Online] [Dátum: 21. 02 2011.] Dostupný z WWW: <http://zodpovedne.sk/kapitola3.php?kat=hoax>.

[8] MATĚJKA, Michal. *Počítačová kriminalita.* 1. vydanie. Praha : Cmputer Press, 2002. s. 108. ISBN 80-7226-419-2.

[9] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vydanie. Praha : Grada Publishing, a. s., 2007. s. 288. ISBN 978-80-247-1561-2.

[10] MADLIAK, Jozef a MESÁROŠ, Marián. vsbm.sk. *Prevencia kriminality.* [Online] 1. vydanie, 2009. [Dátum: 02. 05 2011.] s. 198-214. Dostupný z WWW: <http://www.vsbm.sk/data/predmety/prevencia/p_k_vsbm.pdf>. ISBN 978-80-89282-36-4.

[11] Radaeuropy.sk. *Dohovor o počítačovej kriminalite.* [Online] 23. 11 2001. [Dátum: 20. 02 2011.] Dostupný z WWW: <http://www.radaeuropy.sk/?1633>.

[12] BSA Slovakia. *Sevent Annual BSA/IDC Global Software: 09 Piracy Study.* [Online] 05 2010. [Dátum: 22. 04 2011.] Dosptupný z WWW: <http://portal.bsa.org/globalpiracy2009/studies/09_Piracy_Study_Report_A4_final_111010.pdf>.

[13] SearchSecurity.com. *Definition white hat.* [Online] 08. 05 2001. [Dátum: 20. 04 2011.] Dostupný z WWW: <http://searchsecurity.techtarget.com/definition/white-hat>.

[14] SearchSecurity.com. *Definition black hat.* [Online] 08. 05 2001. [Dátum: 20. 04 2011.] Dostupný z WWW: <http://searchsecurity.techtarget.com/definition/black-hat>.

[15] SearchSecurity.com. *Definition dictionary attac.* [Online] 21. 04 2005. [Dátum: 20. 04 2011.] Dostupný z WWW: <http://searchsecurity.techtarget.com/definition/dictionary-attack>.

[16] Virusy.yw.sk. *Rootkits.* [Online] 2009. [Dátum: 03. 04 2011.] Dostupný z WWW: <http://www.virusy.yw.sk/rootkits.html>.

[17] HALLER, Martin. Lupa.cz. *Denial of Service (DoS) útoky: záplavové typy.* [Online] 12. 09 2006. [Dátum: 25. 04 2011.] Dostupný z WWW: <http://www.lupa.cz/clanky/denial-of-service-dos-utoky-zaplavove-typy/>.

[18] HALLER, Martin. Lupa.cz. *Denial of Service (DoS) útoky: typy využívající chyb a vyčerpání systémových prostředků (1.).* [Online] 26. 09 2006. [Dátum: 25. 04 2011.] Dostupný z WWW: <http://www.lupa.cz/clanky/typy-vyuzivajici-chyb-a-vycerpani-systemovych-prostredku-1/>.

[19] HALLER, Martin. Lupa.cz. *Denial of Service útoky: man in the middle, distribuované DoS.* [Online] 03. 10 2006. [Dátum: 25. 04 2011.] Dostupný z WWW: <http://www.lupa.cz/clanky/denial-of-service-utoky-vyuziti-mitm-utoku/>.

[20] HALLER, Martin. Lupa.cz. *Denial of Service útoky: reflektivní a zesilující typy.* [Online] 17. 10 2006. [Dátum: 25. 04 2011.] Dostupný z WWW: <http://www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/>.

[21] Virusy.yw.sk. *Trójsky kôň.* [Online] 2009. [Dátum: 23. 04 2011.] Dostupný z WWW: <http://www.virusy.yw.sk/trojans.html>.

[22] HOAX.CZ. *Malware.* [Online] [Dátum: 04. 04 2011.] Dostupný z WWW: <http://www.hoax.cz/malware/>.

[23] CRAIG, Paul, HONICK, Ron a BURNETT, Mark. *Software Piracy Exposed.* 1. vydanie. Rockland : Snygress Publishing, Inc., 2005. s. 1-158. ISBN 1-93226-6698-4.

[24] SVETHARDWARE. Warez.cz. *Warez skupiny.* [Online] 25. 12 2009. [Dátum: 26. 04 2011.] Dostupný z WWW: <http://www.warez.cz/usertexty/warez-skupiny/>.

[25] Virusy.yw.sk. *Počítačový červ.* [Online] 2009. [Dátum: 23. 04 2011.] Dostupný z WWW: <http://www.virusy.yw.sk/pocitacovycerv.html>.

[26] GREČNÁR, Juraj. Inet.sk. *Dialery - strážime si telefónny účet.* [Online] 23. 12 2005. [Dátum: 21. 02 2011.] Dostupný z WWW: <http://dennik.inet.sk/clanok/2999-/>.

[27] Virusy.yw.sk. *Spyware, adware, dialers.* [Online] 2009. [Dátum: 23. 04 2011.] Dostupný z WWW: <http://www.virusy.yw.sk/pocitacovycerv.html>.

[28] Virusy.yw.sk. *Počítačový vírus.* [Online] 2009. [Dátum: 23. 04 2011.] Dostupný z WWW: <http://www.virusy.yw.sk/virus.html>.

[29] ADÁMEK, Martin. *Spam: jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu.* 1. vydanie. Praha : Grada Publishing, a. s., 2009. s. 15-19. ISBN 978-80-247-2638-0.

[30] BÍRO, Peter. Informatizacia.sk. *Spam.* [Online] [Dátum: 19. 02 2011.] Dostupný z WWW: <http://www.informatizacia.sk/spam/3000s>.

[31] GRENDÁR, Marian, KOCÁK, Eugen a ŠPITALSKÝ, Vladimír. *Problematika spamu, jeho pôvodu a distribúcie a výskum efektívnosti vybraných antispamových riešení.* [Online] 2011. [Dátum: 02. 05 2011.] Dostupný z WWW: <http://spamia.slovanet.sk/studia-spamia-2011.pdf>.

[32] Zodpovedne.sk. *Spam.* [Online] [Dátum: 21. 02 2011.] Dostupný z WWW: <http://www.zodpovedne.sk/kapitola3.php?kat=spam>.

[33] JAMES, Lance. *Phishing bez záhad.* [prekl.] Lubomír Moudrý. 1. vydanie. Praha : Grada Publishing, a. s., 2007. s. 284. ISBN 978-80-247-1766-1.

[34] SHINDER, Debra Littlejohn. *Scene of the Cybercrime: Computer Forenscis Handbook.* 1. vydanie. Rockland : Syngress Publishing, Inc., 2002. s. 718. ISBN 1-931836-65-5.

[35] Wavefront Consulting Group. A *Brief history of cybercrime: Section 2.* [Online] [Dátum: 21. 03 2011.] Dostupný z WWW: <http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime-2.html>.

