Počítačová kriminalita a terorismus

PC criminality and terrorism

Josef Řeha

Bakalářská práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2007/2008

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Josef ŘEHA**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Informační technologie**

Téma práce: **Počítačová kriminalita**

Zásady pro vypracování:

1. **Historický přehled.**
2. **Vymezení počítačové kriminality.**
3. **Formy počítačové kriminality.**
4. **Obrana před počítačovou kriminalitou.**
5. **Vliv vývoje kybernetiky a výpočetní techniky na počítačovou kriminalitu.**
6. **Výběr a rozbor některých případů počítačové kriminality.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Smejkal, V. Právo informačních a telekomunikačních systémů. Praha: C.H. BECK, 2004.**
2. **Matějka, M. Počítačová kriminalita. Praha: Computer Press, 2002.**
3. **Smejkal, V. Počítačové právo. Praha: C.H. BECK, 1995.**
4. **Smejkal, V. Internet a ÔÔÔ. Praha: Grada Publishing, 2001.**
5. **Čandík, M. Základy informační bezpečnosti. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004.**

Vedoucí bakalářské práce: **Ing. Radek Šilhavý**
Ústav aplikované informatiky

Datum zadání bakalářské práce: **20. února 2008**

Termín odevzdání bakalářské práce: **5. května 2008**

Ve Zlíně dne 20. února 2008

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce pojednává a počítačové kriminalitě a terorismu. Nejprve se zaměřuje na historii po jednotlivých etapách jejího vývoje. Po stanovení základních definic počítačové kriminality se práce soustředí na rozbor jednotlivých trestných činů a motivaci pachatelů provádějících tuto trestnou činnost.

Pojednává i o metodách prevence a vlivu počítačové kriminality v budoucnosti. Závěr patří konkrétním trestným činům provedeným ve spojitosti s použitím počítače a byla tak naplněna podstata počítačové kriminality.

Klíčová slova: PC kriminalita, terorismus, hacker

ABSTRACT

This bachelor work handle about computer criminality and computer terrorism. First survey on story after period its evolution. After assesment basic definition computer criminality work concentrate on analysis single crimes and hackers motivation examining this punishable activity.

It´s handle also about prevention methods and owing to computer criminality in future.

The end belongs to concrete crime effected in continuity computer application so impletion essence computer criminality.

Keywords: PC criminality, terrorism, hacker

Rád bych poděkoval vedoucímu mé bakalářské práce Ing. Radkovi Šilhavému za jeho podmětné připomínky, rady, profesionální vedení při tvorbě bakalářské práce a za odborné konzultace.

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně 15.5.2008

…….
Podpis diplomanta

OBSAH

ÚVOD

Tématem této bakalářské práce je problematika počítačové kriminality a terorismu. Tedy problematika, která je dnes čím dál více aktuální. Již delší dobu dochází k rozvoji moderních informačních technologií a tím i počítačové kriminality samotné. S takto bouřlivým vývojem je možné se setkat na každém kroku, zasahuje téměř do všech oblastí našeho života. Uplatnění těchto technologií je široké od umění až po erotiku. Dnes už si málokdo dovede život bez těchto technologií představit. Je třeba si ale uvědomit, že přínos nových technologií nemá pouze pozitivní význam, ale kromě užitku a zábavy sebou přináší i stinné stránky a negativní důsledky. Právě jedním z těchto nežádoucích vlivů je počítačová kriminalita. Stala se fenoménem dnešní doby, představuje obrovskou hrozbu pro celou společnost. Její přínos na páchání trestné činnosti se rok co rok zvyšuje a proto je potřeba proti počítačové kriminalitě a terorismu bojovat.

Toto téma jsem si vybral proto, že je a stalé bude velmi aktuální a diskutované. Nikdo nemůže dopředu odhadnout, jakým směrem se počítačová kriminalita bude vyvíjet v horizontu dalších několika let a právě to činí počítačovou kriminalitu zajímavou ale i nebezpečnou zároveň.

Ve své práci jsem se snažil nastínit problematiku počítačové kriminality, její rozdělení, druhy provedení, možnosti obrany a její vliv do budoucnosti. Dále jsem provedl rozbor některých konkrétních případů počítačové kriminality a její propojení s terorismem.

V první části jsem zdokumentoval významné milníky historie počítačové kriminality od 19. století až po 90. léta. Poté jsem vymezil základní definici počítačové kriminality a její základní děleni. Velký důraz jsem kladl na zpracování jednotlivých forem počítačové kriminality, kde jsem se zaměřil na aktuálně platné hrozby, jakými jsou *spamming, phishing nebo pharming.* V části ochrany jsem vymezil pojmy psychologické a technologické prevence. V poslední části jsem popsal konkrétní případy počítačové kriminality u nás i ve světě. Vybral jsem ty případy, které byly pro mne zajímavé ať už svým dopadem nebo způsobem provedení.

I. TEORETICKÁ ČÁST

1 HISTORICKÝ PŘEHLED

První počítačový zločin se stal ve Francii roku 1801. Na jeho počátku stál tkadlec a vynálezce Joseph – Marie Jacquard.

Mechanická práce u tkalcovského stavu ho přiměla k automatizaci tohoto procesu. Mechanickému stavu zadal vzor tak, že jej naprogramoval. Stav tak dokázal automaticky a opakovaně tkát složité vzory, které byly vyražené podle čtverečkovaného rastru na děrných štítcích – tzv. děrné štítky pro řízení strojů. Zaměstnanci Jacquardovi továrny se zavedením těchto štítků začali obávat o zaměstnání a živobytí, a tak pomocí série sabotáží donutili Jacquarda od tohoto vynálezu upustit.

1.1 60. léta

V roce 1961 se v institutu MIT (Massachusetts institute of technology) objevují první počítačový hackeři. V této době se vlastně poprvé objevilo slovo hacker. Tímto termínem hackeři, se označovala zájmová skupina nadšenců, kteří si hráli s elektrickými vláčky. Vláčky, koleje i výhybky různě přestavovali „hackovali“ tak, aby vše fungovalo co nejrychleji a taky, aby se odchýlili od původního konstrukčního návrhu.

