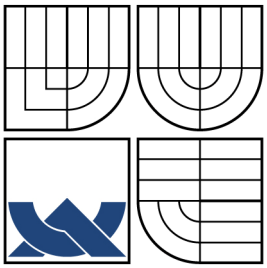
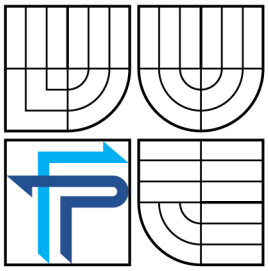


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

KRIMINALITA NA INTERNETU

INTERNET CRIMINALITY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

PETR ZELINKA

VEDOUCÍ PRÁCE
SUPERVISOR

JUDr. TOMÁŠ SOUKUP, BA

BRNO 2009

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2008/2009
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Zelinka Petr

Manažerská informatika (6209R021)

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

Kriminalita na internetu

v anglickém jazyce:

Internet Criminality

Pokyny pro vypracování:

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

Seznam odborné literatury:

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

Vedoucí bakalářské práce: JUDr. Tomáš Soukup

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

L.S.

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

V Brně, dne 15.05.2009

Anotace

Diplomová práce je zaměřena na problematiku internetové kriminality v České republice i ve světě. Popisuje a analyzuje jednotlivé typy této kriminality, použité metody a technologická zařízení. V další části jsou řešeny možné způsoby potlačení internetové kriminality pomocí technických či legislativních opatření.

Annotation

This diploma thesis focuses on the problem of internet crime in the Czech Republic and in the world. It describes and analyses various types of this criminality, used methods and technological equipment. In the second part of diploma thesis there are suggested possible technical and legislative precautions against internet crime.

Klíčová slova

Autorské právo, cracker, hacker, internet, kriminalita, malware, phishing, spamming, vir, warez.

Key words

Copyright, cracker, hacker, internet, criminality, malware, phishing, spamming, virus, warez.

Bibliografická citace:

ZELINKA, P. *Kriminalita na internetu.* Brno: Vysoké Učení technické v Brně, Fakulta podnikatelská, 2009. 58 s. Vedoucí bakalářské práce: JUDr. Tomáš Soukup, BA.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně.

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

V Brně dne 28. května 2009

vlastnoruční podpis autora

OBSAH

1 Úvod

V dnešní době jsou informační a komunikační technologie běžnou součástí našeho života, obklopují nás všude kolem nás, mnozí si nedokážou představit život bez nich. Tyto technologie nám ulehčují společenský i soukromý život ve všech možných oblastech – zdravotnictví, armáda, policie, veřejná správa, školství, bezpečnost, průmysl atd. Staly se tedy velkým přínosem pro lidskou společnost, ovšem v případě zneužití zároveň i ničivou zbraní.

V českém prostředí se nejčastěji setkáváme s termínem počítačová kriminalita, kterou můžeme chápat jako páchání trestné činnosti, v níž figuruje počítač jako souhrn technického a programového vybavení včetně dat, či pouze některá část počítače, případně více počítačů propojených do počítačové sítě.(17) Čili počítač se může stát předmětem i nástrojem trestné činnosti. Největší počítačovou sítí na světě je dnes internet, zejména prostřednictvím něj je páchána veškerá počítačová kriminalita.

Za internetovou kriminalitou dnes stojí např. nelegální šíření multimediálních dat (hudba, filmy a software chráněny autorskými právy, pornografie a jiná zakázaná data), různé útoky, malware, spamming, phishing atd. Boj s tímto druhem kriminality není vůbec jednoduchý a vyžaduje určitou pozornost.

Cílem mé práce je hlouběji tento sociální problém popsat, tedy jaké existují druhy útoků, metody útoků, jak se rozdělují škodlivé programy, tzv. viry a jak je tento druh kriminality vymezen v české legislativě. Čili v první části mé práce se zabývám popisem a analýzou internetové kriminality, ve druhé části popisuji možné vlastní návrhy k potlačení této kriminality. Dále v práci uvádím průzkum, který se zaměřuje na tuto problematiku, jeho zpracování a analýzu výsledků.

2 Charakteristika internetové kriminality

2.1 Popis a druhy internetové kriminality

Internetovou kriminalitu dělíme podle několika hledisek. Její základní dělení je kriminalita páchaná na počítači, nazývána též přímá počítačová kriminalita, a trestný čin s využitím počítače, nebo-li nepřímá počítačová kriminalita.

U prvého typu je subjektem trestného činu přímo počítač. Jedná se například o nepovolené kopírování počítačového programu, neoprávněné použití zařízení výpočetní techniky nebo odcizení dat uložených na počítačových médiích. Ve druhém případě jde například o využití počítače pro připisování fingovaných plateb, účtů nájemného, falešných objednávek zboží nebo i přípravu a plánování jiného trestného činu.

Trestná činnost páchaná na počítačích se dále objevuje i v těchto sférách, jak uvádí ve svém článku Martin Mikulec (14):

- Zneužití přístupu vnitřním pracovníkem
- Viry
- Krádež mobilního zařízení a jeho dat
- Phishing, kde je organizace podvodně reprezentována jako odesílatel
- Instant messaging zneužití
- Denial of service - odmítnutí služby
- Neautorizovaný přístup k informacím
- Bots uvnitř organizace
- Krádež dat zákazníka nebo zaměstnance
- Zneužití bezdrátové sítě
- Vniknutí do systému
- Finanční podvod
- Odposlech hesla
- Smazání stránek
- Zneužití aplikace na veřejné sítí

- Krádež chráněných informací
- Zneužití DNS serveru organizace
- Sabotáž

2.2 Pachatelé počítačové kriminality

Nejčastějšími pachateli internetové kriminality jsou z větší části mladí lidé, kteří mají příslušné odborné vzdělání a smysl pro abstraktní a logické uvažování. Někdy to mohou být i děti.

Pro hackery (průnikáře) je vniknutí do počítačových systémů jenom jakousi hrou nebo intelektuální výzvou. Je potřeba ovšem zmínit, že hackeři přes svou zdánlivou neškodnost vnikají nezákonným způsobem do informačních bank a mohou zcela ovládnout vybraný informační systém. Také podrývají autoritu organizací využívajících výpočetní techniku i firem zabývajících se ochranou informačních a počítačových systémů.(1)

Druhou skupinou pokoušející se proniknout do počítačových sítí jsou tzv. crackeři, jež není možno považovat za tolik neškodné individualisty. Jedná se o pachatele trestných činů, kteří svých schopností zneužívají k nelegálnímu získávání informací, k ovládání bankovních kont, k ničení programů atd. V dnešní době je tento pojem velice málo používán a obě skupiny se nazývají jednotně hackeři.

Hackeři i crackeři se organizují do skupin a sdružení, ve kterých si vzájemně předávají nebo prodávají své znalosti. Nejčastěji shromažďují své poznatky o heslech a strukturách různých počítačových systémů. Jejich motivací je osobní obohacení, v tom horším případě finanční zisk. Z motivů k počítačové kriminalitě byla sestavena následující tabulka (1, str. 25, 26):

- Pocit, že pachatel je natolik inteligentní, že se vyhne dopadení a trestu
- Názor, že velkému podniku nemohou uškodit poměrně menší ztráty
- Snaha kompenzovat nespokojenost s vykonávanou prací
- Touha po dobrodružství a riziku

- Mylné představy o účinnosti bezpečnostních opatření, kontroly vyšetřování a postupů, jimiž se zajišťuje způsobená škoda
- Pocit, že pracovník je podnikem vykořisťován a má proto právo si tuto újmu vynahradit
- Obecná povědomost o podvodech nebo jiném nezákonném jednání řídících pracovníků
- Nespokojenost s celým dosavadním průběhem vlastního života, neukojitelná potřeba bohatství, přepychu nebo výjimečnosti
- Pocit, že podnik ublížil obdivovanému člověku nebo příteli
- Vědomí, že podnik nikoho za kriminalitu nestíhal, nebo neuspěl ve stíhání pachatele

2.3 Metody počítačových útoků

Každá z metod má různé modifikace a varianty, mnoho metod je používáno kombinovaně. V podstatě je tedy můžeme rozdělit na metody přímého pronikání (aktivní metody), kdy pachatel projevuje otevřenou aktivitu se snahou získat především informace v počítačích zpracovávané a metody pasivního pronikání (mohou být kvalifikovány jako neúmyslné, mnohdy však jde o zastírání skutečných zájmů). (1)

2.3.1 Metody aktivního pronikání

Ničení nebo zcizení dat

Zpracovávané informace lze znehodnotit, zničit nebo odcizit ještě před jejich vložením do počítače při jejich zaznamenávání na disková média.

Metoda trojského koně

Jde o nelegální vložení instrukcí do počítačového programu tak, že program zpracuje původní úlohu v nezměněné podobě a navíc nepozorovaně plní úkoly pro pachatele.

Metoda zcizování malých sum z různých zdrojů

Malá množství peněz z různých zdrojů jsou při této metodě připisována na konto pachatele (např. při vyúčtování finančních vkladů, připisování a odpisování procent z jednotlivých účtů). Modifikací této metody je tzv. metoda zaokrouhlování. Zisk při zaokrouhlování může vznikat při velkém množství účtů po dlouhou dobu. Úspěch podvodu je v tom, že zákazník přichází o tak malé částky, že se zpravidla nedožaduje vysvětlení.

Neoprávněné užití aplikačních programů

Pomocí aplikačního programu může neoprávněný uživatel zneužít data v paměti počítače, může v nich provádět změny, neoprávněné přesuny atd.

Zneužití identifikátorů a hesel

Každá osoba, která pracuje s počítačem, jednotlivé terminály i datové soubory, které jsou v počítači zpracovávány, mají obvykle svůj identifikační kód (identifikátor nebo login) a heslo (password). Po zavedení příslušného identifikátoru a hesla je počítač schopen s uživatelem komunikovat a dané informace zpracovávat. Proto se pachatelé kriminality snaží identifikátor nebo heslo opsat, odpozorovat nebo zachytit na přenosných linkách při spojení mezi terminálem a počítačem. Podezřelými osobami mohou být operátoři nebo technický personál.

Časová bomba

Využití interních hodin počítače ke spuštění spícího programu, jehož pomocí mohou být okopírována nebo zničena zpracovávaná data. Pachatel se může dopustit trestného činu v době své nepřítomnosti.

Logická bomba

Tato metoda se podobá metodě časované bomby. Spouští se totiž při současném splnění jedné nebo několika logických podmínek zabudovaných do programu.

Odposlech

Odposlech neboli sniffing je technika, při které dochází k ukládání a následnému čtení TCP paketů. Používá se zejména při diagnostice sítě, zjištění používaných služeb a protokolů a odposlechu datové komunikace. (16)

2.3.2 Metody pasivního pronikání

Ke znehodnocení nebo zneužití informací zpracovávaných na počítačích může dojít také (1, str. 37):

- Poškozením paměťového média
- Chybnou funkcí čtecího zařízení
- Špatným označením souboru
- Záměnou dat
- Nesprávnými pokyny uživatele
- Chybnou adresou uživatele
- Různé vnější vlivy

3 Škodlivé programy - malware

Viry, červi a trojské koně jsou nebezpečné programy, které mohou způsobit poškození počítače a informací v něm obsažených. Mohou také zpomalit internet a dokonce se šířit z jednoho počítače do počítačů našich přátel, rodiny, spolupracovníků i jiných uživatelů webu. (8)

3.1 Viry

3.1.1 Virus

„Kód zapsaný s výslovným záměrem šířit sám sebe. Virus připojí sám sebe k hostitelskému programu a poté se pokusí šířit z počítače do počítače. Může poškodit hardware, software nebo informace.