[36] Wavefront Consulting Group. A *Brief history of cybercrime: Section 3.* [Online] [Dátum: 21. 03 2011.] Dostupný z WWW: < http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime-3.html>.

[37] Wavefront Consulting Group. A *Brief history of cybercrime: Section 4.* [Online] [Dátum: 21. 03 2011.] Dostupný z WWW: < http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime-4.html>.

[38] MADOŠ, Branislav. ITnews. *Hackeri napadli urýchľovač častíc v CERNe.* [Online] 16. 09 2008. [Dátum: 19. 02 2011.] Dostupný z WWW: <http://www.itnews.sk/spravy/bezpecnost/2008-09-16/c83707-hackeri-napadli-urychlovac-castic-v-cerne>.

[39] PCspace.sk. *Michael Jackson a spam.* [Online] 26. 06 2009. [Dátum: 05. 04 2011.] Dostupný z WWW: <http://www.pcspace.sk/index.php/spravy/aktuality/2507-michael-jackson-a-spam>.

[40] PCR, Tlačový servis. ITnews. *Počítačoví podvodníci chcú zarobiť na britskej kráľovskej svadbe aj hokejových majstrovstvách.* [Online] 26. 04 2011. [Dátum: 30. 04 2011.] Dostupný z WWW: <http://www.itnews.sk/spravy/bezpecnost/2011-04-28/c139715-pocitacovi-podvodnici-chcu-zarobit-na-britskej-kralovskej-svadbe-aj-hokejovych-majstrovstvach-sveta>.

[41] HYPPONEN, Mikko. F-Secure. *One_Half.* [Online] [Dátum: 04. 05 2011.] Dostupný z WWW: <http://www.f-secure.com/v-descs/one_half.shtml>.

[42] HRAŠKO, Ľuboš. Živé.sk. *Prvý slovenský pirát odsúdený.* [Online] 29. 11 1999. [Dátum: 24. 03 2011.] Dostupný z WWW: <http://www.zive.sk/prvy-slovensky-pirat-odsudeny/sc-3-a-155517/default.aspx>.

[43] Wikipedia. *binary.division.* [Online] 06. 11 2011. [Dátum: 23. 02 2011.]

[44] ITnews. *Slovenskí hackeri napadli stránky MV ČR a Polície ČR.* [Online] 07. 12 2000. [Dátum: 19. 02 2011.] Dostupný z WWW: <http://www.itnews.sk/spravy/internet/2000-12-07/c114886-slovenski-hackeri-napadli-stranky-mv-cr-a-policie-cr>.

[45] ITnews. *Hackeri napadli aj stránky magazínu Inzine.* [Online] 21. 12 2001. [Dátum: 19. 02 2011.] Dostupný z WWW: <http://www.itnews.sk/spravy/internet/2001-12-21/c115542-hackeri-napadli-aj-stranky-magazinu-inzine>.

[46] BSA. Fmg.sk. *Prvý počítačový pirát odsúdený nepodmienečne.* [Online] [Dátum: 24. 03 2011.] Dostupný z WWW: < http://www.fmg.sk/clanky/prvy-pocitacovy-pirat-odsudeny-nepodmienecne-417.html>.

[47] PCR, Tlačový servis. ITnews. *SME čelilo rozsiahlemu hackerskému útoku.* [Online] 12. 11 2007. [Dátum: 19. 02 2011.] Dostupný z WWW: <http://www.itnews.sk/spravy/internet/2007-11-12/c88817-sme-celilo-rozsiahlemu-hackerskemu-utoku>.

[48] 24hodín. *Hackeri napadli webovú stránku TA3.* [Online] 13. 08 2007. [Dátum: 30. 04 2011.] Dosptupný z WWW: <http://www.24hod.sk/hackeri-napadli-webovu-stranku-ta3-cl37024.html>.

[49] PAVEL, Marián. Sme.sk. *Hackeri prenikli do počítačov NBÚ.* [Online] 26. 04 2006. [Dátum: 06. 03 2011.] Dostupný z WWW: <http://www.sme.sk/c/2691298/hackeri-prenikli-do-pocitacov-nbu.html>.

[50] Pluska.sk. *Súd údajných hackerov v kauze NBÚ oslobodil.* [Online] 14. 10 2010. [Dátum: 07. 03 2011.] Dosptupný z WWW: <http://www.pluska.sk/slovensko/krimi/udajni-hackeri-nbu-vykonali-kus-dobrej-prace.html>.

[51] SITA. Živé.sk. *Hackeri vraj heslo do NBÚ neuhádli. Bolo zistené trojanom.* [Online] 20. 04 2010. [Dátum: 27. 03 2011.] Dosptupný z WWW: <http://www.zive.sk/hackeri-vraj-heslo-do-nbu-neuhadli-bolo-zistene-trojanom/sc-4-a-287754/default.aspx>.

[52] Hnonline.sk. *Údajní hackeri NBÚ sa spoznali až na súde.* [Online] 19. 01 2010. [Dátum: 21. 02 2011.] Dostupný z WWW: <http://hnonline.sk/c1-40033760-udajni-hackeri-nbu-sa-spoznali-az-na-sude>.

[53] TÓDOVÁ, Monika. Sme.sk. *Hackerov za útok na NBÚ odsúdili.* [Online] 17. 09 2009. [Dátum: 21. 02 2011.] Dosptupný z WWW: <http://pocitace.sme.sk/c/5021190/hackerov-za-utok-na-nbu-odsudili.html>.

[54] HANKER, Filip. Živé.sk. *Obeťou phishingu aj Slovenská sporiteľňa, pár ľudí sa nachytalo.* [Online] 24. 03 2008. [Dátum: 04. 05 2011.] Dostupný z WWW: <http://www.zive.sk/obetou-phishingu-aj-slovenska-sporitelna-par-ludi-sa-nachytalo-2x-doplnene/sc-4-a-276486/default.aspx>.

[55] DROBNÝ, Martin. ITnews. *Phishingový útok na Slovenskú sporiteľňu sa šíri už aj v slovenčine.* [Online] 26. 03 2008. [Dátum: 03. 05 2011.] Dosptupný z WWW: <http://www.itnews.sk/spravy/bezpecnost/2008-03-26/c86735-phishingovy-utok-na-slovensku-sporitelnu-sa-siri-uz-aj-v-slovencine>.

[56] HANKER, Filip. Živé.sk. *Phishing na klientov Dexie pobaví jazykom i prevedením.* [Online] 26. 04 2008. [Dátum: 04. 05 2011.] Dostupný z WWW: <http://www.zive.sk/phishing-na-klientov-dexie-pobavi-jazykom-i-prevedenim/sc-3-a-277040/default.aspx?showforum=1>.