1.2 70. léta – období tzv. telefonních pirátů

Mladí chlapci, kteří obsluhovali telefonní ústředny, si dlouhý čas během služby krátili tím, že hovory náhodně přerušovali, chichotali se do telefonu anebo k sobě spojovaly hovory, které k sobě nepatřily. Postupně začali pronikat do telefonního systému New Yorku, vytvářeli vlastní spojení a snažili se zjistit, jak systém vlastně funguje.

Hlavním cílem těchto „ telefonních pirátů “ bylo dobývání telefonních ústředen po celém světě, za účelem hojného a hlavně bezplatného telefonování.

V této době (období po Vietnamské válce) se začínají objevovat skutečné kořeny moderního hackerského undergroundu. Ze zapomenutého anarchistického proudu Hippies se vyprofilovalo hnutí s názvem Yippies. Své jméno vytvořili z názvu fiktivní „YOUTH INTERNATIONAL PARTY” (Mezinárodní strany mládeže).[1]

Jedním z hlavních představitelů tohoto hnutí, které vzniklo kvůli odporu proti vietnamské válce, byl Abbie Hoffmann (1939–1989). Bývá nazýván duchovním otcem hnutí Yppies. Byl hledán federální policií. Na útěku strávil asi 7 let, postupně se ukrýval

v Mexiku, ve Francii a v USA. Věnoval se manipulaci se sdělovacími prostředky. Využíval televizní společnosti, kde pomocí různých lží, podvodů se záměnou osob a dalších nekalých praktik pobuřoval policisty, federální soudce, ba i dokonce prezidentské kandidáty.

Hoffmann byl rovněž nadaným publicistou. Jeho nejslavnějším dílem byla kniha s názvem *Ukradni tuto knihu*. V knize podával návody stoupencům svého hnutí na to, *jak podojit systém podporovaný zkostnatělými trubci.* [6]

Ke komunikaci se svými soudruhy využíval a spolubojovníky telefon, za který neplatil. Místo mincí totiž používal levná mosazná těsnění. Během vietnamské války existoval za použití telefonu zvláštní daňový příplatek. Yppies nejdříve tvrdili, že obcházejí telefonní poplatky proto, že z principu odmítají přispívat na nemravnou a nezákonnou válku. Toto tvrzení se ukázalo pouze jako zástěrka, protože hnutí Yppies se svou činností pokračovali i po ukončení války. Hnutí se začalo systémově zabývat tím, jak obelstít telefonní automaty, ústředny, prodejní a parkovací automaty a nakonec i počítače.

V roce 1971 začal Abbie spolu se svým spolupracovníkem známým pod přezdívkou

„ Al Bell“ publikovat v časopise *International Party line* (Politika mezinárodní strany mládeže). V tomto časopise zveřejňoval a propagoval různé metody šizení, zvláště pak způsoby obelstění telefonu.

A. Hoffmann si nechal udělat plastickou operaci obličeje a zároveň přijal novou identitu, pod jménem Barry Freed. V roce 1989 měl za podivných okolností spáchat sebevraždu.

Dalším z pirátů působících v této době byl John Draper (nar. 1944). Říkal si Captain Crunch, podle případu, kterým se v roce 1971 proslavil. Cap ¨n¨ Crunch se totiž jmenovala značka ovesných cereálií, ke kterým byla jako dětská hračka přibalovaná píšťalka. Draper zjistil, že tato reklamní píšťalka vydává zvuk, jehož frekvence je přesně 2600 Hz.

Zvukem o této frekvenci získal přístup k dálkové ústředně telefonní společnosti. Draper poté sestrojil krabičku, která se při společném použití s píšťalkou nasměrovala na mikrofonní vložku telefonu, a umožnila tak zdarma provádět dálkové i mezinárodní hovory. Tento trik byl později zveřejněn již v zmiňovaném časopise *Youth International Party Line.*

Právě Draperova objevu využili v roce 1975 Dva členové *Homebrew Computer Club of California* a pozdější zakladatelé firmy *Apple Computters*.

Steve Jobs a Steve Wozniak, začali podle návodu uveřejněného v časopise podomácku vyrábět a později i prodávat tzv. modré krabičky, které produkovaly různé tóny a umožňovaly „hacknout“ telefonní systém. Díky zveřejňování těchto „technických fint“ a návodů v různých časopisech, se nelegální telefonování značně rozrostlo a dostávalo nový název, tzv. phreaking (telefandovství).

1.3 80. léta – Zlatá éra BBS

Telefonní piráti se postupně zaměřují na počítače a vznikají první BBS systémy, díky kterým vlastně dochází ke spojení světa telefonů a počítačů. V roce 1978 sestrojil Ward Christensen první BBS. [18]

Co to je BBS? Je to systém elektronických nástěnek, jak napovídá název („BULLETIN BOARD“), které jsou rozděleny podle témat, do kterých mohou uživatelé přispívat podobně jako v diskusních fórech. Z technického hlediska je BBS systém vlastně počítač (je to server, na kterém je spuštěn program umožňující přístup uživatele ke svým zdrojům). Pomocí těchto nástěnek, např. Sherwood Forrest, Catch 22 se mohli piráti a hackeři navzájem kontaktovat a vyměňovat si různé návody a tipy, jak například sdílet ukradená čísla kreditních karet.

Systém BBS byl vlastně předchůdcem Internetu. K připojení do systému BBS používal uživatel telefonní linky a počítač – respektive modem. Tyto technologie se začínají šířit do domácností až na počátku 80. let. Přesně řečeno v srpnu 1981, kdy společnost IBM představila svůj první počítač IMB 5150. V tomto období se začínají objevovat první hackerské skupiny. V USA to byla LOD Legion of doom (legie zkázy nebo legie soudného dne) a skupina Chaos Computer Club v Německu. [1]

1.3.1 Rok 1982 – Vynález prvního CD - ROM

Rok 1982 byl určitým posunem dopředu v období počítačového pirátství.

17. srpna roku 1982 byla v německém Hannoveru zahájena masová výroba nových digitálních médií s názvem CD-ROM. [19] Toto médium pro digitální záznam dat posunulo počítačové piráty o řád výš a výrazně jim umožnilo zvýšit jejich aktivity. Již nemuseli používat pro záznam dat diskety, které měly malou kapacitu a byly velmi

náchylné na poškození, které vedlo k následné ztrátě dat. Kompaktní disk neboli CD, disponoval na svou dobu obrovskou, až neuvěřitelnou kapacitou, která byla 650 MB.