Stejně jako závažnost lidských virů má rozsah od viru Ebola až k 24hodinové chřipce, závažnost počítačových virů se pohybuje v rozmezí od lehce nepříjemných až po naprosto destruktivní. Dobrou zprávou je, že skutečný virus se nebude rozšiřovat bez zásahu člověka. Někdo musí nastavit sdílení souboru nebo poslat e-mail, aby se virus rozšířil.“ (8)

3.1.2 Červ

„Červ je stejně jako virus formován tak, aby kopíroval sám sebe z jednoho počítače do jiného, ale činí tak automaticky. Nejprve převezme kontrolu nad funkcemi v počítači, které mohou přenášet soubory nebo informace. Jakmile se červ ocitne v systému, může se přenášet samostatně. Vysokým nebezpečím červů je jejich schopnost replikace ve velkých objemech. Červ může například rozesílat kopie sebe sama všem členům vašeho e-mailového adresáře, jejichž počítače poté provedou to stejné, což způsobí domino efekt nebo rozsáhlý síťový přenos, který může zpomalit pracovní sítě i Internet jako celek. Pokud se noví červi uvolní, velmi rychle se šíří. Zahlcují sítě a mohou způsobit, že vám (i komukoli jinému) bude dlouho trvat zobrazování webových stránek na Internetu.“ (8)

3.1.3 Trojský kůň

Jak jsem psal již výše, jedná se o program, který se chová jako prospěšný software, ovšem v pozadí svého chodu spouští nebezpečné reakce. Metoda snadného šíření spočívá v tom, že se šíří v programech, které většinou pocházejí z legitimních zdrojů, které působí v podvědomí uživatele jako důvěryhodné.

Na stránkách firmy Eset, která se zabývá bezpečností informačních systémů, je ale trojský kůň definován následovně:

„Na rozdíl od virů není tento typ škodlivého kódu schopen sebe-replikace a infekce souborů. Trojský kůň nejčastěji vystupuje pod spustitelným souborem typu EXE, který neobsahuje nic jiného (užitečného), než samotné ‚tělo' trojského koně. Odtud společně se skutečností, že trojan není připojen k žádnému hostiteli plyne, že jedinou formou dezinfekce je odmazání dotyčného souboru. Starší definice říkají, že trojan je program, vizuálně vypadající jako užitečný, ve skutečnosti však škodlivý." (9)

Jako jednoduchý příklad trojského koně může být program pojmenovaný „waterfalls.scr", který tvrdil, že je volně šiřitelný spořič obrazovky. Když se spustí, začne otevírat porty počítače a poskytovat crackerům vzdálený přístup do uživatelova počítače.

3.1.4 Způsob šíření virů

Ve skutečnosti se žádný virus a téměř žádný červ nemůže rozšířit, pokud se přímo neotevře a nespustí infikovaný program.

Většina nejnebezpečnějších virů se primárně šířila v přílohách e-mailů, to znamená v souborech posílaných s e-mailovými zprávami. Virus se spustí při otevření přílohy infikovaného souboru (příloha se zpravidla otevírá poklepáním na ikonu přílohy).

Je tedy dobré nikdy neotevírat e-mail, pokud obsahuje přílohu, kterou jsme neočekávali, a neznáme přesný obsah přiloženého souboru.

Viry a červi mají možnost zmocnit se informací mimo e-mailové aplikace a rozesílat se všem osobám uvedeným v adresáři. Jiné viry se mohou šířit prostřednictvím programů, které jsou staženy z internetu nebo ze zavirovaných disků či disket, které si půjčíme od kamarádů nebo dokonce zakoupíme v obchodě. Toto jsou méně obvyklé způsoby získání viru. Většina uživatelů si stáhne viry při otevření a spuštění neznámých příloh e-mailů. (8)

3.2 Spyware

3.2.1 Tracking cookie

„Jako cookie (anglicky koláček, oplatka, sušenka) se v protokolu HTTP označuje malé množství dat, která WWW server pošle prohlížeči, který je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Cookies běžně slouží k rozlišování jednotlivých uživatelů, ukládá se do nich obsah "nákupního košíku" v elektronických obchodech, uživatelské předvolby apod.

Pokud cookie využívá běžná stránka, pak o nic nejde (typickým příkladem může být server seznam.cz, kde se cookies využije pro zapamatování přihlašovacího jména do e-mailu).

Představme si ale situaci, kdy vstoupíme na nějakou webovou stránku (např. 123.cz), která je zapojena do reklamního systému a tudíž se na ní vyskytují i tzv. reklamní plochy (bannery). Pokud jsou tyto bannery stahovány z dalšího jiného serveru, může se i tento server postarat o vytvoření cookie (skrze stránku, na kterou jsme vstoupili - 123.cz). Jestliže někdy později navštívíme jinou stránku (např. 456.cz), která je taktéž zapojena do stejného reklamního systému, cizí server se může po své cookie poohlédnout (vytvořené při návštěvě 123.cz) a pokud je nalezena, o tomto si zapsat poznámku. Právě v tuto chvíli můžeme hovořit o tracking cookie ala ‘sledovací sušence‘, jelikož je v podstatě monitorován náš pohyb po Internetu, resp. pohyb po stránkách, které tenhle shodný reklamní systém využívají (tj. minimálně pohyb na serverech 123.cz, 456.cz).“ (23)

3.2.2 Spyware

„Spyware je program, který využívá Internetu k odesílání dat z počítače bez vědomí jeho uživatele. Na rozdíl od backdooru jsou odcizovány pouze ‘statistická‘ data jako přehled navštívených stránek či nainstalovaných programů. Tato činnost bývá odůvodňována snahou zjistit potřeby nebo zájmy uživatele a tyto informace využít pro cílenou reklamu. Nikdo však nedokáže zaručit, že informace nebo tato technologie

nemůže být zneužita. Proto je spousta uživatelů rozhořčena samotnou existencí a legálností spyware. Důležitým poznatkem je, že spyware se šíří společně s řadou sharewarových programů a jejich autoři o této skutečnosti vědí.“ (23)

V dnešní době existují dokonce různé snahy zabránit spywaru pomocí hardwaru. Za zmínku stojí Barracuda Networks Web Filter, který obsahuje filtry proti škodlivým programům nacházející se na webových stránkách.

3.2.3 Adware

„Obvykle jde o produkt, který znepříjemňuje práci s PC reklamou. Typickým příznakem jsou ‘vyskakující‘ pop-up reklamní okna během surfování, společně s vnucováním stránek (např. výchozí stránka Internet Exploreru), o které nemá uživatel zájem. Část Adware je doprovázena tzv. ‘EULA‘ - End User License Agreement – licenčním ujednáním. Uživatel tak v řadě případů musí souhlasit s instalací. Adware může být součástí některých produktů (např. BSPlayer). Ačkoliv nás reklama doprovází během celé činnosti s daným programem, odměnou je větší množství funkcí, které nejsou v klasické free verzi (bez reklamy) dostupné.“ (23)

3.2.4 Dialer

„Dialer je program, který změní způsob přístupu na Internet prostřednictvím modemu. Místo běžného telefonního čísla pro Internetové připojení přesměruje vytáčení na čísla se zvláštní tarifikací, např. 60 Kč / minutu (tzv. ‘žluté linky‘). Éra dialerů se ale týká pouze analogových tel.linek (dial-up) a netýká se ADSL a jiných moderních technologií.“ (23)

3.3 Rootkit

„Rootkit je pojem, který se ve spojitosti s operačním systémem Windows společnosti Microsoft objevil až nedávno. Původně jde o pojem z UNIXového světa, kde byly tímto pojmem označovány programy, které umožnily hackerovi zakrýt nekalou činnost, kterou prováděl. Za tímto účelem byly některé systémové programy (login, ls...) a systémové knihovny (typicky libproc.a) nahrazeny, popř. bylo využito možností modulů kernelu.

Jednoduše řečeno, Rootkit je program, který se snaží zamaskovat vlastní přítomnost v PC (přítomnost souborů, změn v registru Windows...), popř. přítomnost jiných aplikací v PC.“ (21)

4 Spamming

„Spam je nevyžádané sdělení, masově se šířící, a to nejčastěji pomocí internetu. Jako ‚spam‘ se nejprve označovala jen nevyžádaná příchozí e-mailová komunikace většinou reklamního charakteru (neuvěřitelné výhry, zájezdy, pochybné finanční transakce ve váš prospěch, nabídky zázračných léků, atd.). Postupem doby, ale tento nešvar pronikl i do diskusních fór, komentářů a instant messangingu (ICQ, Miranda, QIP, AIM, …). Pro spam se také vžilo označení UBE/UCE (Unsolicited Bulk/Commercial Email).“ (22)

Jelikož se jedná o široký pojem a v dnešní době velmi aktuální téma, chtěl bych se na něj blíže zaměřit nejen z technické stránky, ale i z právního pohledu.

4.1 Znaky spamu

Na spam se můžeme dívat z kvalitativního nebo kvantitativního hlediska. Z hlediska kvantity si všímáme hromadnosti šíření příslušných zpráv a záporného dopadu na komunikační svět, zatímco kvalitativní hledisko je spíše o obsahu zpráv a o její nulové nebo záporné informační hodnotě. Dále je charakteristické pro spam, aby určité sdělení bylo (3, str. 110):

- elektronické
- zasílané hromadně
- zasílané bez vyžádání

Díváme-li se na spam z hlediska kvantitativního s cílem ochránit informační infrastrukturu před zahlcením, můžeme doplnit ještě další znaky (3, str. 110):

- limitní počet adresátů
- limitní segmentace adresátů (např. lokální, mezinárodní nebo globální)
- limitní velikost zprávy
- následný efekt (skutečný negativní vliv na komunikační infrastrukturu)

Co se týče kvalitativního hlediska, sledujeme cíl ochrany adresáta a jeho právního postavení. Potom můžeme vymezit tato kritéria (3, str. 110):

- obchodní charakter sdělení
- podvodný charakter sdělení
- podvodná prezentace – například fingovaná adresa odesílatele
- skrytá funkčnost sdělení (např. u trojských koní šířených spamem)

Kdy ovšem můžeme říct, že se jedná o spam? Jako příklad absolutní nejistoty mě napadá tento: Mám odborné vzdělání v informačních technologiích a živím se jako programátor. Mimo zaměstnání se mi povedl vymyslet program, který dokáže z jakéhokoliv PDA udělat webkameru. Rozhodl jsem se tento software nabídnout k zakoupení několika mým kamarádům a známým prostřednictvím elektronické pošty. Těžko se dá v tomto případě tuto nevyžádanou poštu označit jako komerční spam. Obecně lze tedy říci, že žádná přesná definice pro spam neexistuje.

4.2 Účinnost spamu

Kouzlo spamu spočívá v minimálních nákladech na ještě efektivnější marketing. Ideální pro spamming jsou tyto informační kanály:

- e-mail
- diskusní fóra a blogy
- telekomunikační služby
- instant messengery

Z těchto uvedených kanálů je pro spamming nejrozšířenější email, jelikož je také oblíbený u koncových uživatelů díky nízkým nákladům. Dále získat tyto adresy z nejrůznějších volně dostupných zdrojů je relativně jednoduché. Z pohledu obsahu rozlišujeme tyto spamy (3, str. 112):

- obchodní
- kriminální (nebo jinak společensky nebezpečný)
- politický
- náboženský

První a druhá varianta je nejrozšířenější. V každém případě je ovšem hlavním cílem přitáhnout pozornost společnosti k nějakému druhu aktivit spammera, od těch prospěšných až po kriminální.

„Spammer je však skutečně úspěšný až tehdy, podaří-li se mu tuto pozornost (komunikační potenciál) přetavit do hodnoty, o kterou primárně usiluje, tj. do podoby obchodních vztahů, politického kapitálu, trestné činnosti atd. I v tomto směru je spam velmi atraktivním nástrojem, protože i zde může dojít k velmi příznivému poměru výkon/cena, tj. výnosy/náklady na rozeslání. Pro nejčastější případy obchodních spamů dokonce existují ekonomické modely s více proměnnými, s jejichž pomocí lze přesně

spočítat budoucí výnosnost spamu včetně kalkulace rizik plynoucích například z nasazení antispamových filtrů.