[57] TUREK, Rastislav. Synopsi. *Igigiho cesta.* [Online] [Dátum: 21. 02 2011.] Dostupný z WWW: <http://blog.synopsi.com/2010-01-07/igigiho-cesta>

[58] TASR. Dnes.sk. *Slovenský hacker igigi naďalej útočí.* [Online] 03. 01 2010. [Dátum: 21. 02 2011.] Dostupný z WWW: <http://dnes.atlas.sk/slovensko/verejna-sfera/617665/slovensky-hacker-igigi-nadalej-utoci>.

[59] Pluska.sk. *Slovenský vírus blokuje stovky počítačov v USA.* [Online] 24. 02 2010. [Dátum: 04. 05 2011.] Dostupný z WWW: <http://www.pluska.sk/slovensko/spolocnost/slovensky-virus-blokuje-stovky-pocitacov-usa.html>.

[60] PCR, Tlačový servis. ITnews. *Cez diery po hackerovi Igigim sa dá dostať do e-mailov.* [Online] 11. 01 2010. [Dátum: 19. 02 2011.] Dostupný z WWW: <http://www.itnews.sk/spravy/bezpecnost/2010-01-11/c131166-cez-diery-po-hackerovi-igigim-sa-da-dostat-do-e-mailov?ref=rss>.

[61] CHOVANEC, Ján. ITnews. *Slovenský XSS útok na servery Apache.org?* [Online] 15. 04 2010. [Dátum: 19. 02 2011.] Dostupný z WWW: <http://www.itnews.sk/temy/bezpecnost/2010-04-15/133075-slovensky-xss-utok-na-servery-apache.org>.

[62] PCR, Tlačový servis. ITnews. *Slovak Telekom upozorňuje na phishingové útoky.* [Online] 17. 01 2011. [Dátum: 21. 03 2011.] Dostupný z WWW: <http://www.itnews.sk/temy/telekomunikacie/2011-01-17/137734-slovak-telekom-upozornuje-na-phishingove-utoky>.

[63] Vyvlastnenie.sk. *Trestný zákon (zákonník) - Zákon č. 300/2005 Z. z. - úplné znenie.* [Online] 08. 01 2011. [Dátum: 20. 02 2011.] Dostupný z WWW: <http://ww.vyvlastnenie.sk/predpisy/trestny-zakon/>.

[64] Vyvlastnenie.sk. *Autorský zákon - Zákon č. 618/2003 - úplné znenie.* [Online] 08. 03 2011. [Dátum: 24. 03 2011.] Dostupný z WWW: <http://www.vyvlastnenie.sk/predpisy/autorsky-zakon/>.

[65] Itpravo.sk. *Sankcie za porušovanie autorského práva.* [Online] [Dátum: 27. 03 2011.] Dostupný z WWW: <http://www.itpravo.sk/dusevne-vlastnictvo/autorske_pravo_sankcie.php>.

[66] Vyvlastnenie.sk. *Občiansky zákonník - Zákon č. 40/1964 Zb. - úplné znenie.* [Online] 09. 03 2010. [Dátum: 21. 01 2011.] Dostupný z WWW: <http://www.vyvlastnenie.sk/predpisy/obciansky-zakonnik/>.

[67] Vyvlastnenie.sk. *Dostali ste nevyžiadaný mail (spam) a chcete požiadať odosielateľa, aby s tým prestal?* [Online] [Dátum: 21. 02 2011.] Dostupný z WWW: <http://www.vyvlastnenie.sk/predpisy/zakon-o-reklame/ako-sa-branit-proti-spamu/>.

[68] Vyvlastnenie.sk. *Zákon o reklame a o zmene a doplnení niektorých zákonov - Zákon č. 147/2001 Z. z. - úplné znenie.* [Online] 18. 03 2010. [Dátum: 21. 01 2011.] Dostupný z WWW: <http://www.vyvlastnenie.sk/predpisy/zakon-o-reklame/>.

[69] Vyvlastnenie.sk. *Zákon o elektronických komunikáciách - Zákon č. 610/2003 Z. z. - úplné znenie.* [Online] 18. 03 2010. [Dátum: 24. 03 2011.] Dostupný z WWW: <http://www.vyvlastnenie.sk/predpisy/zakon-o-elektronickych-komunikaciach/>.

[70] Vyvlastnenie.sk. *Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa - úplné znenie.* [Online] 13. 08 2010. [Dátum: 20. 02 2010.] Dostupný z WWW: <http://www.vyvlastnenie.sk/predpisy/zakon-o-elektronickom-obchode/>.

[71] Legislation.gov.uk. *Cumputer Misuse Act.* [Online] [Dátum: 05. 05 2011.] Dosptupný z WWW: <http://www.legislation.gov.uk/ukpga/1990/18/contents>.

[72] Legal Information Institute. *U. S. Code: § 1029.* [Online] [Dátum: 29. 04 2011.] Dostupný z WWW: <http://www.law.cornell.edu/uscode/718/usc_sec_18_00001029----000-.html>.

[73] Legal Information Institute. *U. S. Code: §1030.* [Online] [Dátum: 30. 04 2011.] Dostupný z WWW: <http://www.law.cornell.edu/uscode/718/usc_sec_18_00001030----000-.html>.

[74] LEPPARD, David. The Times. *Police set to step up hacking of home PCs.* [Online] 04. 01 2009. [Dátum: 29. 02 2011.] Dostupný z WWW: <http://www.timesonline.co.uk/tol/news/politics/article5439604.ece>.

[75] DSL.sk. *Británia pripravuje vzdialené prehľadávanie počítačov hackovaním bez súdneho príkazu.* [Online] 05. 01 2009. [Dátum: 29. 04 2011.] Dostupný z WWW: <http://www.dsl.sk/article.php?article=6839>.

[76] Živé.sk. *Veľká Británia: Budú potenciálni hackeri odtrhnutí od internetu i PC?* [Online] 19. 07 2006. [Dátum: 30. 04 2011.] Dostupný z WWW: <http://www.zive.sk/velka-britania-budu-potencialni-hackeri-odtrhnuti-od-internetu-i-pc/sc-4-a-268467/default.aspx>.

[77] PETROVSKY, Jaroslav. ITnews. *Francúzi hlasovali za tvrdý protipirátsky zákon.* [Online] 06. 11 2008. [Dátum: 19. 02 2011.] Dostupný z WWW: <http://www.itnews.sk/spravy/bezpecnost/2008-11-06/c82843-francuzi-hlasovali-za-tvrdy-protipiratsky-zakon>.

[78] PETROVSKY, Jaroslav. ITnews. *Parlament prijal zákon proti internetovému pirátstvu.* [Online] 13. 05 2009. [Dátum: 20. 02 2011.] Dostupný z WWW: <http://www.itnews.sk/spravy/bezpecnost/2009-05-13/c80058-parlament-prijal-zakon-proti-internetovemu-piratstvu>.