CD disky se začaly nejprve používat v hudební oblasti k záznamu hudebních nahrávek. Jako nosiče pro uložení dat se začaly používat na začátku 90. let, kdy se v prodeji objevila první CD-ROM mechanika, která sloužila ke čtení CD nosičů. O něco později byla vynalezena první CD-R mechanika, která uměla data nejen číst, ale i zaznamenávat, neboli vypalovat. Tyto CD-ROM a CD-R mechaniky byly zpočátku velmi pomalé a navíc velmi drahé. Zlom nastal v roce 1996, kdy byly na trh uvedeny první DVD disky.

Ceny CD-ROM a CD-R mechanik (neboli vypalovaček) začaly výrazně klesat a jejich koupi si mohla dovolit většina uživatelů. Téměř každý se tak mohl stát potencionálním počítačovým pirátem.

1.3.2 Rok 1983 – Filmy s hackerskou tématikou a první zatčení hackerů

Film War Games (někde pod názvem dětské hry) přispěl k rozšíření systému BBS jako zdroje zábavy. Jednalo se o thriller, který dával možnost nahlédnout pod pokličku hackerského světa. Film uvedl problematiku hackerů a hackerství do veřejného podvědomí. Hlavním hrdinou je mladý hacker, který si touží pořádně zahrát počítačovou hru, a proto se pokusí proniknout do systému výrobce počítačových her. Omylem však provede úspěšný průnik do vojenského systému s vojenským simulátorem nukleárního konfliktu. Díky tomu, že si mladík myslí, že hraje hru a nerozpozná ji od reality, tak málem rozpoutá třetí světovou válku.

V roce 1983 dochází vůbec k prvnímu zatčení hackerů. FBI zatkla nezletilé, teprve šestnáctileté hackery z Milwaukee. Skupina nezletilců byla známá pod jménem *„414 Gang“*. Říkali si podle oblasti, kde bydleli a kde byli také později vystopování. Členové tohoto hnutí měli na svědomí více než 60 proniknutí do počítačových sítí, které spáchali v průběhu pouhých 9 dnů. Mezi jejích největší „úspěchy“ patřily průniky do Sloan – Ketteringova centra, zabývajícího se léčbou rakoviny a do vojenských počítačů patřících pod Národní laboratoř v Los Alamos, kde se vyvíjely jaderné zbraně.

Z šesti zatčených teenagerů byl jeden člověk propuštěn a zbylých pět hackerů dostalo podmíněné tresty.[6]

1.3.3 Rok 1984 – Objevují se první hackerské časopisy

Začal vycházet první hackerský magazín, který publikoval Eric Corley.

Časopis se jmenoval „2600: The hacker quaterly". Název 2600 není náhodný. Číslo 2600 symbolizuje frekvenci tónu, kterým John Drapper přistupoval do New-yorských telefonních ústředen.[6] Tento magazín vychází dodnes v papírově podobě, v souladu s americkou ústavou. Stal se předním zdrojem informací v oblasti telefonování a počítačového hackingu.

Pod názvem 2600 jsou každý první čtvrtek v měsíci pořádána setkaní, kde se legálně scházejí hackeři z celého světa.

O rok později, tedy v roce 1985 přichází na svět první elektronický samizdatový on-line magazín s názvem *Phrack.* [20] Časopis obsahuje stejně, jako magazín 2600 : The hacker quaterly nejznámější návody na hackování, novinky, popisy systému, komentáře hackerských útoků. Navíc obsahuje i návody na výrobu výbušnin a zbraní. I když byl časopis postupem času terčem nejrůznějších soudních pří a skandálu vychází každého čtvrt roku dodnes. Je k dispozici na adrese *www.2600.org.*

1.3.4 Rok 1986 – Přijetí zákona o počítačovém podvodu

Vzhledem k rostoucímu počtu útoků a průniků zaměřených zejména na vládní a firemní počítače přijal kongres USA federální zákon o počítačovém podvodu a zneužití počítače FCFAAA *(*Federal Computer Fraud And abuse Act), který říká, že nelegální průnik do počítačového systému je zločin.

Později se ukázalo, že v tomto zákoně je spousta chyb a nedostatků: „*Byl vykonán velký a dobře míněný kus práce na udržení zákonů na vyšší doby. Ale v každodenním provozu reálného světa má i ten nejelegantnější software sklon k překvapivým projevům svých skrytých chyb.“* [1]

1.3.5 Rok 1986 – Vypuštění internetového červa (tzv. Morrisův červ)

Robert Tappan Morris Jr. byl postgraduálním studentem na Cornellově univerzitě.

Jeho otec pracoval jako hlavní vědecký pracovník pro americkou Národní agenturu pro bezpečnost (NSA). [1]

V rámci výzkumného projektu, na kterém Robert Morris Jr. pracoval, vytvořil kus zdrojového kódu (programu). Jakmile se tento program zkompiloval a spustil, začal se sám šířit v prostředí sítě. Zdrojový kód nebyl příliš rozsáhlý, obsahoval pouze 99 řádků. Postupem času začal Morris s programem experimentovat. Program využíval bezpečnostní díru v systému UNIX. Jeho hlavní předností bylo to, že při svém šíření nenapadl každý z počítačů pouze jednou, ale opakovaně, a to tak dlouho, dokud nevyčerpal všechny jeho zdroje, které mohl napadnout.

Výsledkem šíření tohoto viru bylo to, že Morris (respektive jeho vir) infikoval téměř 6000 počítačů propojených v síti. Tento počet infikovaných počítačů byl na tehdejší dobu značně vysoký, neboť v 90. letech bylo pomocí internetu spojeno kolem 60 000 počítačů.

Tímto útokem způsobil zablokování a tedy vyřazení z provozu jednu desetinu počítačů zapojených do sítě, převážně ohrozil chod vládních a univerzitních systémů.

1.3.6 Konec 80. let – Situace na území tehdejší ČSSR

V ČSSR je možné mluvit o počítačové kriminalitě až na konci 80. let.

Do té doby v českých domácnostech neexistovaly osobní počítače, celý svět IT vlastně patřil k tzv. zakázanému zboží na dovoz.

Výpočetní techniku převážně ruského původu u nás mělo pouze několik podniků a

univerzit. Tyto počítače byly navíc neustále prověřovány komunistickým režimem, tudíž pro žádné potencionální piráty nebyl vůbec prostor.