Skutečnost, že spam opravdu funguje, dokládají vedle teoretických kalkulací i empirická data. V tomto směru lze použít i poněkud banální, přesto však pádný empirický argument, že totiž spam fungovat musí, protože jinak by to spammeři přeci nedělali.“ (3, str. 113)

4.3 Vymezení spamu v české legislativě

V České republice byl článek 13 směrnice č. 2002/58/ES proveden hlavně zákonem č. 480/2004 Sb. Česká právní úprava pracuje s kategorií obchodního sdělení vymezeného v ustanovení § 2 písm. f zákona č. 480/2004 Sb. následovně:

Pro účely tohoto zákona se rozumí

f) obchodním sdělením všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost nebo je podnikatelem vykonávajícím činnost, která není regulovanou činností; za obchodní sdělení se považuje také reklama podle zvláštního právního předpisu. Za obchodní sdělení se nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle

Vymezení věcné působnosti zákona č. 480/2004 Sb. vzhledem ke spamu je pak konkretizováno ještě ustanovením § 7 odst. 1 následujícího znění:

(1) Obchodní sdělení lze šířit elektronickými prostředky jen za podmínek stanovených tímto zákonem

Z těchto uvedených ustanovení vyvozuje Radim Polčák ve své knize tyto závěry (3, str. 122):

- Zákon se vztahuje jen na obchodní spam – nezakazuje tedy politický, náboženský či jiný spamming.
- Zákon upravuje pouze rozesílání zpráv elektronickými prostředky – nevztahuje se tak na letákové nebo poštovní kampaně, naopak se kromě e-mailu vztahuje i na ostatní formy elektronické komunikace, tj. fax, SMS, diskusní skupiny apod.
- Za spam se nepovažují metadata, tj. linky a nejrůznější formy elektronických adres – není tedy zakázáno distribuovat elektronickými prostředky bez dalšího například linky na WWW stránky nebo e-mailové adresy.

Zákon č. 480/2004 Sb. nám dává určité možnosti, jak postupovat při rozesílání elektronické pošty bez rizika sankce následovně:

§ 7

1) Obchodní sdělení lze šířit elektronickými prostředky jen za podmínek stanovených tímto zákonem.
2) Podrobnosti elektronického kontaktu lze za účelem šíření obchodních sdělení elektronickými prostředky využít pouze ve vztahu k uživatelům, kteří k tomu dali předchozí souhlas.
(3) Nehledě na odstavec 2, pokud fyzická nebo právnická osoba získá od svého zákazníka podrobnosti jeho elektronického kontaktu pro elektronickou poštu v souvislosti s prodejem výrobku nebo služby podle požadavků ochrany osobních údajů upravených zvláštním právním předpisem, může tato fyzická či právnická osoba využít tyto podrobnosti elektronického kontaktu pro potřeby šíření obchodních sdělení týkajících se jejích vlastních obdobných výrobků nebo služeb za předpokladu, že zákazník má jasnou a zřetelnou možnost jednoduchým způsobem, zdarma nebo na účet této fyzické nebo právnické osoby odmítnout souhlas s takovýmto využitím svého elektronického kontaktu i při zasílání každé jednotlivé zprávy, pokud původně toto využití neodmítl.

4) Zaslání elektronické pošty za účelem šíření obchodního sdělení je zakázáno, pokud

a) tato není zřetelně a jasně označena jako obchodní sdělení,

b) skrývá nebo utajuje totožnost odesílatele, jehož jménem se komunikace uskutečňuje, nebo

c) je zaslána bez platné adresy, na kterou by mohl adresát přímo a účinně zaslat informaci o tom, že si nepřeje, aby mu byly obchodní informace odesílatelem nadále zasílány.

4.4 Správní postihy

Při nedodržení zákonných požadavků se vystavujeme nebezpečí správního postihu, konkrétně pokuty. Zákon č. 480/2004 Sb. svěřuje dozor nad dodržováním podmínek Úřadu na ochranu osobních údajů (ÚOOÚ). Nezákonný spamming lze nahlásit prostřednictvím jednoduchého on-line formuláře. Úřad totiž sám spamming nevyhledává, jelikož je to také v tom nepředstavitelně velkém množství nemožné. V některých případech sleduje dodržování stanovených podmínek ještě orgány profesních samospráv.

„Sankce za porušení obecných povinností stanovených § 7 zákona č. 480/2004 Sb. má formu pokuty a její horní mez je nastavena relativně vysoko na 10 mil. Kč. ÚOOÚ, který o udělení pokuty rozhoduje, má v tomto případě širokou možnost správního uvážení co do její výše, přičemž je veden pouze obecným pravidlem stanoveným v § 12 odst. 2, a to že *‚při stanovení výše pokuty právnické osobě se přihlédne k závažnosti správního deliktu, zejména ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž byl spáchán‘*.

Organizace profesní samosprávy mohou sankcionovat porušení speciálního ustanovení zákona, tj. § 8 odst. 3, uložením pokuty až do výše 1 mil. Kč. Jestliže spammer poruší navíc i stavovský předpis příslušné organizace, může mu být vedle zákonné pokuty uložena i další sankce v souladu s vnitřními disciplinárními předpisy. Vzhledem k tomu, že zákon a stavovské předpisy jsou na sobě vzájemně nezávislé,

může tedy dojít i k situaci, že bude spamming v návaznosti na způsob provedení postižen jen úřadem, jen komorou, nebo oběma institucemi zaráz.“ (3, str. 130)

Právnická osoba za správní delikt ovšem nebude odpovídat, pokud prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení povinností dle zákona zabránila.

5 Autorské právo

5.1 Autorské právo a jeho podmínky

„Autorské právo (anglicky označováno jako copyright) je odvětví práva, které popisuje nároky tvůrců tzv. ‚autorských děl‘, tzn. spisovatele, hudebníky, filmaře, programátory apod. na ochranu před nespravedlivým využíváním jejich tvorby. Prostřednictvím autorského práva poskytuje stát po jistou omezenou dobu autorům výlučnou možnost rozhodnout o některých aspektech využívání jejich děl. Autorské právo je součástí tzv. duševního vlastnictví.“ (25)

Pokud má být konkrétní dokument chráněn naším autorským zákonem, musí se rozlišovat dvě podmínky, a to zda je materiál takové povahy, že používá ochrany dle AutZ a zda v případě děl cizího původu spadá takové dílo do věcné působnosti našeho autorského zákona.

5.1.1 První podmínka

Je důležité, zda materiály, které lze na internetu nalézt, spadají pod definici díla dle platných českých norem. Autorský zákon definuje, co je dílem a může používat ochrany v § 2:

§ 2 Dílo

(1) Předmětem práva autorského je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam (dále jen "dílo"). Dílem je zejména dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické, dílo fotografické a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo kinematografické, dílo výtvarné, jako je dílo malířské, grafické a sochařské, dílo architektonické včetně díla urbanistického, dílo užitého umění a dílo kartografické.

(2) Za dílo se považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem a jejíž součásti jsou systematicky nebo metodicky uspořádány a jednotlivě zpřístupněny elektronicky či jiným způsobem, je dílem souborným. Jiná kritéria pro stanovení způsobilosti počítačového programu a databáze k ochraně se neuplatňují. Fotografie a dílo vyjádřené postupem podobným fotografii, které jsou původní ve smyslu věty první, jsou chráněny jako dílo fotografické.

Z výše uvedené části zákona vyplývá, že definice díla jakožto předmětu práva autorského je značně široká. Z pohledu uživatele se tedy dá dodat, že v podstatě veškeré dokumenty, které lze na internetu nalézt, jsou autorským dílem. Požadavek jedinečnosti (§ 2 odst. 1 AutZ) nebo pouze původnosti (§ 2 odst. 2 AutZ – počítačové programy a fotografie) může samozřejmě konkrétní materiál z ochrany vyloučit, ale půjde spíš o výjimky. To může například taková stránka, která bude na tak nízké úrovni, že po nějakém jedinečném výsledku tvůrčí činnosti autora nebude ani stopy nebo půjde o zcela primitivní kresbu, pár holých vět a podobně. Ovšem takový materiál nebude moc zajímavý pro zpřístupnění pomocí internetu, a tak z praktického hlediska se dá říci, že je potřeba raději při pochybnostech považovat každý materiál, který je vhodný k užití na internetu, za autorské dílo a jako takový za chráněný. Usuzovat z vlastního uměleckého

dojmu (který není žádným zákonným předpokladem), jaký daná stránka či obrázek na příslušnou osobu učiní, zda je nebo není splněn požadavek jedinečnosti či původnosti, je poměrně riskantní. Opačně se dá tedy postupovat pouze v případě těch materiálů, které jsou příkladmo uvedeny v § 2 odst. 6 (námět, denní zpráva, myšlenka, postup, matematický vzorec atd.), který dává vodítko k tomu, co se nedá považovat za dílo ve smyslu autorského zákona. Tyto výtvory nemohou být předmětem autorskoprávní ochrany, protože nejsou způsobilé být dílem. (2)

Dále je potřeba zmínit výtvory, které mají charatkter díla, ovšem zákon jim neposkytuje ochranu:

§ 3 Výjimky z ochrany podle práva autorského ve veřejném zájmu

Ochrana podle práva autorského se nevztahuje na
a) úřední dílo, jímž je právní předpis, rozhodnutí, veřejná listina, veřejně přístupný rejstřík a sbírka jeho listin, jakož i úřední návrh úředního díla a jiná přípravná úřední dokumentace, včetně úředního překladu takového díla, sněmovní a senátní publikace, pamětní knihy obecní (obecní kroniky), státní symbol a symbol jednotky územní samosprávy a jiná taková díla, u nichž je veřejný zájem na vyloučení z ochrany,
b) výtvory tradiční lidové kultury, není-li pravé jméno autora obecně známo a nejde-li o dílo anonymní nebo o dílo pseudonymní (§ 7); užít takové dílo lze jen způsobem nesnižujícím jeho hodnotu.
c) politický projev a řeč pronesenou při úředním jednání, autorovo právo k užití takových děl v souboru zůstává nedotčeno.

5.1.2 Druhá podmínka

Je potřeba zmínit problematiku věcné působnosti autorského zákona. „Problematika věcné působnosti autorského zákona je upravena v jeho závěrečných ustanoveních, a to konkrétně v ustanovení § 107. Podle ustanovení § 107 odst. 1 se ustanovení autorského zákona vztahují na díla autorů a umělecké výkony výkonných umělců, kteří jsou státními občany České republiky, ať byly vytvořeny nebo zveřejněny kdekoli. Autorský zákon se tedy bezpodmínečně a výslovně vztahuje na počítačové

programy vytvořené programátory, kteří jsou občany České republiky. V této souvislosti je však vhodné poznamenat, že v rámci komunitárního práva platí zákaz diskriminace na základě státní příslušnosti a v tomto smyslu jsou tak českým státním příslušníkům rovni státní příslušníci dalších států EU. Ochrana poskytovaná autorským zákonem počítačovým programům vytvořeným cizinci je pak zakotvena v dalších odstavcích tohoto ustanovení: ‚Na díla a umělecké výkony cizích státních příslušníků a osob bez státní příslušnosti vztahují se ustanovení tohoto zákona podle mezinárodních smluv, jimiž je Česká republika vázána a které byly vyhlášeny ve Sbírce zákonů České republiky, a není-li jich, je-li zaručena vzájemnost' (§ 107 odst. 2 autorského zákona). ‚Není-li splněna žádná z podmínek uvedených v odstavci 2, vztahuje se tento zákon na díla autorů a výkony výkonných umělců, kteří nejsou státními občany České republiky, byla-li poprvé v České republice zveřejněna, anebo má-li zde autor či výkonný umělec bydliště' (§ 107 odst. 3 autorského zákona).“ (24)

5.2 Rozmnožování díla

Rozmnoženinou se rozumí též kopie, jedná se tedy o duplikáty v elektronické formě. Může to být například počítačový program, internetové stránky, fotografie atd. AutZ o rozmnožování díla píše v § 13 takto:

1) Rozmnožováním díla se rozumí zhotovování dočasných nebo trvalých, přímých nebo nepřímých rozmnoženin díla nebo jeho části, a to jakýmikoli prostředky a v jakékoli formě.
2) Dílo se rozmnožuje zejména ve formě rozmnoženiny tiskové, fotografické, zvukové, obrazové nebo zvukově obrazové, stavbou architektonického díla nebo ve formě jiné trojrozměrné rozmnoženiny anebo ve formě elektronické zahrnující vyjádření analogové i digitální.