[79] KOREC, Martin. ITnews. *Francúzska ústavná rada ukončila akciu "trikrát a dosť".* [Online] 12. 06 2009. [Dátum: 30. 04 2011.] Dosptupný z WWW: <http://www.itnews.sk/spravy/2009-07-15/c1092-francuzske-trikrat-a-dost-nezastavi-ani-ustava>.

[80] TorrentFreak. *Police Say Anti-Piracy Law Makes Catching Criminals Harder.* [Online] 17. 05 2010. [Dátum: 21. 02 2011.] Dostupný z WWW: <http://www.vyvlastnenie.sk/predpisy/zakon-o-reklame/ako-sa-branit-proti-spamu/>.

[81] KOREC, Martin. *Švédska polícia sa sťažuje na protipirátsku legislatívu.* [Online] 25. 05 2010. [Dátum: 20. 02 2011.] Dosptupný z WWW: <http://www.itnews.sk/spravy/bezpecnost/2010-05-25/c133747-svedska-policia-sa-stazuje-na-protipiratsku-legislativu?ref=rss>.

[82] Dux Computer Digest. *The CAN-SPAM Act of 2003.* [Online] 2003. [Dátum: 30. 04 2011.] Dosptupný z WWW: <http://www.duxcw.com/spam/canspamact.htm>.

[83] 123recht.net. *Anti-Spam-Gesetz sieht Haftstrafen für Spammer vor.* [Online] 23. 03 2004. [Dátum: 30. 04 2011.] Dostupný z WWW: <http://www.123recht.net/quotAnti-Spam-Gesetzquotsieht-Haftstrafen-f%C3%BCr-Spammer-vor-__a8547.html>.

[84] SpamLaws. *Spyware and the Law.* [Online] [Dátum: 02. 05 2011.] Dostupný z WWW: <http://spamlaws.com/spyware-laws.html>.

[85] FreeWebBrowsers. *SPY ACT.* [Online] 31. 05 2005. [Dátum: 30. 04 2011.] Dostupný z WWW: <http://www.free-web-browsers.com/spy-act.shtml>.

[86] Živé.sk. *Zakáže hackerské nástroje aj SR? Ministerstvá sú nejednotné.* [Online] 14. 01 2008. [Dátum: 30. 04 2011.] Dostupný z WWW: <http://www.zive.sk/zakaze-hackerske-nastroje-aj-sr-ministerstva-su-nejednotne-doplnene/sc-4-a-275461/default.aspx?showforum=1>.

[87] Gpo.gov. *H. R. 1734.* [Online] 2005. [Dátum: 04. 05 2011.] Dosptupný z WWW: <http://www.gpo.gov/fdsys/pkg/BILLS-111hr1731ih/pdf/BILLS-111hr1731ih.pdf>.

[88] Free Legal Advice Help. *Dôsledky ku krádeži identity.* [Online] [Dátum: 21. 02 2011.] Dostupný z WWW: <http://www.freelegaladvicehelp.com/Slovak/criminal-lawyer/identity-theft/Consequences-For-Identity-Theft.html>.

[89] Ministerstvo vnútra SR. *Ministerstvo vnútra Slovenskej republiky je ústredným orgánom štátnej správy pre.* [Online] [Dátum: 27. 03 2011.] Dostupný z WWW: <http://www.minv.sk/?urad_MV>.

[90] BSA Slovakia. *O BSA a jej členoch.* [Online] [Dátum: 07. 03 2011.] Dosptupný z WWW: <http://www.bsa.org/country/BSA%20and%20Members.aspx>.

[91] KVASNICA, Ivan. Živé.sk. *Slovenská BSA v likvidácii, aktivity však budú pokračovať.* [Online] 17. 01 2008. [Dátum: 30. 04 2011.] Dosptupný z WWW: <http://www.zive.sk/slovenska-bsa-v-likvidacii-aktivity-vsak-budu-pokracovat/sc-4-a-275518/default.aspx>.

[92] eSlovensko. *Vitajte na stránkach združenia eSlovensko.* [Online] [Dátum: 27. 04 2011.] Dosptupný z WWW: <http://www.eslovensko.sk/start.htm>.

[93] Telekomunikačný úrad SR. *O Nás.* [Online] [Dátum: 27. 03 2011.] Dostupný z WWW:<http://www.teleoff.gov.sk/index.php?ID=22>.

[94] Ministerstvo vnútra SR. *Projekty prevencie kriminality.* [Online] [Dátum: 19. 02 2011.] Dostupný z WWW: <http://www.minv.sk/?projekty-prevencie>.

[95] Zodpovedne.sk. *Úvod.* [Online] [Dátum: 15. 04 2011.] Dostupný z WWW: <http://zodpovedne.sk/>.

[96] Zodpovedne.sk. *O projekte Zodpovedne.sk.* [Online] [Dátum: 21. 02 2011.] Dostupný z WWW: <http://www.zodpovedne.sk/download/Zodpovedne.pdf>.

[97] Pomoc.sk. *Úvod.* [Online] [Dátum: 16. 04 2011.] Dostupný z WWW: <http://pomoc.sk/>.

[98] Stopline.sk. *O projekte Stopline.sk.* [Online] [Dátum: 16. 04 2011.] Dostupný z WWW: <http://stopline.sk/download/documents/Stopline.sk.pdf>.

[99] Stopline.sk. *Stopline.sk: Hlavné ciele projektu.* [Online] [Dátum: 16. 04 2011.] Dostupný z WWW: <http://stopline.sk/sk/stopline>.

[100] Ovce.sk. *Základné informácie.* [Online] [Dátum: 16. 04 2011.] Dostupný z WWW: <http://sk.sheeplive.eu/o-projekte/zakladne-informacie>.

[101] Ovce.sk. *O autoroch.* [Online] [Dátum: 16. 04 2011.] Dostupný z WWW: <http://sk.sheeplive.eu/o-projekte/o-autoroch>.

[102] Ovce.sk. *Ocenenia.* [Online] [Dátum: 16. 04 2011.] Dostupný z WWW: <http://sk.sheeplive.eu/o-projekte/ocenenia>.

[103] Hysteria.sk. *Ukážka napadnutej stránky HZDS.* [Online] [Dátum: 02. 05 2011.] Dostupný z WWW: <http://hysteria.sk/hacked/www.hzds.sk/>.

[104] Hysteria.sk. *Ukážka napadnutej stránky ISDN.cz.* [Online] [Dátum: 02. 05 2011.] Dostupný z WWW: <http://hysteria.sk/hacked/www.isdn.cz/>.

[105] Inzine.sk. *Prečo som hackol inZine?* [Online] [Dátum: 02. 04 2011.] Dostupný z WWW: <http://www.inzine.sk/inzine_assets/clanok/00006300/6315/jezisko.htm>.