Změna nastala právě na konci osmdesátých let. Pracovníci československé plavby k nám na lodích z německého Hamburku přiváží první osmibitové počítače. Byly to Atari, Commodore nebo Sinclair. [1] V roce 1987 přišlo výrobní družstvo ze Skalice s výrobou prvních osmibitových domácích počítačů značky Didaktik.

V souvislosti s počátkem fungování počítačů v Československu se začíná rozvíjet také trh s hrami a aplikacemi pro tyto počítače.

Populární byly především modely počítačů Sinclair ZX Spectrum nebo Atari. Hry se do paměti počítačů nahrávaly z magnetofonových pásků. Docházelo ke kopírování kazet a takto šířený software byl tedy nelegální. K nelegálním šiřitelům software patřil vlastně i stát, protože provozoval různé kroužky počítačových techniků fungujících pod hlavičkou organizace Svazarm, kde k takovému kopírování a šíření her samozřejmě docházelo.

Česká ústava v oblasti zákonů a autorských práv s existencí a použitím počítačů jako prostředku pro zneužití zákona vůbec nepočítala. Vůbec první případ „počítačové kriminality“ se u nás odehrál ještě v 70. letech. Skutečná existence tohoto případu je však neověřená, protože neexistují oficiální informace o rozsudku. Hlavním aktérem případu měl být nespokojený zaměstnanec Úřadu důchodového zabezpečení, který poškozoval pomocí magnetu záznamy na magnetických páskách. Tento případ byl kvalifikován jako sabotáž a jeho aktér byl odsouzen na více než 10 let vězení. Následně byl obviněn i jeho kolega za to, že počínání svého spolupracovníka neoznámil, přestože o něm věděl.

Druhý případ byl u nás spáchán v letech (1985-1987). Programátoři výpočetního střediska vědomě poškozovali sovětský počítač značky SMEP, protože chtěli docílit zrušení jeho instalace a následnou výměnu za kvalitnější západní počítač. Trestní stíhání začala vyšetřovat StB jako sabotáž. Tento případ měl zajímavý vývoj, byl dvakrát překvalifikován na jiný trestný čin a nakonec zastaven. Poprvé byl případ překvalifikován na poškozování socialistického majetku, podruhé na porušování povinností v socialistické organizaci. Na základě amnestie pro obviněné programátory bylo trestní stíhání zcela zastaveno.[6]

Dalším případem byl tzv. dokladový delikt, šlo o typickou zpronevěru spáchanou za požití počítače. Pracovnice zásilkového obchodu Magnet odebírala zboží na adresu své matky a v počítači u jednotlivých objednávek měnila status z „nezaplaceno“ na „zaplaceno“.

Další z případů počítačové kriminality, které se u nás objevily, bylo zneužití počítačů (nejčastěji firemních) k provádění soukromých aktivit. Tyto případy byly výsledkem toho, že byly počítače pro obyčejné lidi stále velmi nedostupné a proto využívali počítače svého zaměstnavatele. Využívali je už k zmíněným soukromým nebo zábavním aktivitám.

Prováděli například různé výpočty nebo si tiskli obrázky. Výjimkou nebyly ani aktivity, které vedly k obohacení a také k nelegálnímu podnikání.

1.4 90. léta

V 90. letech dochází k masovému rozšíření osobních počítačů PC, které nahradili 8b počítače. Většina těchto počítačů pracuje se systémem MS Windows, dochází k růstu vývoje software.

Dochází k velkému rozvoji Internetu, z akademických kruhů se přesouvá do domácností. Tím pádem vzrůstá trestná činnost, Internet se stává lákavou příležitostí k páchání nelegálních aktivit. Disketové mechaniky nahrazují CD-ROMy, vznikají anonymní FTP servery a začíná se rozvíjet počítačová kriminalita ve velkém měřítku-globální počítačová kriminalita.

Pachatelem počítačových zločinů už není počítačový nadšenec, jako tomu bylo v předchozím období. Z nynějších útočníků se stávají profesionálové, jejichž hlavním cílem je vlastní obohacení. Fenoménem konce 90. let se stávají sítě P2P.

2 VYMEZENÍ POČÍTAČOVÉ KRIMINALITY

Mezi běžně používané názvy pro tuto problematiku patří počítačová kriminalita, kriminalita informačních technologií, v tisku se lze setkat i s anglickými termíny cyber-crime, IT crime a computer crime.[1]

Kromě termínu počítačová kriminalita se často používá i souhrnný název informační kriminalita. Hlavním důvodem je postupné prolínání výpočetní techniky s komunikačními technologiemi.

Problematika počítačové kriminalita začala brzy nabývat mezinárodního charakteru. Bylo potřeba sjednotit legislativu evropských zemí, provést úpravu stávajících zákonů a vytvořit zákony nové, které by umožňovaly postih trestných činů spáchaných za pomocí počítače respektive počítačové sítě.

Jeden z nejvyšších mezivládních evropských orgánů, Rada Evropy (RE) proto navrhla jedno z možných členění počítačové kriminality. Základní rozdělení podle RE spočívá ve vymezení trestných činů zařazených do Minimálního seznamu a do Volitelného seznamu.

2.1 Členění dle Rady Evropy

Minimální seznam trestných činů zahrnuje: [2]

- počítačové podvody
- počítačové falsifikace
- poškozování počítačových dat a programů
- počítačovou sabotáž
- neoprávněný přístup
- neoprávněný průnik
- neoprávněné kopírování autorsky chráněného programu
- neoprávněné kopírování fotografie

Volitelný seznam trestných činů zahrnuje: [2]

- změnu v datech nebo počítačových programech
- počítačovou špionáž

- neoprávněné užívání počítače
- neoprávněné užíváni autorsky chráněného programu

Do Minimálního seznamu spadají provinění, která by měla být zapracovány do právních řádů a umožnit tak bojovat proti počítačové kriminalitě.

Ve volitelném seznamu jsou zahrnuta jednání, která by bylo vhodné kvalifikovat jako trestný čin, ale není to nutné.

Termínem počítačová respektive informační kriminalita se označují trestné činy zaměřené proti počítačům stejně tak i trestné činy spáchané pomoci počítačů.