5.3 Počítačové programy

Počítačové programy vlastně patří do kategorie děl literárních, ale mají svůj specifický režim včetně licenčních smluv, půjčování apod. Zde uvádím z AutZ § 65 a některé vybrané pasáže z obsáhlého § 66:

§ 65 Obecná ustanovení

1) Počítačový program, bez ohledu na formu jeho vyjádření, včetně přípravných koncepčních materiálů, je chráněn jako dílo literární.

2) Myšlenky a principy, na nichž je založen jakýkoli prvek počítačového programu, včetně těch, které jsou podkladem jeho propojení s jiným programem, nejsou podle tohoto zákona chráněny.

§ 66 Omezení rozsahu autorových práv k počítačovému programu

1) Do práva autorského nezasahuje oprávněný uživatel rozmnoženiny počítačového programu, jestliže

a) rozmnožuje, překládá, zpracovává, upravuje či jinak mění počítačový program, je-li to potřebné k užití počítačového programu v souladu s jeho určením, včetně opravování chyb programu, není-li dohodnuto jinak,

b) zhotoví si záložní rozmnoženinu počítačového programu, je-li to potřebné pro jeho užívání,

c) zkoumá, studuje nebo zkouší sám nebo jím pověřená osoba fungování počítačového programu za účelem zjištění myšlenek a principů, na nichž je založen kterýkoli prvek počítačového programu, činí-li tak při zavedení, uložení počítačového programu do paměti počítače nebo při jeho zobrazení, provozu či přenosu,

d) rozmnožuje kód nebo překládá jeho formu při rozmnožování počítačového programu nebo při jeho překladu či jiném zpracování, úpravě či jiné změně, a to ať již sám nebo jím pověřená osoba, jsou-li takové rozmnožování nebo překlad nezbytné k získání informací potřebných k dosažení vzájemného funkčního propojení nezávisle vytvořeného počítačového programu s jinými počítačovými programy, jestliže informace potřebné k dosažení vzájemného funkčního propojení nejsou pro takové

osoby jinak snadno dostupné a tato činnost se omezuje na ty části počítačového programu, které jsou potřebné k dosažení vzájemného funkčního propojení.
2) Za rozmnožování počítačového programu se považuje i zhotovení rozmnoženiny, která je nezbytná k zavedení a uložení počítačového programu do paměti počítače, jakož i pro jeho zobrazení, provoz a přenos.
3) Informace získané při činnosti podle odstavce 1 písm. d) nesmějí být poskytnuty jiným osobám ani využity k jiným účelům než k dosažení vzájemného funkčního propojení nezávisle vytvořeného počítačového programu. Dále nesmějí být tyto informace využity ani k vývoji, zhotovení nebo k obchodnímu využití počítačového programu v podstatě podobného v jeho vyjádření nebo k jinému jednání ohrožujícímu nebo porušujícímu právo autorské.
4) Ustanovení odstavce 1 písm. d) a odstavce 2 nesmí být vykládána nepřiměřeně na újmu oprávněných zájmů autora ani v rozporu s běžným využíváním počítačového programu.
5) Není-li sjednáno jinak, ustanovení § 54 se na počítačový program nevztahují.

5.4 Trestní postihy

„Užití díla či jiného předmětu ochrany podle práv souvisejících s právem autorským bez souhlasu vykonavatelů práv k nim je porušením práva autorského resp. práv souvisejících s právem autorským a zakládá občanskoprávní i trestněprávní resp. přestupkovou či správní odpovědnost. Kdo svévolně, tedy bez souhlasu nositelů autorských práv a práv souvisejících s právem autorským, užívá předmět ochrany podle těchto práv, dopouští se neoprávněného zásahu do autorského práva a práv souvisejících s právem autorským a měl by si být vědom nepříznivých důsledků, které pro něho z jeho jednání vyplývají. Především mohou oprávněné osoby žádat, aby se protiprávního jednání zdržel a závadný stav napravil. Dále pak mohou žádat vydání bezdůvodného obohacení, a to podle § 40 odst. 3 aut. zák. ve výši dvojnásobku odměny, která byla na získání příslušné licence k užití obvyklá v době neoprávněného nakládání s předmětem ochrany, a poskytnutí přiměřeného zadostiučinění a to i finančního.

Ceny licence k šíření filmových děl jsou velmi vysoké; pohybují se od tisíců až desetitisíců amerických dolarů. Vznikla-li škoda, mohou oprávněné osoby požadovat

její náhradu. Škodou může být například snížení zisku vysílatele z poskytování licencí k užití vysílání přenosem třetím subjektům, především kabelovým televizím. Zároveň se však porušovatel autorského práva a práv souvisejících s právem autorským nemůže zříci ani trestní či přestupkové a správní odpovědnosti. Svým jednáním může naplnit trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 152 trestního zákona, za což mu hrozí trest odnětí svobody až na dvě léta, peněžitý trest až do výše 5 milionů Kč a propadnutí věci. Dopustí-li se pirátství ve značném rozsahu nebo získal-li jím značný prospěch hrozí mu kromě pokuty a propadnutí věci (tj. např. zařízení, kterým k porušování předmětných práv došlo) i trest odnětí svobody na 6 měsíců až 5 let.“ (11)

Konkrétní znění § 152 trestního zákona o porušování autorského práva zní takto:

§ 152 Porušování autorského práva

1) Kdo s dílem, které je předmětem ochrany podle práva autorského, nebo s výkonem výkonného umělce, zvukovým či obrazovým záznamem nebo rozhlasovým či televizním pořadem, které jsou předmětem práva příbuzného právu autorskému, neoprávněně nakládá způsobem, který přísluší autoru, výkonnému umělci, výrobci zvukového či obrazového záznamu, rozhlasové či televizní organizaci nebo jinému nositeli těchto práv, anebo kdo jinak tato práva porušuje, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci.

2) Odnětím svobody na šest měsíců až pět let nebo peněžitým trestem nebo propadnutím věci bude pachatel potrestán,

a) získá-li činem uvedeným v odstavci 1 značný prospěch, nebo

b) dopustí-li se takového činu ve značném rozsahu.

6 Warez

6.1 Warez obecně

Dle mého názoru je warez snad nejvíce problematická část celé internetové kriminality. Pojem warez je termín počítačového slangu a označuje autorská díla, se

kterými je nakládáno v rozporu s autorským právem. Warez má širší pojem, může také zahrnovat internetovou subkulturu, která se vůbec warezem zabývá. Lidé, kteří se zabývají warezem, jsou piráti. Nejsou to ovšem klasičtí vypalovači CD/DVD, kteří tuto činnost provádí za vidinou vysokých zisků. Warezové skupiny nemají z jejich činností žádný ekonomický prospěch, jde spíš o osobní hodnocení mezi touto komunitou. Stát bojuje s touto problematikou prostřednictvím softwarové policie.

6.2 Softwarová policie

Oddělení informační kriminality u Policie ČR se na centrální úrovni zaměřuje na odhalování, vyšetřování a monitorování kriminálních aktivit. Jeho úkolem je zajištění důkazního materiálu na internetu, servisní činnost a podpora jiným útvarům Jakmile některý z útvarů řeší případ v rámci problematiky IT, obrací se právě na toto oddělení a dostává se mu odborného servisu a podpory. Skupina pro informační kriminalitu rovněž zajišťuje vzdělávací aktivity uvnitř PČR a komunikuje s obdobnými zahraničními pracovišti. Různé informace zpracovává z poznatků vyplývajících z šetření jiných případů, využívá vlastní informátory a přijímá oznámení přímo od občanů. (7)

6.3 Warezové skupiny

„Každá skupina je vysoce organizovaná. Každý člen má své dané postavení a nemůže figurovat ve více konkurenčních skupinách. Hlavním šéfem je Leader, který kontroluje chod skupiny a shání nové členy. V jeho práci s údržbou skupiny a vytvářením pravidel mu pomáhají Councils. Další osobou je Supplier (zásobovač). Ten je extrémně důležitý, jelikož shání nový nevydaný software pro svoji skupinu. Jakmile ho získá, nahraje ho na server skupiny - DUMP. Často se může jednat o docela vysoko postavené lidi v některé společnosti. Cracker (SW) /Ripper (filmy) je další elementární člen warezových skupin. Je to ten, který odstraní nebo překoná ochrany daného produktu. Jakmile se na DUMPu objeví nový SW od Suppliera, dá se do práce. Carder je temná postava, která napadá slabě zabezpečené databáze serverů a krade databáze

kreditních karet. Z těch se pak kupuje například vybavení pro warezovou skupinu nebo samotný software. Vytvořený release pak otestuje Tester. Specifických členů je ještě mnohem víc, nicméně tihle jako základní přehled stačí.

Release pak putuje na Pre-server a pak TOPSITE - špičkové servery propojené 10Mb a rychlejším spojením, kam má přístup opět jen omezené množství lidí. Skupiny navíc mají s různými servery dohody o exkluzivitě - jejich release bude vydán nejdříve. Pak se release s crackem rozkopíruje i na ostatní servery a skupina, co to stihne nejdříve, tento závod vyhrála.

Tím ale teprve začíná cesta releasu od warezové skupiny k uživateli. To mají za úkol kurýrské skupiny typů ODAY, mp3, ISO. Jejich funkcí je co nejrychleji šířit data mezi servery. Top kurýři pak vytvářejí i hodnocení serverů a dostat se do jejich komunity je opravdu velmi obtížné, obvykle prakticky nemožné. Každý server má také svá vlastní pravidla a akceptuje jen určité druhy warezu. Každý server také vede statistiky, kolik který kurýr nahrál dat. To je jeden z důvodů, proč kurýři svou práci dělají a je to opět prestiž. Druhý důvod je zcela prozaický a to okamžitý přístup ke všemu warezu. Přísná formální pravidla zaručují velmi dobrý chod. Pak se software mezi obyčejné uživatele šíří pomocí tzv. PUB FTP serverů (FT server s anonymním přístupem a právy pro zápis) a boardů, tedy v podstatě jakýchsi nástěnek. Další zdroje šíření jsou pomocí P2P sítí, torrentů nebo speciálních serverů na sdílení dat. Pro snazší distribuci bývá tento software uložen jako CD obraz. Aby byl daný produkt dobře a rychle dostupný, bývá často nahrán právě na specializované servery a to v několika zabalených a zaheslovaných kusech, aby správci měli ztíženou možnost kontroly obsahu.“ (12)

Celé počínání pochopitelně není legální a skupiny jsou si toho dobře vědomy, proto pečlivě střeží své soukromí.

6.4 Pornografie

Tuto část počítačové kriminality bych zařadil právě mezi warez, jelikož se ve většině případů jedná o porušování autorských práv. Pornografie na internetu představuje nevýslovné nebezpečí, jelikož dohledat se jí je velice snadné, vše kolem ní je anonymní, právě proto nejvíce jsou ohroženy děti.

Další velké nebezpečí představuje sexuální nutkavost. „Pornografie zneužívá silné vizuální smysly muže, aby vzbuzovala sexuální touhu. Slibuje nereálné a podporuje falešná očekávání od vztahu. Pro mnohé je přitažlivá. To by nás nemělo překvapovat: pornografie bere něco ve své podstatě dobrého – sexuální vztah mezi muži a ženami – a pokřiví to. Přejídání je podobný jev: krátkodobý příjemný zážitek z něčeho, co má být pro lidské tělo přínosem, ale dlouhodobě působí jeho destrukci.“ (28) Říká se, že existují tři typy uživatelů internetové pornografie: rekreační uživatelé, uživatelé s rozvinutou sexuální nutkavostí a ohrožení (at-risk) uživatelé.