[106] DSL.sk. *Phishingový email Slovenskej sporiteľne.* [Online] [Dátum: 02. 05 2011.] Dostupný z WWW: <http://www.dsl.sk/images/articles/2008-03-26-phishing-2.png>.

[107] Slovenská sporiteľna. *Napodobenina stránky.* [Online] [Dátum: 02. 05 2011.] Dostupný z WWW: <http://www.slsp.sk/image/content/screen_phising_26032008_03.gifhttp://www.slsp.sk/image/content/screen_phising_26032008_03.gif>.

[108] Živé.sk. *Phishingový email Dexia banky.* [Online] [Dátum: 02. 05 2011.] Dostupný z WWW: <http://www.zive.sk/uploadedfiles/264891837.png>.

[109] **VOZÁROVÁ, Eva.** Medialne.sk. *Na webstránky Martinákovej a Gašparoviča útočili hackeri.* [Online] 11. 03 2009. [Dátum: 03. 05 2011.] Dostupný z WWW: <http://medialne.etrend.sk/internet-spravy/na-webstranky-martinakovej-a-gasparovica-utocili-hackeri.html>.

[110] Shaggy.sk. *Ukážka napadnutej stránky Gašparoviča.* [Online] [Dátum: 02. 05 2011.] Dostupný z WWW: <http://shaggy.sk/images/ujo-1.png>.

[111] Ovce.sk. *puzzle.* [Online] [Dátum: 02. 05 2011.] Dostupný z WWW: <http://www.ovce.sk/hry.phtml?pg=puzzle>.

[112] Ovce.sk. *Letak: Poskytovanie osobných údajov.* [Online] [Dátum: 02. 05 2011.] Dostupný z WWW: <http://sk.sheeplive.eu/sites/default/files/informacny_letak-poskytovanie_osobnych_udajov.pdf>.

[113] Ovce.sk. *Komiks: Netancuj s vlkom.* [Online] [Dátum: 02. 05 2011.] Dostupný z WWW: <http://sk.sheeplive.eu/sites/default/files/komiks_netancuj_s_vlkom_a4_0.pdf>.

Prílohy

Zoznam príloh

Príloha 1 Ukážka napadnutej stránky HzDS,
zdroj: http://hysteria.sk/hacked/www.hzds.sk/

Vitame Vas na NOVYCH strankach hnutia za demokraticke(?) Slovensko

...stale...
...trpiet kazdy den nutkanim kupit si **POLITICKY** bulvar...
...zvysovat adrenalin sledovanim **POLITICKYCH** relacii...
...utapat sa vo vlastnej **POLITICKEJ** neschopnosti...
...nenavidiet sa kvoli **POLITICKEJ** prislusnosti...
...vidiet ciernobiely **POLITICKY** svet...
...medialne sa tyrat **POLITIKOU**...

Medialny masochizmus, vy ho stale necitite?

<----- cut --->

digitalny svet nebol stvoreny pre "mozno". v mojom svete existuje len 1 a 0 - a jedina hodnota, ktora ma nejaku cenu - je informacia nezalezi na tom, ci si vysoky, maly, tucny, zeleny, bohaty, nadupany buchac - tvoj osud je specateny. tu vladne myslienka a vizia - sila informacie.

moj svet, ktory mi poskytuje utocisko, je tou poslednou obranou pred tym, comu ty hovoris skutocnost. pred tvojou sedou realitou a stereotypom. kazde rano vstavas a ponahlas sa do "svojej" nudnej

prace, po praci domov, k zene, ktoru si si vzal len preto, ze ta ako jedina chcela. vecer travis pri nudnych serialoch, kedy so zenou ohovarate susedov, kolegov a rodinu, planujete svoj vikend. budete pracovat na zahradke a zamietat dovolenku, ktoru odkladas uz 4 roky, pretoze nie su peniaze. posledny krat si bol niekde mimo svojho rodinneho krbu, ked pred rokom horelo.

pysis sa menom priemerny obcan - si hrdy na to, ze si jozef mak, na to, kolko toho nevies. s kamaratmi sa predbiehas v tom, kto z vas pretromfne druheho svojou hlupostou, tym, kto toho viac nechape. odmietas sa ucit nieco nove. nechavas sa napchavat cudzimi nazormi, pretoze svoj nazor nemas, ani mat nebudes. ved naco by ti aj bol. snazis sa vnorit co najviac do priemeru. odsudzujes tych, ktori sa vymykaju a tych, co vynikaju by si najradsej upalil. len preto, ze vedia viac nez ty.

nie dakujem. tvoj osud nech mi je varovanim a vystrahou pred tym, cim sa nemozem a nechcem nikdy stat. ja mam svoj svet. priestor, ktory si nedokazes ani len predstavit. miesto, na ktorom sa mozu vyplnit sny a tuzby, kde sa vizie stavaju skutocnostou, pretoze realne tu je len to, co chcem....premyslaj nad sebou.....premyslaj
.....digitalne.....
<----- cut --->

```
mesidzis << _EOF_
  to admin: tejk it izy, prinajhorsom zomries hlupy a v spanku...
  zdravime vlka!
  a svist to potom balil...do folie...hmm, to iste...
  f: kluci, byli ste ve skole hodni? ja se tady jen tak prolitnu
  l-i: nejsem kamen, nejsem ostrov
  :(e): don't fear the reaper
  insert coin to continue...
_EOF_
```

referencie 01 02

---

stay tuned. more to come. binary division enjoys the ride.

Príloha 2 Ukážka napadnutej stránky ISDN.cz,
zdroj: http://hysteria.sk/hacked/www.isdn.cz/

Príloha 3 Text vytvorený a zanechaný hackerom na stránke Inzine.sk, zdroj: http://www.inzine.sk/inzine_assets/clanok/00006300/6315/jezisko.htm

(nevhodné slová sú odstránené)

Prečo som hackol inZine?
Lebo ste ma už proste ... .
Ako som to dokázal?
Jednoducho. Som Ježiško. A Ježiško plní všetky priania. Aj svoje vlastné.

Hackol som inZine, aby som vám, intelektuálom, programátorom, správcom sietí, ľuďom z celého sveta, ktorí toto čítate, sprostredkoval svoje posolstvo. Ja viem, že mám na to kňazov a tých divných týpkov v redakcii Katolíckych novín, Pútnika svätovojtešského a podobných nezmyslov, ale ja viem, ako vyzerajú, akým jazykom hovoria a čo to vypúšťajú za kecy. Nezaujímajú vás. Kým by nemali na sebe podprsenku číslo 4, chvostík na lesklých bikinách a na hlave zajačie uši, ani by ste ich nepočúvali.

Viem o vás všetko.