Proto rozlišujeme dvě kategorie počítačové kriminality:

a) protiprávní jednání směřující proti počítači, kdy počítač sám je terčem útoku; jde o průniky do systémů zaměřené na krádež dat, zneužití osobních údajů, průmyslovou špionáž či bankovní podvody

b) protiprávní jednání páchaná s využitím počítačů; počítač tedy slouží jako prostředek trestné činnosti, případně ji usnadňuje – právě zde je stěžejním způsobem protiprávního jednání porušování autorského práva.

Dalším možným dělením je kategorizace na trestné činy klasické, kdy počítač pouze usnadňuje její páchání (bankovní loupeže on-line) či je nástrojem protiprávního jednání (dětská pornografie), anebo se jedná o trestné činy zcela nové, podmíněné nástupem informačních technologií (hacking, cracking).

3 FORMY POČÍTAČOVÉ KRIMINALITY

Podle komise expertů Rady Evropy pro zločin v kyberprostoru se počítačová kriminalita dělí na dva druhy. Podle postavení PC při páchání trestného činu a Podle typu činu [1]

1. Dělení podle postavení počítače při páchání trestného činu

A. Protiprávní jednání, kde je terčem útoku PC (tzv. proti počítači)

B. Protiprávní jednání spáchané PC jako nástrojem trestné činnosti

2. Dělení podle typu činu
   I. Tradiční protiprávní jednání, kde je počítač v postavení bodu A či B
   II. Nová protiprávní jednání, která se objevila až s výsledkem moderních IT

3.1 Protiprávní jednání proti počítači

3.1.1 Tradiční jednání

3.1.1.1 Krádež

O trestním činu krádeže počítače je v souvislosti s počítači možno mluvit právě tehdy, dojde li k odcizení počítače samého. V takovém to případě je spáchán přestupek podle paragrafu 247 TZ. Kvůli své vysoké hodnotě je výpočetní technika pro zloděje značným lákadlem. Cílem zlodějů nemusí být počítač celý, mohou být zcizeny pouze jeho části

3.1.1.2 Loupež

O trestný čin loupeže postihnutelný dle paragrafu 234 TZ, jestliže lupič zcizí při přepadení například notebook.

3.1.1.3 Zpronevěra

Samotná zpronevěra, které se muže dopustit zaměstnanec odcizením výpočetní techniky nemá s počítačovou kriminalitou mnoho společných rysů. Zpronevěra nabývá na významu teprve až s využitím počítače.

3.1.2 Nová jednání

3.1.2.1 Hacking neboli pronikání do sysémů

Pojem hacking popisuje průnik do systému nestandardní cestou, která je ilegální.

Hackeři jsou lidé, kteří se vyznají v programování a v principech fungování sítě. V praxi je osoba hackera vnímaná jako někdo, kdo se pokouší násilím a ilegálně vniknout do počítačového nebo síťového systému a tím ho nějak zneužít nebo poškodit.

„ Správný hacker “ své útoky často směřuje tak, aby si ověřil, co vlastně dokáže a vyzkoušel si své znalosti. Nemá zlé úmysly, netouží po tom, aby poškodil cílový systém. Existuje ovšem i takový typ hackerů, kteří své útoky provádí pro svůj osobní prospěch a proto, aby se zviditelnili. Cílem jejich útoků bývá převážně materiální zabezpečení.

Členění hackerské komunity:

a) Script kiddies

   Členové této skupiny nejsou opravdovými hackery, patří na nejnižší příčku hackerského žebříčku. Jsou to mladí lidé, kteří mají pouze průměrné znalosti o programování a o fungování počítačů. Díky tomu se jim někdy přezdívá Lamy. Ke svým útokům používají nástroje, tzv. skripty, které vytvořil někdo jiný. Tento hotový program pro napadení systému tzv. Exploit pouze spustí a baví se tím, že po průniku do systému vymažou data a zanechají vzkaz typu *„byl jsem zde, Fantomas“*. [21] Díky tomu, že Script kiddies využívají programy jiných, nerozumí tak jejich funkcí. Kvůli svým omezeným schopnostem programování neumí stopy svých útoků zamaskovat, a proto jsou snadno odhalitelní.

U ostatních hackerských skupin jsou právě díky své omezenosti a ubohým schopnostem značně neoblíbení.

b) Střední třída

Do této třídy spadají hackeři, jejichž znalost operačních systému a programovacích jazyků je na vysoké úrovni. Dokáží vyhodnotit typ a úroveň zabezpečení operačních systémů. K průniku do systému tak použijí ten nejvhodnější nástroj, který mají dopředu nachystaný. Jakmile proniknou do systému, tak sleduji celou síť, aby získali informace a přístup k dalším systémům. Členové této třídy se dělí na White Hats a Black Hats. [21]

c) White hats (bílé klobouky)

Někdy jsou označování jako "hodní" nebo etičtí hackeři. Svým jednáním nezpůsobují žádné škody. Jsou to obvykle uznávání experti. Slabiny systému, které svým útokem odhalí, zveřejňují, a upozorňují tak na bezpečnostní chybu. [18]

d) Black hats (černé klobouky)

Tito hackeři mají obvykle kriminální motivy, tvoří několik uzavřených skupin. Objeví-li bezpečnostní slabinu, tak ji na rozdíl od bílých klobouků nezveřejní, ale využijí ji pro své obohacení.

e) Gray hats (černé klobouky)

Jedná se o tzv. šedou zónu hackerů. Bezpečnostní díry, které objeví, zveřejní pod dojmem, že tak přispějí k růstu bezpečnostních opatření na síti. Řadí se tak zároveň mezi Bílé i Černé klobouky. [18]

f) Top Class

Tato skupina má název ELITE (v hackerském slangu 3Lit3).

Spadají sem jen ti nejlepší neboli elitní hackeři s nejdokonalejšími znalostmi. Jsou to hackeři, kteří se proslavili těmi největšími útoky (lidé jako Mitnick či Levin).[21]

Do systému pronikají komplexními útoky. Hackovací a maskovací nástroje, které vytvořili, poté prodávají. K zamaskování svých činů používají ty nejdokonalejší a nejdražší

maskovací nástroje, které sami vyvinuli. Za jejich organizovanými útoky stojí touha po ovládnutí celého systému, ve kterém mohou působit i několik let. Jejich útoky souvisí především s únikem osobních dat, zdrojových kódu programů a čísel platebních karet.

Motivace lidí pracujících ve skupině ELITE je různá, od upozornění až po zviditelnění se nebo obohacení se. Hackeři z této skupiny proto mohou patřit mezi bílé, černé, nebo šedé klobouky.