Šíření pornografie je v našem právním řádu postihováno zejména v § 205 TrZ:

Ohrožování mravnosti

(1) Kdo uvádí do oběhu, rozšiřuje, činí veřejně přístupnými, vyrábí nebo dováží pornografická díla písemná, nosiče zvuku nebo obrazu, zobrazení nebo jiné předměty ohrožující mravnost, v nichž se projevuje neúcta k člověku a násilí, nebo která zobrazují sexuální styk s dítětem, se zvířetem nebo jiné sexuálně patologické praktiky, bude potrestán odnětím svobody až na jeden rok, peněžitým trestem nebo propadnutím věci.

(2) Kdo pornografická díla písemná, nosiče zvuku nebo obrazu nebo zobrazení nabízí, přenechává nebo zpřístupňuje osobě mladší osmnácti let, nebo je na místě, které je osobám mladším osmnácti let přístupné, vystavuje nebo jinak zpřístupňuje, bude potrestán odnětím svobody až na jeden rok, peněžitým trestem nebo propadnutím věci.

Pojem pornografické dílo ovšem není žádným naším zákonem ani jiným právním předpisem definován. Za toto dílo se tedy v praxi považuje takové, jehož účelem je vyvolat sexuální vzrušení. Předměty určené k vědeckým, uměleckým, osvětovým cílům nelze považovat za pornografická díla. „Ve smyslu prvního odstavce tohoto paragrafu navíc samotné splnění požadavku na pornografické dílo k trestnosti nestačí. Zde se požaduje, aby se v pornografických dílech projevovala neúcta k člověku a násilí nebo některé, demonstrativně vyjmenované, podoby pornografie (např. díla, která zobrazují sexuální styk s dítětem, se zvířetem nebo jiné sexuálně patologické praktiky). Samotné zveřejňování pornografických děl (bez dalšího) trestné není (viz. odst.1). S ohledem na skutečnost, že ve většině případů však mají na Internetové

stránky obsahující pornografická díla přístup i osoby mladší osmnácti let, lze se domnívat, že nemá valný význam toto rozlišovat (samozřejmě s výjimkou stránek, na které je těmto osobám efektivně omezen přístup). Nepochybně to však bude mít vliv na nebezpečnost tohoto trestného činu pro společnost a tudíž i na samotnou sankci, případně na prokazování úmyslu (nejde totiž o nedbalostní delikt).“ (13)

7 Phishing

7.1 Definice phishingu

„Phishing (někdy převáděno do češtiny jako rhybaření) je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od obětí útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku. Tato stránka může například napodobovat přihlašovací okno internetového bankovnictví a uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze.“ (26)

7.2 Oběti phishingu

Obětí phishingu se mohou stát lidé a jsou jím přímo postiženi a dále to mohou být instituce, kde poškození měli účet. Tyto instituce musí kvůli phishingu investovat nemalé prostředky a zdroje do reklamací a zabezpečení, jinak pak klesá jejich důvěryhodnost, i když se do podvodu dostaly úplně nevinně.

„U nás zatím phishing není příliš rozšířený. Důvodů je několik. Především jsou zatím na světě větší a ekonomicky silnější oblasti - nekorunovaným králem jsou v dotyčném případě Spojené státy. Čili pokud budeme uvažovat jako phisher, samozřejmě se zaměříme na zajímavější oblast.

Na toto pak navazuje jazyková bariéra: čeština (i slovenština) je dosti specifický jazyk, phisheři zatím raději využívají jazyky univerzálnější (angličtina, španělština, francouzština apod.). Je to dáno třeba i náklady na ‘lokalizaci‘. A oblafnout

česko-slovenského uživatele anglicky psanou zprávu od renomovaného domácího bankovního domu bude jistě obtížné.

Náš trh je navíc malý - vystopovat phishera (mj. i díky pověstně pomalým mezibankovním převodům) by nebylo při troše dobré vůle nikterak obtížné. Otázkou je, zda by dobrá vůle existovala, ale na druhé straně je pochopitelné, že dokud jsou jiné možnosti, nikdo to pokoušet nebude. Ani phisher nemá důvod jít do většího než nezbytně nutného rizika, protože jinak by o své pracně odcizené prostředky mohl přijít a navíc se dočkat i dalších nepříjemných postihů (omezená svoboda pohybu na několik let nepodmíněně apod.).

Dalším problémem je, že phisheři zatím často útočí ‘naslepo‘. Prostě odešlou sto tisíc (milión, deset miliónů apod.) e-mailů a doufají, že mezi příjemci bude dostatek osob, které jsou klienty určité organizace. Takže je celkem jednoduché si uvědomit, že i z tohoto důvodu je malý český trh zatím nezajímavý. I při rozeslání deseti miliónů e-mailů po celém světě - kolik asi bude mezi jejich příjemci zákazníků největších českých bank?“ (22)

7.3 Phishing v ČR

Jak už jsem psal výše, tato metoda útoků není zatím v České republice tolik používána, i když v posledních letech několik takových útoků proběhlo. První takový útok podvodných e-mailů přišel v roce 2005, kdy v e-mailové schránce některých uživatelů internetu se začaly objevovat formuláře k vyplnění bankovních údajů, které byly určeny zákazníkům Citybank. Formuláře byly napsány velice dobrou češtinou, tudíž u běžných lidí nevzbuzovaly žádné větší podezření.

Největším a nejznámějším phishingovým útokem u nás byl nejspíš útok na Českou spořitelnu. V listopadu 2006 se objevily první zprávy, které ovšem byly napsány umělou češtinou, čímž se prozradily, ovšem i přesto mnoho českých uživatelů internetu těmto útokům podlehlo. Na Českou spořitelnu přišla v březnu 2008 druhá vlna útoků, tentokrát už šlo o e-maily psané angličtinou. Čeština byla pro tvůrce tohoto phishingu zřejmě natolik obtížná, že zvolil univerzálnější jazyk. Z toho vyplývá, že se nejspíš nejednalo o českého phishera.

7.4 Phishing ve světě

Úspěšnost phishingu ve světě je stále na vzestupu. Například ve Spojených státech měl phishing více než 5 mil. obětí, což je meziroční nárůst až 40%. Za oběť se počítá každý, kdo utrpěl finanční ztrátu, nepočítají se ostatní komplikace s tímto druhem nevyžádané pošty. Přesto, že phishing každým rokem stále roste, počet obětí neroste tak rapidně. Tohle téma je v posledních dvou letech velice diskutované a zavádí se stále různé preventivní filtry v e-mailových klientech, aniž by to běžný uživatel věděl. Letos se průměrná finanční újma snížila a činí zhruba 350 dolarů na incident.

Jak jsem již výše zmínil, kromě koncových zákazníků trpí hlavně instituce, tedy banky nebo různé platební systémy. Ve světě se stala velkou obětí phishingu například společnost PayPal, což mohli pocítit i čeští uživatelé tohoto platebního systému.

8 Návrhy na zlepšení bezpečnostní situace

8.1 Činnost softwarové policie

Jde o nedostatečnou činnost, kterou vyvíjí Policie ČR v oblasti informačních technologií. Příčinou jsou nedostatečné finanční prostředky, které Ministerstvo vnitra investuje do tohoto sektoru, což způsobuje nedostatek kvalifikovaných pracovníků v tomto oboru. Na odborníky pro internetovou kriminalitu jsou kladeny stejné nároky jako na odborníky zaměstnané ve firmách, jde především o programátory, počítačové experty atd., kteří jsou na rozdíl od těch policejních mnohem lépe platově ohodnoceni. Ke zvýšení aktivity softwarové policie je potřeba posílit její tým o tyto odborníky, což dosáhneme nabídkou motivující mzdy, která je rovna nejméně té ve firmách. Čili stát by měl investovat více finančních prostředků do této problematiky a Policie ČR by měla zajistit vhodnou reklamní kampaň pro nábor nových odborníků.

8.2 FTP servery

Jednou z největších metod šíření warezu po internetu je pomocí architektury klient – server, kde jednotlivý klienti komunikují vždy s centrálním FTP serverem. V praxi se jedná o webové stránky, na jejichž servery je možné anonymně uložit jakákoliv data, která následně může kdokoliv stáhnout. Tato služba vznikla pro zálohování vlastních dat a jako náhražka za posílání objemnějších souborů přes elektronickou poštu, která je nedokáže odesílat. Tyto tzv. Upload Servery se ale díky anonymitě a jednoduchosti staly jedním z hlavních nástrojů pro nelegální šíření multimediálních dat. Tyto severy se navíc zříkají odpovědnosti za jejich obsah.

Možné řešení tohoto problému vidím v povinné registraci. Po vyplnění osobních údajů a jejich zpětném ověření by uživatel mohl zdarma využívat služeb Free Upload Serveru, strach z předání osobních dat Policii ČR by mu zabránil uploadovat data chráněná autorskými právy. FTP servery ovšem tato opatření nikdy nezavedou, jelikož celý proces registrace by byl příliš zdlouhavý a mnoho uživatelů by odradil. Další možné řešení by mohla být tvrdší legislativa, která by majitelům těchto serverů přikazovala pravidelnou kontrolu obsahu disků.

8.3 Obrana proti phishingu

Nejlepší obranou je vždy udělat to tak, aby problém vůbec nevznikl, čili důležitá je prevence. Ovšem prevence v technickém podání je dosti složitá a dnes velice málo účinná, proto důležitá je individuální opatrnost. Antivirové programy totiž nedokážou stoprocentně čelit phishingovým útokům. Na druhé straně se poslední dobou objevují ochranné programy, které v sobě mají implementované antiphishingové technologie. Jedná se o kombinaci antivirové ochrany, firewallu a jiných bezpečnostních prvků. Fungují třeba tak, že na bázi firewallu monitorují odesílané informace a upozorňují uživatele na možná nebezpečí v případě, že se pokusí třeba i regulérně odeslat své citlivé údaje.

Phishing má dvě základní fáze:

- získávání informací
- nakládání s informacemi

Je tedy důležité pamatovat na to, že pokud útočník už získal citlivé informace, je zapotřebí zajistit, aby s nimi spáchal co nejmenší škody. Tedy například pokud jsme už citlivé informace útočníkovi odeslali prostřednictvím formuláře, je zapotřebí zavčas tyto údaje změnit, popřípadě zablokovat účet.

Jak jsem psal výše, je tedy potřeba být opatrný, hlídat si svá hesla a nevěřit těmto podvodným e-mailům. Rozhodně nevyplňovat formuláře obsažené v e-mailech nebo takové, na něž z e-mailu vede odkaz. Dále je důležité pravidelně kontrolovat svůj bankovní účet.

Odpovědnost za problém phishingu by měly převzít také komerční instituce. Americké banky už začínají povinně přecházet na silnější ověřování totožnosti, než jen pomocí jména a hesla. Stejně tak všechny významné instituce zveřejňují vyhrazené e-mailové adresy, kde je možné ověřovat některé požadavky nebo hlásit podezření na phishing.

Další možnou prevencí by mohlo být zavedení tvrdších pravidel i zákonů, a to na nadnárodní úrovni. Pomohlo by též zavedení přísnější registrace internetových domén (zvláště pro případné registrace podobných doménových jmen s již existujícími stránkami). To sice nejspíše spustí vlnu protestů svobodomyslných jedinců na internetu, ale na druhé straně přinese v tomto světě větší bezpečí. Správně nastavené podmínky slušné uživatele nikterak nepostihnou, podvodníkům minimálně zkomplikují život. Ovšem na druhé straně si musíme připustit, že nalézt onu tenkou hranici mezi svobodou a bezpečím je velmi obtížné.