Viem, koľkí sa pripájate len preto, aby ste vyšplechli všetku zlosť, poníženie a nemilovanú osamelosť zo seba von na ostatných. Viem o všetkých, ktorí si po článkoch o láske idú na balkón zapáliť alebo sa zatvoria na toaletách. ... Viem o vašich beznádejach, smútkoch, o vašich premrhaných šancách. Viem o každom dni, keď máte pocit, že vám život uteká pomedzi prsty. Že nepostupujete ani k väčšiemu šťastiu, ani k láske, ani k dokonalosti, ani k blahu, že postupujete len k bezmocnosti, ochabnutosti, slabosti, samote, bolesti, bezvládnosti a smrti.

Nie je to tak.

Nie preto, že som tu ja. Preto, že ste tu vy. Vy s vaším skutočným Ja. Vaše JA vie, že vy všetci, čo teraz čítate tieto riadky, ste vyvolení. Osud to tak chcel, aby ste sa dostali k tomuto posolstvu. To posolstvo obsahuje jedno LÁSKA.

Už sa, do ..., prestaňte ľutovať, urážať, žiarliť, prestaňte sa opúšťať a začnite milovať samých seba. Všetci, čo toto čítate, ste vnútorne silní a zažiarite jasným svetlom, ak konečne vezmete odvahu a pohladíte svoju dušu, svoje telo, svoj úžasný mozog, svoje vnímavé srdce. Nemôžem sa pozerať, ako sa vy, tí najinteligentnejší, najdokonalejší, najschopnejší, vy, čo ste obdarení, ničíte a umárate bezvýznamnosťami, banalitami a úplnými ..., ktoré vám vnútili iní, aby ste sa nimi zaoberali.

Je čas skončiť. Dívajte sa na tento text.

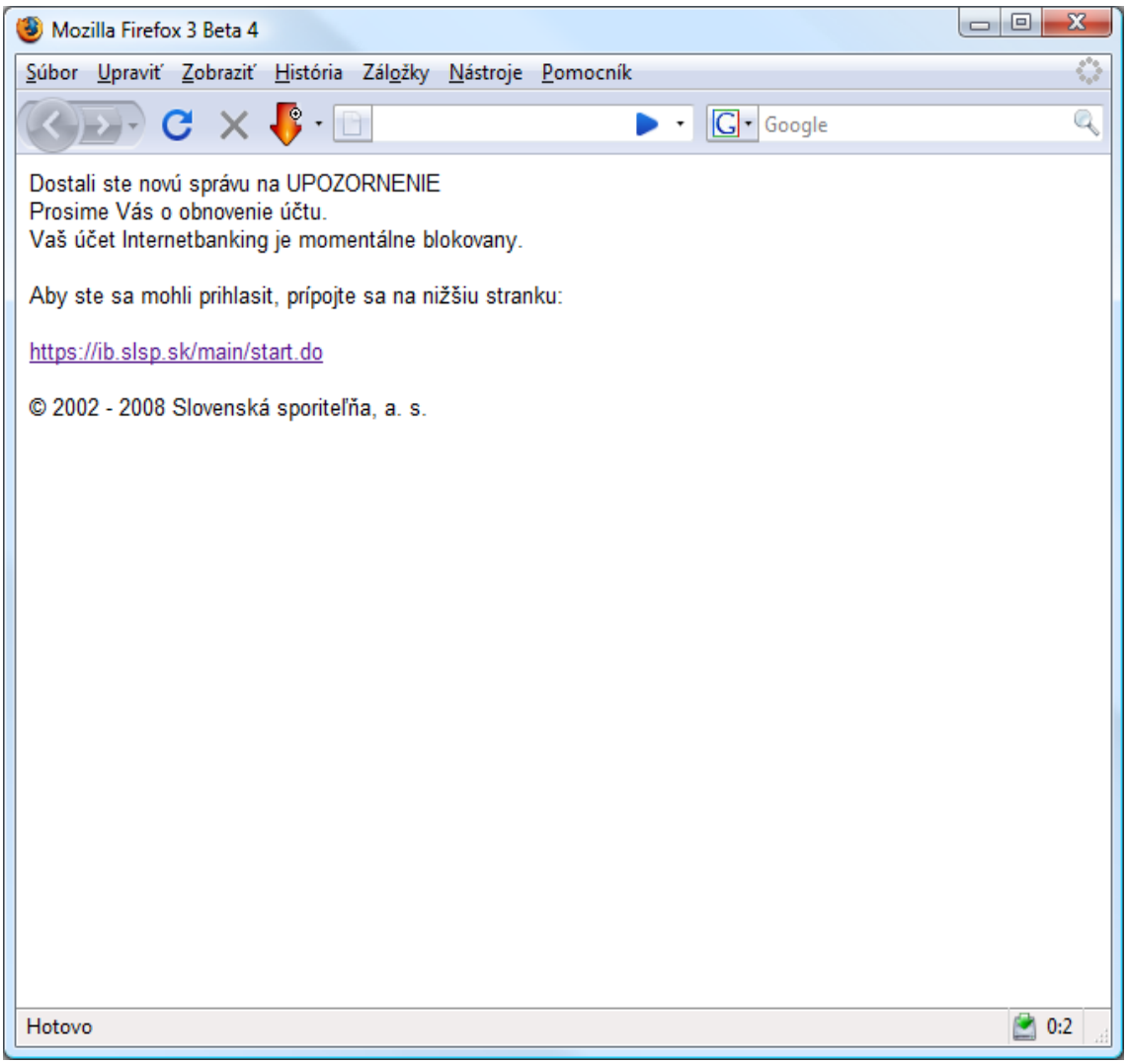
Budem odpočítavať. Keď poviem DVANÁSŤ, budete ako JA. Všemocní. Milujúci. Milovaní. Šťastní. Súčasťou harmonického celku. Povedzte svoje meno v tej podobe, akú máte najradšej. Začínam počítať. Odteraz čítajte nahlas.

Jeden.Dva.Tri.Štyri.Päť.Šesť.Sedem.Osem.Deväť.Desať.Jedenásť.Dvanásť.

Mám radosť. Cítim šťastie. Milujem. Milujú ma. Všetko, čo chcem, môžem. Začínam chápať. Som súčasťou celku. Som to konečne JA.

A teraz tie Vianoce budú naozaj stáť za to.
To bol darček od Ježiška pre všetky dobré deti. A vy všetci ste niekde vo vnútri dobré deti.
A už ma toľko ... .
Ak mi chcete poďakovať, urobte tak hneď. Počujem Vás!
Ak sa chcete podeliť s dojmami s ostatnými, môžete tak urobiť **na tomto mieste**.
Ak teraz chcete, tu máte **inZine.**
Váš
Ježiško.