3.2 Protiprávní jednání s využitím počítače

3.2.1 Tradiční jednání

3.2.1.1 Hoaxes

Anglické slovo Hoax v překladu znamená žert, mystifikací, falešnou zprávu apod.

Ve světě počítačů se pojem Hoax používá pro označení falešné zprávy, která varuje např. před nebezpečným virem (virus hoaxes).

Definice HOAXu: Jedná se o šíření nepravdivých varování (Hoaxes) více či méně uvěřitelných historek (urban legends) a vyvolání paniky prostřednictvím internetu. [8]

Hoax se šířil již v dřívějších dobách ústně nebo prostřednictvím tisku, ale díky nástupu Internetu dostává tento pojem zcela nové rozměry. Hoax tak může celosvětově ovlivnit chování mnoha lidí, které Internet spojuje. Vzhledem k tomu, že Hoax často obsahuje výzvu, která žádá o další odeslání co největšímu počtu lidí, říká se těmto zprávám také řetězové emaily. [1]

Poplašná zpráva neboli Hoax obsahuje tyto charakteristické prvky, podle kterých lze snadno odhalit její pravdivost: [8]

- Popis nebezpečí (viru)
  Smyšlené nebezpečí (vir) bývá stručně popsané, v případě viru bývá uváděný i způsob šíření.

- Ničivé účinky viru
  Zde záleží převážně na autorově fantazii. Ničivé účinky mohou být celkem

obyčejné, třeba zformátování disku nebo už míň důvěryhodné - zběsilý útěk myši do ledničky, roztočení HDD opačným směrem, výbuch počítače… Autoři hororů zde mohou hledat inspiraci.

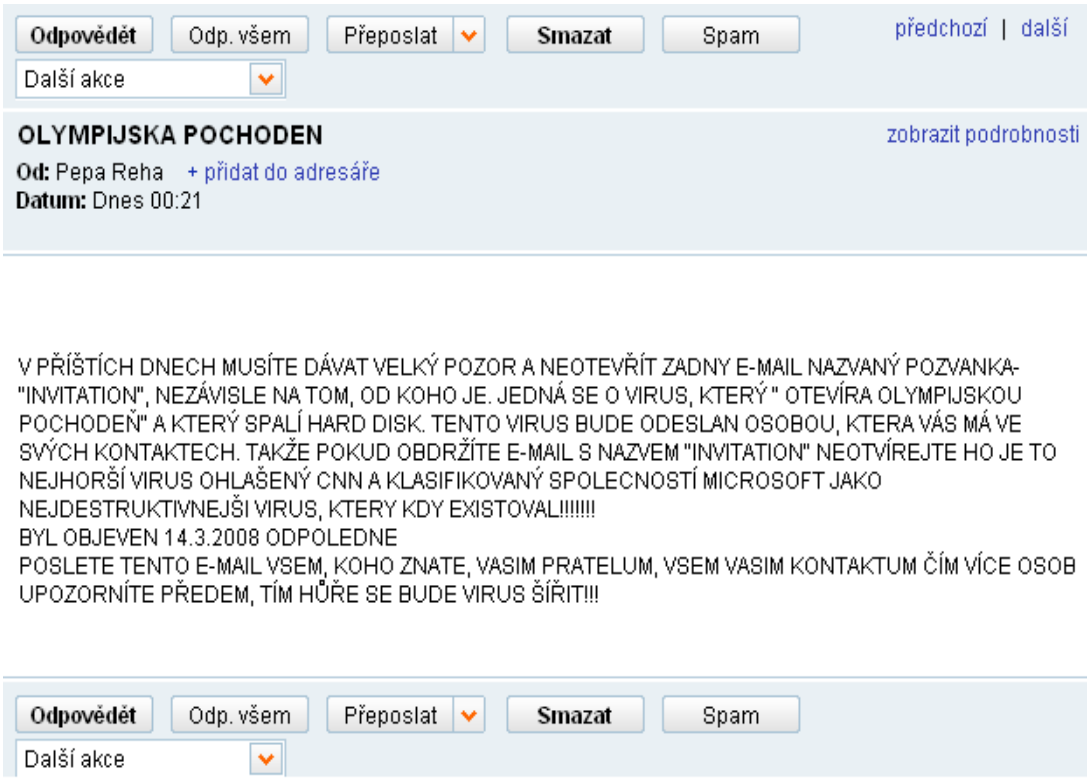
- Důvěryhodné zdroje varují

  Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů ("IBM a FBI varují" nebo "Microsoft upozorňuje" atd.)

  - Výzva k dalšímu rozeslání

  Tento bod HOAX vždy obsahuje! Mnoho nezkušených uživatelů se nechá zprávou napálit a bez přemýšlení výzvu uposlechnou. Právě proto se tyto nesmysly lavinovitě šíří.

Hoaxy se šíří hlavně díky soucitu uživatelů. Běžný uživatel, který zprávu obdrží, začne litovat a s vidinou pomoci i v dobré víře odešle dalším lidem. Touto formou se zprávy lavinově šíří mezi další uživatele bez ohledu na jejich aktuálnost či pravdivost.



Obr. 1 Typický příklad Hoaxu

Důvody škodlivosti Hoaxu: [9]

1) Obtěžování příjemce

   Uživatel přijímá nesmyslnou zprávu opakovaně, často i několikrát denně

2) Poskytování nebezpečných či nepravdivých rad

   Uživatel je prostřednictvím obdržené zprávy vyzván, aby smazal určitý soubor a odstranil tak údajný vir ve svém počítači. Uživatel pod obavou z viru uposlechne a soubor opravdu smaže. Smazáním údajně napadeného souboru však počítači paradoxně uškodí.

3) Ztráta důvěryhodnosti

   Odesílatel posílá falešné zprávy z pracovního emailu, a tím ohrožuje svoji důvěryhodnost. Stalo se i pár případů kdy nepravdivé zprávy odesílali i pracovníci firmy zabývající se výpočetní technikou. V takovém případě ohrožuje odesílatel nejen svoji pověst ale i věrohodnost celé firmy.

4) Zbytečné zatěžování serverů a linek

   Při odesílaní hoaxů často uživatel použije možnost předat dál a odešle jej na všechny adresy hromadně. Postupným přidáváním adres samozřejmě narůstá i celková velikost zprávy. Stahováním nebo odesíláním takto rozsáhlé zprávy dochází k velké zátěži počítačových sítí a serverů.