Obecně se dá říci, že je potřeba různými mediálními prvky dostat informace o této hrozbě více do povědomí laické veřejnosti. Když například byly páchány útoky na Českou spořitelnu, instituce vydala informativní letáčky pro veřejnost, kde upozorňovala na hrozbu phishingu.

8.4 Obrana proti spamu

Zabránit spamu v našich e-mailových schránkách je prakticky nemožné, existují však určité metody, jak aspoň částečně zabránit průniku této nevyžádané pošty. Naprostá většina spamu je rozesílána z počítačů napadených různými viry a červy. Tyto nákazy otevírají v PC zadní vrátka (backdoor) a stávají se tzv. zombie − počítač je pod vlivem škodlivého kódu (potažmo spammera) a je připraven na rozesílání spamu. Ochranou proti napadení je aktualizovaný antivirový program.

Stejně jako u phishingu je zapotřebí vlastní opatrnosti, tedy uživatel e-mailové schránky by zbytečně neměl všude zveřejňovat svou adresu. Dobré je mít více e-mailů, např. jeden k různým registracím a další pro soukromé účely.

Další konkrétní metody boje jsou takové:

Blacklisting

Je to forma, která určuje, zda doručený e-mail je nebo není spam podle adresy odesílatele. Blacklisty (černé listiny) obsahují seznam IP adres, které jsou odesílateli spamu. Pokud blacklist označí e-mail za spam, následuje buď odmítnutí doručení nebo je e-mail přijat, ovšem je označen jako spam.

Graylisting

Funguje na stejném principu jako blacklisting, ovšem pracuje dynamicky. SMTP server, který provozuje greylisting, udržuje databázi, kde pro trojici (IP adresa, odesílatel, příjemce) je uvedeno, zda dopis s těmito atributy má být převzat k dopravě, nebo zda jeho převzetí má být dočasně odmítnuto. První dopis je odmítnut a je zaznamenán čas, kdy k tomu došlo. Po určitou dobu (typicky několik desítek minut) pak jsou dopisy s týmiž atributy odmítány. Po uplynutí této doby, pokud se původní SMTP server stále pokouší o odeslání dopisu, je záznam v databázi potvrzen a dopisy jsou naopak přijímány a dopravovány bez zdržení. Po další době (typicky několik málo týdnů) je záznam z databáze smazán, takže příští dopis bude opět pozdržen. K odstranění záznamu z databáze dojde také v případě, že v příslušném intervalu, kdy byly dopisy odmítány, se nepokusí původní SMTP server o znovudoručení. (15) Nevýhodou greylistingu je možné zdržení dopisů nebo že přijdou v přeházeném pořadí.

Filtrování podle obsahu dopisu

Předchozí zmíněné metody nedosahují potřebné účinnosti, a tak je třeba kombinovat metody. Je to z toho důvodu, že každý uživatel považuje za spam něco jiného. Předešlé metody se hodí hlavně pro odstranění těch nejznámějších a nejagresivnějších metod spamingu.

Filtry založené na pravidlech

Tyto filtry vyhledávají v e-mailech slovní spojení nebo samotná slova, která jsou pro spam typická (např. great offer, university atd.). Pokud filtr rozpozná spam, bodově ho ohodnotí. Hodnocení se sčítají a pokud dosáhne určitého počtu bodů, e-mail je považován za spam a nakládá se s ním podle nadefinovaných pravidel.

Filtry založené na schopnosti učení (bayesovské filtry)

Bayesovské filtry využívají prvky z A.I., což je umělá inteligence. Tyto filtry mají učící se režim, ve kterém jsou filtru předkládány e-maily označené jako spam (nežádoucí) a ham (povolené). Filtr si z těchto e-mailů vyextrahuje text a strukturu zpráv a ukládá si je do databáze. Filtr pak podle vytvořené databáze kontroluje každý nový příchozí e-mail a podle statistických údajů v databázi rozhodne, zda zpráva je spam či nikoliv. Nejčastěji se pro výpočet pravděpodobnosti používá vzorec, který navrhl matematik Bayes. Výhodou těchto filtrů je, že je může učit i počítačový laik a každý uživatel si může sám nadefinovat co je spam a co ne. Proto jsou také tyto filtry nejúčinnější. Přesto se bayesovské filtry používají i na serverech, kde učení probíhá pro všechny uživatele serveru společně. (15)

U nás bych možná udělal i úpravy v legislativě. Ministerstvo vnitra, pod které ÚOOÚ spadá (dříve to bylo ministerstvo informatiky), by mělo navrhnout antispamový zákon, který je skutečně zaměřen více na spam než na obchodní sdělení, a to v tom smyslu, že by to byl i trestný čin. Protože jakmile se dostaneme do oblasti trestního práva, vyšetřovací pravomoci jsou výrazně vyšší. Pak je tady ještě jedna chyba a to taková, že z hlediska mezinárodního jsou tři důležitá kritéria spamu a to je hromadnost zprávy, jestli někomu vznikla újma a jestli způsobil nějakou škodu. Náš zákon

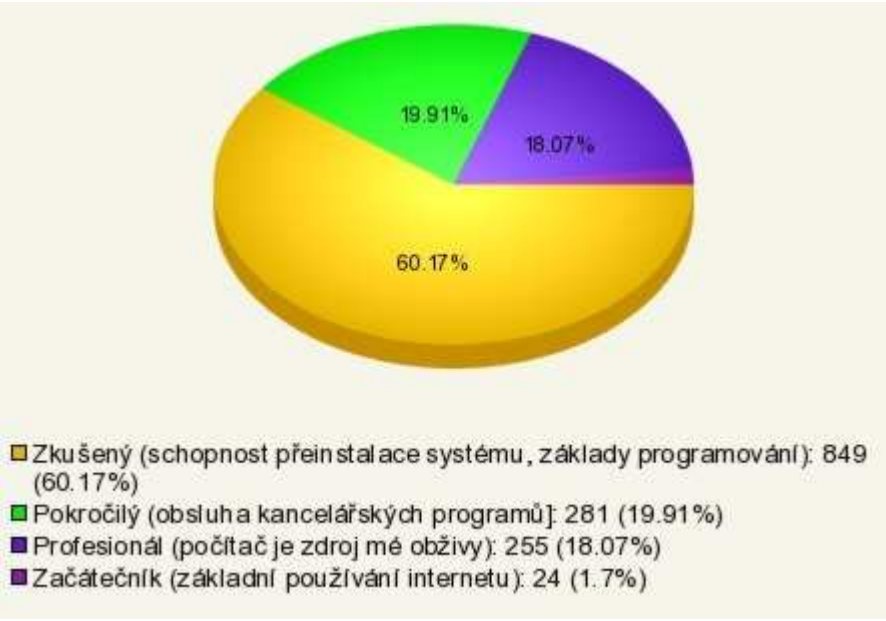
nepostihuje ani jedno z nich. ÚOOÚ tedy v rámci mezinárodní spolupráce velmi těžko uplatňuje jejich stížnosti, protože neobsahují to podstatné.

9 Průzkum na internetu

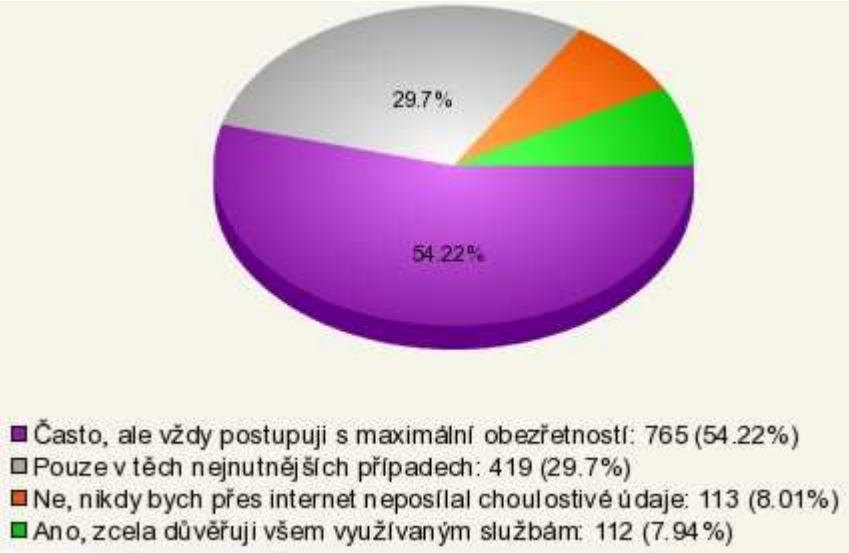
Na internetu probíhal dotazníkový průzkum na téma Internetová kriminalita, kterého jsem se také zúčastnil. Autorem tohoto průzkumu je Jan Srp, který mi poslal výsledky a s jeho laskavým svolením mi je dovolil interpretovat v mé bakalářské práci.

Průzkum se skládal s patnácti otázek a zúčastnilo se jej 1411 respondentů. Odpovědi jsou interpretovány pomocí grafů, pod nimi jsou vždy zobrazeny možné odpovědi, za každou odpovědí je uveden počet respondentů a procentuální rozložení.

1. Jak byste klasifikoval(a) svoji schopnost pracovat s počítači?

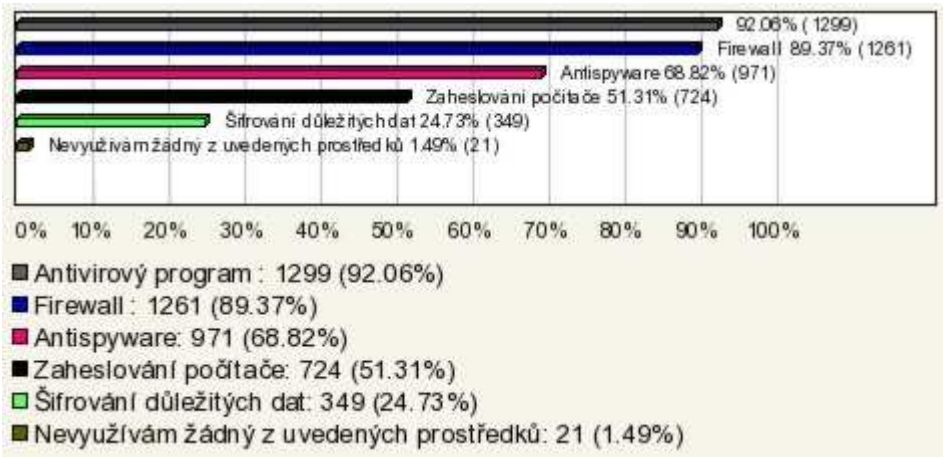


2. **Používáte internet pro práci s choulostivými daty (internetové bankovnictví, tajné komunikace, intimní fotky, ...)?**