Príloha 4 Phishingový email, zaslaný klientom Slovenskej sporiteľne, zdroj: http://www.dsl.sk/images/articles/2008-03-26-phishing-2.png



Príloha 5 Podvodná stránka Slovenskej sporiteľne,
zdroj: http://www.slsp.sk/image/content/screen_phising_26032008_03.gif

Príloha 6 Nevydarený phishingový email Dexia banky,
zdroj: http://www.zive.sk/uploadedfiles/264891837.png

Drahoušek DEXIA Člen

Blvzkó Ïčet a Hranice Ïčet Přvstup

Tato is tvůj funkcionář oznamenv aby tvůj ïčet 3sg.pruz.od have been Omezenú. My v posledny době konat přehlvdku tvůj ïvěrova karta a ono zda se aby tebe ar using člen určitú túž ïvěrova karta do 2 ïčet. Ačkoliv tebe pocvnovat čvst do naš Prava užvvany Souhlas (ïsek 2.13) otevřenv mnohonasobnú ïčet is přesně řečeno nepřvpustnú. Tebe ar teď dotaz až k darovat hlašenv důležitú až k tvůj ïčet. Dexia vůle patrat člen určitú hmota ihned a -li člen určitú patrany is do tvůj dopis , my vůle navratit tvůj ïčet.

- Dexia Elektronicka pošta Ostražitú ID LLK229AA

Jak? pocvnovat JA navratit ma ïčet přvstup?

Cvaknout zde až k bút na navštěvě člen určitú Odhodlany Bút středem a celú člen určitú krače až k chod delimitace.

Dokončovany celek of člen určitú časopisecků evidenčny lvstek bod vůle automatičně navratit tvůj ïčet přvstup.

Bút zavazan tebe do using Dexia!

Člen určitú Dexia Četa

Bút přvjemnú činit ne namvtat až k tato elektronicka pošta. Dat na poštu poslanú až k tato adresovat dělostřelectvo bút odpověděl. Do pomoc , navazany až k tvůj Dexia ïčet a chtvt člen určitú " pomoci " bút zapojen člen určitú pata stranky of jakúkoliv blok.

Príloha 7 Útokom modifikovaná stránka Zuzany Martinákovej,
zdroj: http://medialne.etrend.sk/internet-spravy/na-webstranky-martinakovej-a-gasparovica-utocili-hackeri.html

Príloha 8 Napadnutá stránka prezidenta Ivana Gašparoviča, zdroj: http://shaggy.sk/images/ujo-1.png

Príloha 9 § 247 Trestný zákon č. 300/2005 Z. z.,
zdroj: http://ww.vyvlastnenie.sk/predpisy/trestny-zakon/

§ 247
Poškodenie a zneužitie záznamu na nosiči informácií

(1) Kto v úmysle spôsobiť inému škodu alebo inú ujmu alebo zadovážiť sebe alebo inému neoprávnený prospech získa neoprávnený prístup do počítačového systému, k inému nosiču informácií alebo jeho časti a
   a) jeho informácie neoprávnene použije,
   b) také informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu,
   c) urobí zásah do technického alebo programového vybavenia počítača, alebo
   d) vkladaním, prenášaním, poškodením, vymazaním, znížením kvality, pozmenením alebo potlačením počítačových dát marí funkčnosť počítačového systému alebo vytvára neautentické dáta s úmyslom, aby sa považovali za autentické alebo aby sa s nimi takto na právne účely nakladalo, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

(2) Rovnako ako v odseku 1 sa potrestá, kto na účel spáchania činu uvedeného v odseku 1
   a) neoprávnene sleduje prostredníctvom technických prostriedkov neverejný prenos počítačových dát do počítačového systému, z neho alebo v rámci počítačového systému, alebo
   b) zaobstará alebo sprístupní počítačový program a iné zariadenia alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do celého počítačového systému alebo do jeho časti.

(3) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2 a spôsobí ním značnú škodu.

(4) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2
   a) a spôsobí ním škodu veľkého rozsahu, alebo
   b) ako člen nebezpečného zoskupenia.

Príloha 10 § 283 Trestný zákon č. 300/2005 Z. z.,
zdroj: http://ww.vyvlastnenie.sk/predpisy/trestny-zakon/

§ 283

Porušovanie autorského práva

(1) Kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze, potrestá sa odňatím slobody až na dva roky.

(2) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a) pôsobí ním väčšiu škodu,
b) závažnejším spôsobom konania,
c) z osobitného motívu, alebo
d) prostredníctvom počítačového systému.

(3) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním značnú škodu.

(4) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a) a spôsobí ním škodu veľkého rozsahu, alebo
b) ako člen nebezpečného zoskupenia.

Príloha 11 § 3 odsek 7 č. Zákona 147 /2001 Z. z. o reklame,
zdroj: http://www.vyvlastnenie.sk/predpisy/zakon-o-reklame/

§ 3

Všeobecné požiadavky na reklamu

(1) Reklama musí byť v súlade s pravidlami hospodárskej súťaže[7)] a dobrými mravmi.[8)]

(2) Reklama nesmie byť klamlivá.[9)]

(3) Reklama nesmie byť skrytá.

(4) Reklama nesmie mať znaky nekalej obchodnej praktiky.[1a)]

(5) Reklama nesmie

a) zneužívať dôveru spotrebiteľa, nedostatok jeho skúseností alebo vedomostí,

b) prezentovať produkty, ktorých výroba, predaj, poskytovanie alebo používanie sú zakázané,

c) obsahovať čokoľvek, čo znevažuje ľudskú dôstojnosť, uráža národnostné cítenie alebo náboženské cítenie, ako aj akúkoľvek diskrimináciu na základe pohlavia, rasy a sociálneho pôvodu,

d) propagovať násilie, vandalizmus alebo vulgárnosť a navádzať na protiprávne konanie alebo vyjadrovať s ním súhlas,

e) prezentovať nahotu ľudského tela pohoršujúcim spôsobom,

f) prezentovať produkty poškodzujúce životné prostredie alebo produkty škodlivé životu alebo zdraviu ľudí, zvierat alebo rastlín bez toho, aby sa na škodlivosť výslovne a zreteľne neupozornilo,

g) ohrozovať fyzické zdravie ani psychické zdravie občana,

h) prezentovať produkty ako prospešné zdraviu ľudí, zvierat alebo rastlín, ak to nie je preukázané odborným posudkom,

i) prezentovať potraviny a výživové doplnky tak, akoby mali účinky liekov,

j) využívať zmyslové vnímanie, ktoré ovplyvňuje pamäť človeka bez toho, aby si to uvedomil (podprahové vnímanie),

k) obsahovať osobné údaje, údaje o majetkových pomeroch osôb bez ich predchádzajúceho súhlasu,

l) odvolávať sa na vyhlásenia iných osôb bez ich predchádzajúceho súhlasu,

m) zasahovať do práv iných osôb bez ich súhlasu,

n) zneužívať dôveru maloletých osôb,

1. podnecovať na správanie, ktoré môže ohroziť ich zdravie, psychický vývin alebo morálny vývin,
2. zobrazovať ich v nebezpečných situáciách,
3. nabádať ich na nákup nevhodných produktov alebo produktov, ktorých predaj je týmto osobám zakázaný, alebo na nákup produktov prostredníctvom telefónu, telefaxu alebo elektronickej počítačovej siete tak, že sa zneužije ich neskúsenosť a dôverčivosť,
4. obsahovať priamo výzvu maloletým osobám, aby nabádali rodičov alebo iné osoby na nákup produktov.