5) Ztráta důvěryhodných informací

   Tím pádem, že se hoax přeposílá mezi velké množství adres, dochází k tomu, že se šíří obrovský seznam emailových adres mezi předem neurčený počet náhodných příjemců. Takto získané adresy často využijí spameři pro šíření spanů nebo počítačových virů. Některé hoaxy jsou koncipovány jako petice či podpisové akce a vyžadují vyplnění osobních údajů, jako je adresa nebo rodné číslo. Takové počínání je velmi riskantní, protože nikdy nemůže vědět, kdo a jakým způsobem tyto diskrétní informace zneužije.

Obrana proti HOAXU

Hlavní obranou proti hoaxu je ověřování si informací před tím, než zprávu rozešleme dalším uživatelům. Pokud by si každý ověřil věrohodnost zprávy před jejím odesláním, pojem hoax by vlastně vůbec nevznikl.

Pravdivost obdržené zprávy je možné si ověřit na adrese www.hoax.cz.

Web obsahuje databázi rozšířených řetězových zpráv neboli HOAXů.

Šíření takových poplašných zpráv je trestné. V případě, že šířená zpráva znepokojuje větší počet lidí, lze ji kvalifikovat jako trestný čin podle § 199 TZ, tj. šíření poplašné zprávy. [1] Pachatel této trestné činnosti může být odsouzen k peněžitému trestu, nebo trestu odnětí svobody na jeden rok. Pokud se viníkovi prokáže, že zprávu, o které věděl, že je nepravdivá poskytl policii či mediím, je trestní sazba samozřejmě vyšší (až 3 roky)

3.2.2 Nová jednání

3.2.2.1 Sociotechnika (sociální inženýrství)

Tuto metodu zavedl Kevin Mitnick. Poprvé ji použil už na střední škole při pronikání do telefonních sítí (phreaking), kdy využíval vstřícnosti zaměstnanců telefonních služeb.

Sociotechnika označuje činnost přesvědčování lidí, aby dělali věci, které se pro neznámé lidi obvykle nedělají. [21]

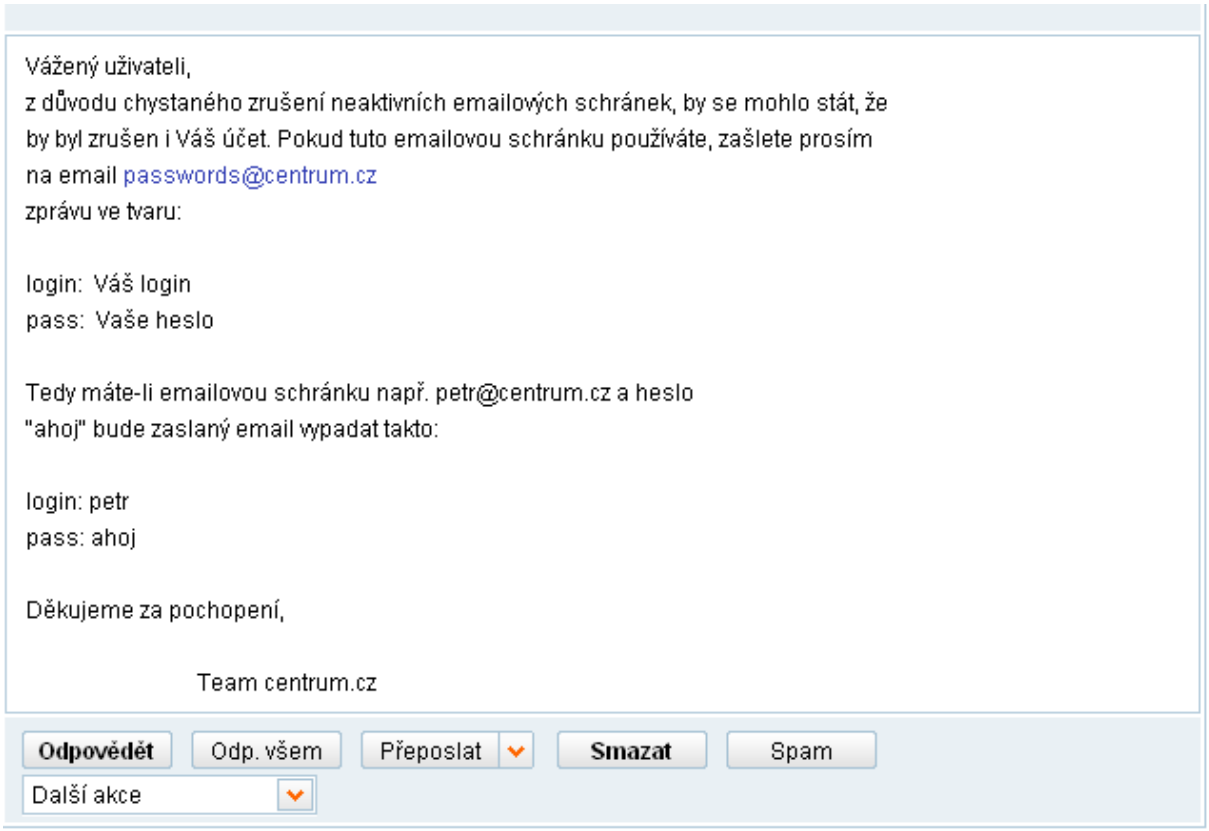
Tato nátlaková metoda vede počítačové uživatele k tomu, že nevědomě poskytnou útočníkovi (počítačovému pirátovy) nějaké soukromé informace, popřípadě hesla. Tím tak útočníkovi umožní, aby se bez problému, bez sebemenší námahy dostal do jejich počítačového systému.

Je několik způsobů, jak sociotechniku v praxi uplatnit.

a) Zasíláním falešného emailu

Útočník si založí emailovou schránku na stejném serveru, který používá jeho oběť. Při založení schránky použije útočník věrohodné jméno, aby tak zvýšil věrohodnost svého činu. Schránku pojmenuje např. heslo@centrum.cz.