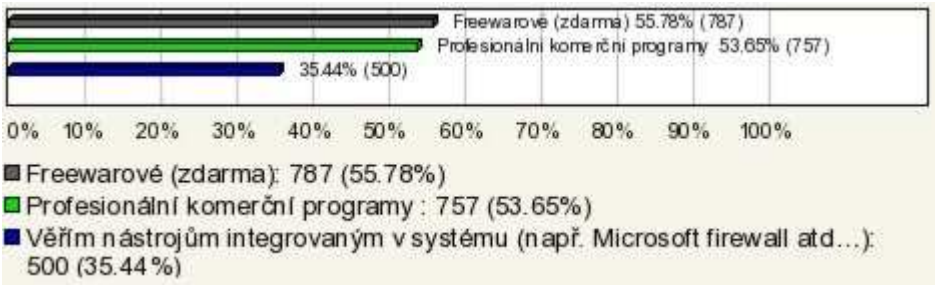


3. **Bojíte se, že byste se mohli stát terčem počítačové kriminality?**

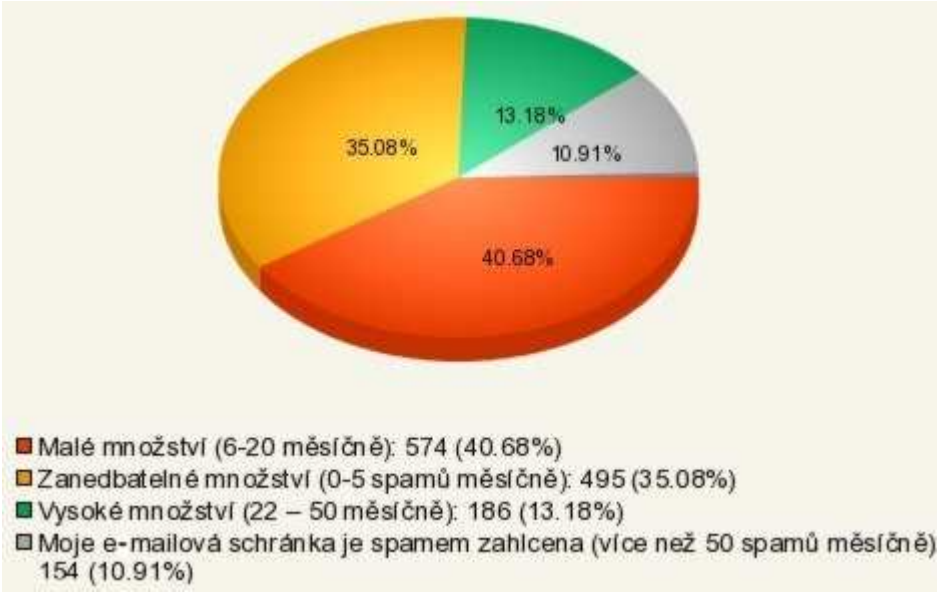
4. Zaškrtněte, které z následujících zabezpečení využíváte ve svém počítači:



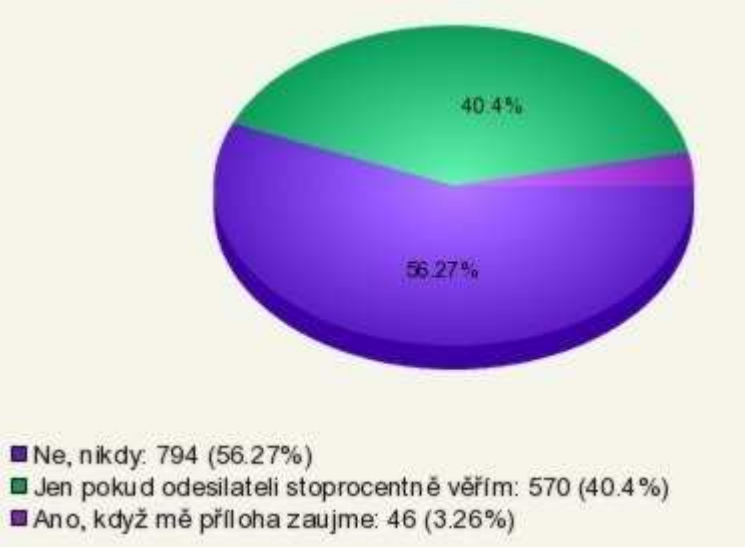
5. Jaké využíváte programy na zabezpečení?



6. Kolik spamů dostáváte do Vaší (nejpoužívanější) e-mailové schránky?



7. **Prohlížíte si nevyžádané přílohy u příchozí elektronické pošty?**



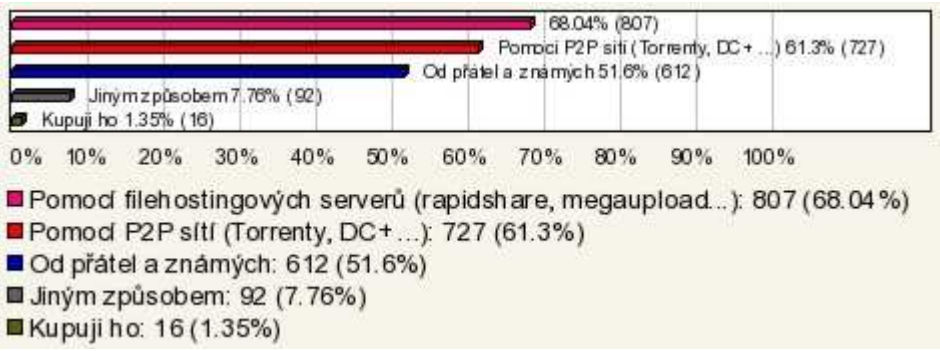
8. **Pokud byste z jakéhokoli důvodu chtěli navštívit stránky s xenofobním a rasistickým obsahem nebo stránky obsahující dětskou pornografii, myslíte, že byste je dokázali najít?**

9. Používáte ve svém počítači nelegální software?

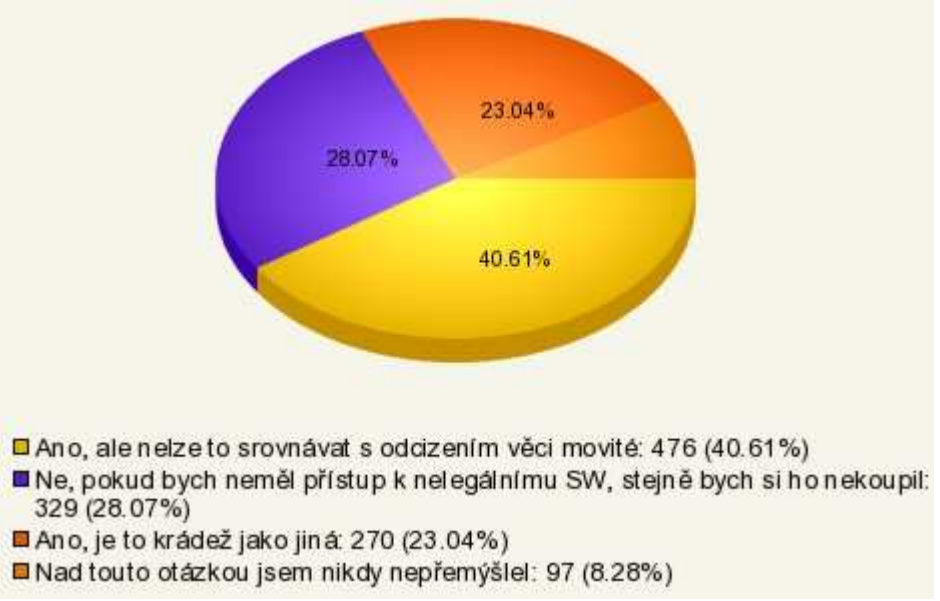
10. Ohodnoťte, nakolik se ztotožňujete s následujícími výroky (1-zcela nesouhlasím, 5- s výrokem se zcela ztotožňuji):

Odpověď	***Průměr***
Používám nelegální SW, protože je SW příliš drahý	3.837
Používám nelegální SW, protože tento SW je pro mě jinak nedostupný (u nás se neprodává, abandonware, nevlastním kartu schopnou platby po internetu…)	2.705
Používám nelegální SW, protože s koupeným SW jsou jen potíže (nutnost registrace, otravné protipirátské kontroly…)	2.645
Používám nelegální SW, protože je často k dispozici dříve než originál	2.704
Používám nelegální SW, protože nevidím důvod platit za něco, co mohu mít zdarma	2.542

11. Jakým způsobem si nelegální software opatřujete?



12. Vnímáte používání nelegálního softwaru jako krádež?



13. Zaškrtněte všechny položky, které platí pro heslo, jež používáte pro přístup k Vašim soukromým údajům (e-mail, diskusní fórum, ...)

14. Už jste se někdy stali terčem některé z následujících událostí?

15. Ohodnoťte jednotlivé druhy kriminality podle toho, jak myslíte, že jsou nebezpečné (1 - nepředstavuje žádné nebezpečí, 5 - představuje největší nebezpečí)

Odpověď	*Průměr*
Hacking (útoky na data, na webové stránky, e-mailové schránky atd…)	4.078
Počítačové viry a jiný škodlivý software	3.932
Propagace rasismu a xenofobie	3.544
Dětská pornografie	4.164
Porušování autorských práv	2.72
Spam (nevyžádaná reklamní pošta)	2.553
Internetové podvody (sociální inženýrství, phishing, nigerijské dopisy…)	3.879

Shrnutí

Naprostá většina uživatelů internetu, která se zúčastnila tohoto průzkumu, se hodnotí jako pokročilý až profesionál. Z toho vyplývají i následující výsledky. Více jak 60% respondentů běžně používá internet k práci s citlivými daty, bankovnictví atd. Zároveň si téměř 62% uživatelů uvědomuje, že jim na internetu hrozí nebezpečí. Proto kolem 90% lidí používá na svém PC různý obranný software, jako jsou antivirové programy nebo firewall. Pokud jde o to, zda lidé používají více komerční nebo freewarové programy, výsledky průzkumy ukázaly, že čeští uživatelé PC jsou na tom zhruba půl na půl, třetina dokonce důvěřuje nástrojům integrovaným v systému.

Co se týče spamu v ČR, nejsou na tom české e-mailové schránky tak špatně. Tři čtvrtiny uživatelů elektronické pošty uvedlo, že měsíčně dostávají do jejich nejpoužívanější e-mailové schránky max. 20 spamů. Při jejich prohlížení postupují velmi obezřetně, 56% vůbec přílohu neotvírá.

Jak jsem psal výše, úroveň znalostí práce s PC respondentů, kteří se tohoto průzkumu zúčastnili, značně ovlivnila jeho výsledky. Není divu, že na otázku „Pokud

byste z jakéhokoli důvodu chtěli navštívit stránky s xenofobním a rasistickým obsahem nebo stránky obsahující dětskou pornografii, myslíte, že byste je dokázali najít?“ více jak 63 % uvedlo, že by takové stránky dokázali najít.

Co se týče nelegálního softwaru, jeho používání je podle tohoto průzkumu celkem dost rozšířené. Hlavním důvodem jeho používání je vysoká cena. Nejvíce si uživatelé tento software opatřují prostřednictvím FTP serverů, P2P architektury nebo od přátel a známých. Není divu, že tolik lidí používá nelegální software. Vždyť více jak 40% lidí nepovažuje jeho používaní za krádež srovnatelnou s movitou věcí a dokonce 28% to nepovažuje za krádež vůbec.

Podle výsledků jaké uvedli respondenti, je používání hesel celkem na slušné úrovni. Nejvíce se stali terčem útoků jako je spam (98%), počítačový vir (92%) a phishing (56%). Za nejvíce nebezpečné útoky lidé považují dětskou pornografii, hacking, počítačové viry a podvody jako např. phishing.

10 Závěr

Ve vyspělém světě se výpočetní technika stala úplnou samozřejmostí, usnadňuje nám život a její vývoj jde nezadržitelně rychle dopředu. Tento trend nám přináší výrazně pozitivní přínos pro rozvoj naší společnosti, ovšem musíme brát v úvahu, že zároveň nám přináší i mnoho negativních jevů, mezi které patří právě počítačová kriminalita.

Ve své práci jsem se snažil tuto problematiku popsat a analyzovat. K tomu bylo zapotřebí prostudovat poměrně rozsáhlou odbornou literaturu, která se kriminalitou na internetu zabývá. Tato bakalářská práce nesleduje velké odborné cíle, snaží se spíš z použité literatury nastínit možné způsoby k potlačení této kriminality. Vymítit tuto kriminalitu ze světa úplně je totiž nemožné a nereálné.

Počítačová kriminalita probíhá prostřednictvím internetu, tedy prostřednictvím mezinárodní sítě. Je tedy nasnadě, že se jedná o mezinárodní problém a všechny státy se snaží s touto kriminalitou bojovat vlastními zbraněmi. Většinou státy svádí tento nekonečný boj prostřednictvím policie a pomocí legislativy. Boj proti internetové kriminalitě vedou i soukromé instituce, jako například Microsoft, neboť je v jejich zájmu, aby hackeři nepoškozovali a nedávali volně k dispozici jejich výrobky.