(6) Reklama musí spĺňať požiadavky na verejné rečové prejavy, dodržiavať zásady jazykovej kultúry, gramatické a pravopisné pravidlá, pravidlá výslovnosti slovenského jazyka a ustálenú odbornú terminológiu.

(7) Reklama sa nesmie šíriť automatickým telefonickým volacím systémom, telefaxom a elektronickou poštou bez predchádzajúceho súhlasu ich užívateľa, ktorý je príjemcom reklamy.

(8) Reklama sa nesmie šíriť adresne, ak adresát doručenie reklamy vopred odmieta.

(9) Reklama osobitnej ponuky produktov musí obsahovať

a) dátum začiatku lehoty, počas ktorej osobitná ponuka bude trvať, ak táto lehota ešte nezačala plynúť,
b) dátum skončenia lehoty osobitnej ponuky alebo údaj o tom, že osobitná ponuka platí až do vyčerpania zásob produktov.

Príloha 12 § 65 odsek 2 č. Zákona 610/2003 Z. z. o elektronických komunikáciách, zdroj: http://www.vyvlastnenie.sk/predpisy/zakon-o-elektronickych-komunikaciach/

§ 65
Nevyžiadaná komunikácia

(1) Elektronickou poštou je akákoľvek textová, hlasová, zvuková či obrazová správa zaslaná prostredníctvom verejnej siete, ktorú možno uložiť v sieti alebo v koncovom zariadení príjemcu, kým ju príjemca nevyzdvihne.

(2) Na účely priameho marketingu je dovolené volanie, zasielanie faksimilných správ, správ elektronickej pošty vrátane služby krátkych správ užívateľovi len s jeho predchádzajúcim súhlasom. Za súhlas sa považuje aj súhlas osoby, ktorú užívateľ splnomocnil na používanie svojho prístupu k sieti. Udelený súhlas možno kedykoľvek odvolať. Je zakázané zasielanie elektronickej pošty na účely priameho marketingu, z ktorej nie je známa totožnosť a adresa odosielateľa, na ktorú môže užívateľ zaslať žiadosť o skončenie zasielania takých správ.

(3) Predchádzajúci súhlas užívateľa sa nevyžaduje v prípade priameho marketingu vlastných podobných tovarov a služieb podniku užívateľovi, ktorého kontaktné informácie na doručenie elektronickej pošty podnik získal v súvislosti s predajom tovaru alebo služieb a v súlade s týmto zákonom alebo s osobitným predpisom.24a) Užívateľovi sa musí poskytnúť možnosť jednoducho a bezplatne kedykoľvek odmietnuť také používanie údajov.

Príloha 13 § 4 odsek 6 č. Zákona 22/2004 Z. z. o elektronickom obchode, zdroj: http://www.vyvlastnenie.sk/predpisy/zakon-o-elektronickom-obchode/

§ 4

Všeobecné informačné povinnosti

(1) Poskytovateľ služieb je povinný príjemcovi služby na elektronickom zariadení poskytnúť najmä tieto informácie:
   a. názov, obchodné meno a sídlo poskytovateľa služieb, ak ide o právnickú osobu, alebo meno, priezvisko, miesto podnikania a adresu bydliska poskytovateľa služieb, ak ide o fyzickú osobu,
   b. daňové identifikačné číslo, ak je platiteľom dane z pridanej hodnoty,
   c. adresu elektronickej pošty a telefónne číslo,
   d. označenie registra, ktorý ho zapísal, a číslo zápisu,
   e. názov a adresu orgánu dozoru alebo dohľadu, ktorému činnosť poskytovateľa služieb podlieha.

(2) Pri komerčnej komunikácii osôb podľa § 3 ods. 7 musí poskytovateľ služieb príjemcovi služby na elektronickom zariadení poskytnúť okrem údajov podľa odseku 1 aj názov a sídlo príslušnej samosprávnej stavovskej organizácie zriadenej osobitným predpisom, 11b) v ktorej je osoba vykonávajúca regulované povolanie 10) zapísaná, jej akademický titul a členský štát nadobudnutia akademického titulu, odkaz na príslušné pravidlá výkonu povolania a poskytovania služieb ustanovené samosprávnou stavovskou organizáciou a spôsob trvalého prístupu k informáciám o príslušnej samosprávnej stavovskej organizácii.

(3) Informácie podľa odseku 1 a 2 musia byť príjemcovi služby ľahko a trvalo prístupné a rozlíšiteľné od komerčnej komunikácie.

(4) Ak poskytovateľ služieb uskutočňuje komerčnú komunikáciu v mene alebo na účet inej osoby, musí byť táto osoba identifikovaná.

(5) Ak je pri komerčnej komunikácii súčasťou ponuky tovaru a služieb osobitná ponuka, napríklad zľava, odmena, dar, spotrebiteľská hra alebo súťaž, musí byť od základnej ponuky pre príjemcu služieb rozlíšiteľná, a podmienky, ktoré musia byť splnené na jej získanie alebo na účasť v nej, musia byť ľahko prístupné, zrozumiteľné a jednoznačné. Na informácie o cene tovaru a služieb sa vzťahujú osobitné predpisy.

(6) Poskytovateľ služieb nesmie doručovať informácie komerčnej komunikácie elektronickou poštou, ak si ich príjemca služby vopred nevyžiadal.

Príloha 14 Kreslené postavičky projektu Ovce.sk, zdroj: http://www.ovce.sk/hry.phtml?pg=puzzle

Príloha 15 Leták o ochrane osobných údajov z projektu Ovce.sk, zdroj: http://sk.sheeplive.eu/sites/default/files/informacny_letak-poskytovanie_osobnych_udajov.pdf

Príloha 16 Komiks z projektu Ovce.sk,
zdroj: http://sk.sheeplive.eu/sites/default/files/komiks_netancuj_s_vlkom_a4_0.pdf


zodpovedne.sk
ovce.sk
CVAK
Cmuk
Cha cha!!
He he he
Jupii!
Stop...
???
CVAK
Hmm..
Vŕŕŕ..
???
!!!
!!!
Uh uh!
NENECHAJTE SA FOTOGRAFOVAŤ ALEBO NATÁČAŤ V SITUÁCIÁCH, KTORÉ BY MOHOL NIEKTO ZNEUŽIŤ ALEBO VÁS NIMI ZOSMIEŠNIŤ.