Útočníci, kteří tento druh kriminality nejčastěji páchají, jsou většinou mladí lidé, kteří disponují velmi dobrými znalostmi z oboru IT. A tato mládež si právě neuvědomuje, že počítačový program, stejně jako další nehmotné výtvory, je chráněn autorským zákonem a jeho krádež je to stejné, jako by se jednalo o odcizení movité věci. Ostatně tato skutečnost vyplývá i z průzkumu, který je součástí této práce. Je zapotřebí docílit toho, aby si tento fakt tito hackeři uvědomili. Toho bychom mohli dosáhnout například prostřednictvím médií.

Proti těmto útočníkům je potřeba posílit kriminální policii, která se zabývá porušováním autorských práv. Jak jsem psal výše, tato náročná práce je u Policie ČR finančně nedoceněna. Obecně se dá říci, že do sektoru informatiky je v České republice vyčleněno málo financí. Osobně si myslím, že tento obor je natolik důležitý, aby bylo znovu zřízeno Ministerstvo informatiky, které bylo zrušeno k 1. červnu 2007 a jeho agendu převzaly Ministerstvo vnitra, Ministerstvo průmyslu a obchodu a Ministerstvo pro místní rozvoj.

V současné počítačové kriminalitě je nespíš největším problémem volné šíření warezu, se kterým je nakládáno v rozporu s autorským právem. Toto šíření probíhá prostřednictvím internetu P2P sítí, pomocí FTP serverů nebo na diskových nosičích. Činnost softwarové policie může v této oblasti výrazně ovlivnit danou situaci, ovšem k tomu je zapotřebí i změna v technickém směru. Mám na mysli omezit anonymitu pro uživatele služeb FTP serverů, více hlídat obsah těchto serverů, popř. navrhnout program, tzv. robota, který by prohlížel obsah disků a tak dělal tuto velmi náročnou práci za člověka.

V této práci se dále zabývám nejrozšířenějším problémem mezi běžnými uživateli – spammingem a s ním spojeným phishingem. Kromě klasických metod boje proti spamu a individuální prevenci se zde zmiňuji o návrhu zvláštního zákona přímo určeného pro spam a jeho porušení zahrnout mezi trestné činy.

Kriminalita na internetu je velice široké téma a proto popsat všechny druhy útoků je téměř nemožné. V této práci jsem se zaměřil na tu část počítačové kriminality, která se nejvíce týká běžných uživatelů. Jelikož se počítačová gramotnost stále zvyšuje, je potřeba pamatovat na to, že spolu s ní se zvyšuje i kriminalita na internetu, proto musíme stále hledat způsoby, které nám zaručí, že virtuální svět bude bezpečnější.

11 Seznam použité literatury

11.1 Knižní zdroje

1) Bímová, A.: *Počítačová kriminalita a naše doba.* Praha: IDG Czechoslovakia, a.s., 1990. ISBN: 80-900872-2-1.

2) ČERMÁK, J.: *Internet a autorské právo.* 2. aktualiz. a rozš. vydání. Praha: Linde, 2003. ISBN 80-7201-423-4.

3) POLČÁK, R.: *Právo na internetu : spam a odpovědnost ISP*. 1. vydání. Brno: Computer Press, 2007. str. 150. ISBN 978-80-251-1777-4.

4) PROSISE, Ch. a MANDIA, K.: *Počítačový útok : detekce, obrana a okamžitá náprava.* Praha: Computer Press, 2002. 432 s.
ISBN 80-7226-682-9.

5) SMEJKAL, V.: *Právo informačních a telekomunikačních systémů.* Praha: C. H. Beck, 2004. 770 s. ISBN 80-7179-765-0.

6) SMEJKAL, V., SOKOL, T. a VLČEK, M.: *Počítačové právo.* Praha: C.H. Beck, 1995. str. 264. ISBN 80-7179-009-5.

11.2 Internetové zdroje

7) AMBROŽ, J. *Jak silná je naše "softwarová" policie. Lupa.* [online]. 24.5.2005 [cit. 18.3.2009]. Dostupný z WWW:
<http://www.lupa.cz/clanky/jak-silna-je-nase-softwarova-policie/>.

8) *Co je to virus, červ a trojský kůň? Microsoft.* [online]. [cit. 24.4.2009]. Dostupný z WWW: <http://www.microsoft.com/cze/athome/security/viruses/virus101.mspx>.

9) *Eset*. [online]. [cit. 24.4.2009]. Dostupný z WWW: <http://www.eset.cz/podpora/rejstrik>.

10) CHLEBOUN, M. *Stav internetové kriminality v Česku. Lupa.* [online]. 26.3.2004 [cit. 15.3.2009]. Dostupný z WWW: <http://www.lupa.cz/clanky/stav-internetove-kriminality-v-cesku/>.

11) *Jaké hrozí v ČR tresty za porušování autorského práva.* [online]. 25.7.2007 [cit. 13.3.2009]. Dostupný z WWW: <http://www.mpx.cz/ZAJIMAVOSTI/Jake-hrozi-v-CR-tresty-za-porusovani-autorskeho-prava.html>.

12) JINDRA, M. Warez. [online]. 2007 [cit. 29.3.2009]. Dostupný z WWW: <http://www.ventum.net/items/warez/show>.

13) MATEJKA, J. *Je šíření pornografie po Internetu trestné? Juristic.* [online]. 17.9.2001 [cit. 30.3.2009]. Dostupný z WWW: <http://trestni.juristic.cz/82136/clanek/trest3>.

14) MIKULEC, M. *Bezpečnost v síti (2.díl), počítačová kriminalita.* [online]. 14.4.2009 [cit. 22.4.2009]. Dostupný z WWW: <http://www.owebu.cz/pc-site/vypis.php?clanek=2488>.

15) MLEJNEK, M. *Spam – praxe a obrana. SWMag.* [online]. 26.11.2007 [cit. 3.5.2009]. Dostupný z WWW: <http://www.swmag.cz/154/spam-praxe-a-obrana/>.

16) OBR, J. S*niffing: Odposlech datové komunikace. IZBiz.* [online]. 6.3.2009 [cit. 12.4.2009]. Dostupný z WWW: <http://www.itbiz.cz/sniffing-odposlech-datove-komunikace>.

17) PAUKERTOVÁ, V. *Elektronická informační kriminalita.* [online]. 2.8.2006 [cit. 18.2.2009]. Dostupný z WWW: <http://www.ikaros.cz/node/3554>.

18) POLZER, J. *PayPal Phishing stále zákeřnější.* [online]. 13.6.2006 [cit. 12.4.2009]. Dostupný z WWW: <http://www.maxiorel.cz/paypal-phishing-stale-zakernejsi>.

19) PROTIVINSKÝ, M. *Internetová kriminalita (Z německých zkušeností). Kriminalistika.* [online]. 2008 [cit. 2.3.2009]. Dostupný z WWW: <http://web.mvcr.cz/archiv2008/casopisy/kriminalistika/2002/02_02/protivin.html>.

20) PŘIBYL, T. *Nebezpečí jménem phishing. SecurityWorld.* [online]. 1.9.2007 [cit. 11.4.2009]. Dostupný z WWW: <http://securityworld.cz/securityworld/nebezpeci-jmenem-phishing-964>.

21) *Rootkit.cz* [online]. [cit. 24.4.2009]. Dostupný z WWW: <http://www.rootkit.cz/go.php>.

22) *Spammer.cz* [online]. [cit. 24.4.2009]. Dostupný z WWW: <http://www.spammer.cz/go.php>.

23) *Spyware.cz* [online]. [cit. 24.4.2009]. Dostupný z WWW: <http://www.spyware.cz/go.php?p=spyware&t=clanek&id=9>.

24) *Věcná působnost autorského zákona.* [online]. [cit. 28.4.2009]. Dostupný z WWW: <http://licence.root.cz/vecna-pusobnost-autorskeho-zakona/>.

25) *Wikipedie* [online]. 17.2.2009 [cit. 26.4.2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Autorsk%C3%A9_pr%C3%A1vo>.

26) *Wikipedie* [online]. 12.4.2009 [cit. 14.4.2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Phishing>.

27) *Týdenní revize: phishing, piráti a Youtube. Lupa.* [online]. 14.10.2006 [cit. 8.4.2009]. Dostupný z WWW: <http://www.lupa.cz/clanky/tydenni-revize-phishing-pirati-a-youtube/>.

28) *Zneužívání internetu – Online pornografie.* [online]. [cit. 29.3.2009]. Dostupný z WWW: <http://www.ea.cz/Opustit_ghetto/Internetova_pornografie/IP_online>.

11.3 Ostatní zdroje

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

29) Zákon č. 140/1961 Sb., trestní zákon

30) Zákon č. 480/2004 Sb., o některých službách informační společnosti

12 Přílohy

Phishing v České spořitelně

Text podvodného emailu od České spořitelny z 10. října 2006, jak jej uvádí server www.root.cz. Zpráva vyzývá uživatele k přechodu na nový bezpečnostní systém z důvodu množících se případů podvodů. Nabízí také přímý odkaz, na kterém by měl údajný systém běžet.

Předmět: Ceska sporitelna - Pozor! Nove bezpecnostni standardy.
Od: "Ceska sporitelna" servise@csas.cz
Datum: Wed, 11 Oct 2006 14:45:52 -0500

Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci. Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku. Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu.

S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem. Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu. Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.

Vy jste byl(a) zvolen(a) jako jeden z ucastniku finalniho stadia testovani systemu. V soucasne dobe Vam navrhujeme vyuzit odkaz https://www.servis24.cz/ebanking-s24/ a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system. V aktualnim stadiu provozu jsou mozne nektere nesrovnalosti. Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji.

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

S pozdravem, Oddeleni Banky pro ochranu pred frodem.

Existuje i varianta rozesílaná s diakritikou. E-maily přicházely z celého světa z mnoha různých serverů a nebyly doručovány jen klientům České spořitelny, ale obecně na velké množství českých schránek. Podvodný e-mail obdrželo asi 100 tisíc uživatelů freemailu na Seznamu.

Odkaz, který je součástí zprávy a na první pohled ukazuje na regulérní stránky České spořitelny, však v sobě skrývá odkaz na úplně jiný server s falešnou webovou stránkou. Na této adrese byl v době rozeslání podvodných e-mailů spuštěn webový server s falešnou stránkou, která se tváří jako přihlašovací stránka České spořitelny.

Vše vypadá naprosto reálně, stránka dokonce obsahuje odkazy na standardní stránky Servis24 České spořitelny. Při zadání klientského čísla dokonce stránka upozorňuje na to, že číslo musí mít alespoň deset znaků. Funguje také virtuální klávesnice, s jejíž pomocí je možné zadat heslo (viz. obrázek).

Proti reálné přihlašovací stránce je ovšem na té „nové” navíc položka Bezpečnostní kód. Jedná se o nový kód, který byl nedávno rozesílán klientům České spořitelny. Pomocí tohoto kódu je možné změnit telefonní číslo, na které jsou zasílány bankovní bezpečnostní kódy.

Autor podvodných stránek se tak jistě chtěl pojistit a požaduje proto po uživatelích i toto číslo. Pokud by pak chtěl pracovat s cizím účtem, může změnit toto číslo a nechat si zasílat certifikační zprávy na vlastní telefon.

Pokud se do formuláře zadají údaje, objeví se prázdná stránka s hlavičkou, pod kterou je vidět jen „Ok” a dál se nic neděje. Uživatel totiž právě naletěl podvodníkům a vydal jim své přihlašovací informace. (www.root.cz)

„Většina klientů díky dobré informovanosti na podvodný e-mail nereagovala, ale informovala banku. Česká spořitelna má v současné době informaci, že někteří klienti na e-mail přesto reagovali, avšak počet těchto klientů zatím není znám. Důležité je, že nedošlo k žádnému poškození klienta, tedy nebyly odčerpány neoprávněně žádné finanční prostředky z účtu klientů ČS,” píše se v tiskové zprávě České spořitelny.