Z tohoto emailu pošle oběti mail takového znění:



Obr. 2 Email založený na principu sociotechnicky

Vzhledem k tomu, že oběť čelí hrozbě zrušení schránky, je pravděpodobné že své heslo útočníkovi skutečně pošle. Tento trik však zafunguje jen u méně zkušených uživatelů internetu, kteří nebudou považovat za divné, že se sever obrací na uživatele s požadavkem na heslo.

b) Pomocí telefonního hovoru

Útočník se vydává například za zaměstnance firmy, u které má oběť zřízenu emailovou schránku nebo bankovní účet a snaží se z oběti vylákat požadované informace k provedení svého nekalého útoku.

Tato metoda je složitější, protože jde o přímý rozhovor útočníka a oběti. Úspěšné provedení tak závisí na hereckých dovednostech útočníka, který musí mít rozhovor dopředu připravený a zároveň musí být schopen improvizace. Techniky sociologie spočívají v použití nátlakových metod za účelem využití selhání lidského faktoru.

3.2.2.2 Spamming

Termín Spam označuje nevyžádaný email. Samotné rozesílání zpráv se nazývá spamování neboli Spamming a definuje se jako hromadné zasílání nevyžádané elektronické pošty. Nejčastěji jsou zasílány reklamní informace (hlavně propagační informace). [4]

Někdy se také používá označení UBE (UNSOLICITED BULK EMAIL) – nevyžádaná hromadná pošta.

Osoby, které se zabývají hromadným rozesíláním zpráv, se nazývají spameři. Emailové adresy, které využijí pro Spamming získávají pomocí různých technik, včetně automatizovaných programů. Takovýto program prochází jednotlivé stránky a hledá požadované informace. Program například projde diskusní příspěvky a emailové adresy vyfiltruje. Nejčastěji jsou tak adresy získávané z různých diskusních skupin nebo www konferencí. Velice často se stane, že uživatel poskytne Spamerovi svou emailovou adresu tak, že se zaregistruje na některých pochybných stránkách nabízejících nejrůznější služby zdarma. Aby registrace proběhla úspěšně, je nucen vyplnit svou emailovou adresu včetně dalších osobních informací.

Vůbec první email, který lze označit jako spam, byl odeslán 1. května 1987 zaměstnancem firmy Digital Equipment Corporation, prostřednictvím sítě ARPANET. [11]

V České republice měla největší ohlas kauza ohledně spamu společnosti Media Online, s.r.o.

Firma byla vlastníkem serveru o bydlení Tvůjdum.cz a prostřednictvím hromadných emailů informovala uživatele o novinkách na svých stránkách a o trendech v bydlení.

Podle ředitele této reklamní kampaně však nešlo o hromadné zasílání emailů, nýbrž byli uživatele pečlivě vybraní pomocí globální rešerše. Hájil se tím, že zprávy posílali pouze lidem, kteří se na svých webových stránkách věnovali problematice bydlení. Někteří uživatele podali na počínání firmy stížnost, kterou adresovali na Živnostenský odbor Magistrátu hlavního města Prahy. Živnostenský odbor zahájil proti firmě Media Online, s.r.o. správní řízení a udělil jí pokutu několik desítek tisíc korun. [12]

Mezi další známé spammingové kauzy, které se odehrály v ČR, patří případy Aleše Slabého a Čechoameričana Rosse Hedvíčka.

Za dnešní rozšířenost Spammingu stojí hlavně jeho ekonomická nenáročnost a díky nedokonalým zákonům také beztrestnost. Ekonomická výhodnost je však pouze jednostranná ve prospěch spamerů. Výrobní a doručovací cena jejich „produktů" je nulová. Tím, že zákazníka osloví prostřednictvím jeho emailové schránky, ušetří tak finance, které by vynaložili za zisk letáků a následnou distribuci pomocí klasické roznášky. Hlavní náklady nesou poskytovatelé internetových služeb a hlavně koncový příjemce spamu. Náklady jsou spojeny především v navyšování přenosných kapacit, rostou rovněž nároky na kapacitu úložných systémů a hlavně časové náklady při likvidaci těchto nevyžádaných zpráv.

1) Nebezpečí Spamu [4]

a) Zaplnění emailové schránky

- jestliže uživatel pravidelně nemaže příchozí zprávy (hlavně ty spamové) čelí hrozbě zaplnění schránky. Zaplněním schránky nevyžádaných emailů, ztrácí schopnost přijímat nové zprávy, o které nenávratně přijde

b) Zpomalení přenosu pošty

- na rozdíl od běžných textových zpráv obsahují spamy velké množství obrázku, někdy i zvuků. Zabírají tudíž daleko více místa, než obyčejné textové zprávy a to vede k zahlcení schránky a následnému zpomalení linky. Přenos pošty tak zabere daleko více času.

c) Zneužití informací

- emailová adresa, ale i další osobní informace mohou být zneužity i k závažnějším účelům než je spamování.

2) Některá proti-spamová pravidla:

a) Odstranit z PC veškerý spyware

- vzhledem k tomu, že spyware odesílá z hostitelského PC určenému uživateli různé informace, je často zdrojem nepříjemností a proto je nutné jej odstranit

b) Na pochybných stránkách se registrovat s rozvahou

- úplně nejlepší volbou je se na pochybných stránkách vůbec neregistrovat
- tyto nevěrohodné stránky většinou poskytují něco zadarmo, opak je ale pravdou, a jediné co návštěvník stránky obdrží zadarmo je právě Spam.
- když se ho uživatel rozhodne zaregistrovat, neměl by uvádět žádné osobní údaje, pokud je server k registraci přímo nevyžaduje. Pro registraci na takto pochybném serveru se doporučuje použít separátní email a smýšlené osobní údaje.

c) Uvádět adresu v bezchybném tvaru rozvahou

- pokud uživatel potřebuje uvést svoji skutečnou adresu přímo na webovou stránku, nebo do nějakého diskusního fóra, doporučuje se zadat adresu ve tvaru, která bude pro robota nečitelná:

  Příklad:

  adresa v normálním tvaru: jan.novak@seznam.cz

  adresa pro robota nečitelná: jan.novak(zavináč)seznam(tečka)cz [13]

Boj proti Spamu je běh na dlouhou trať. Vytvoří-li se nějaké nové metody ochrany, přizpůsobí se i metody Spammerů a jejich výsledných „produktů“. Proto neexistuje žádná komplexní a efektivní rada, jak Spam nadobro vymítit. Dostatečná softwarová podpora opřená o kvalitní ústavu by mohla znamenat obrat k lepšímu.

3) Metody obrany proti spamu: [4]

   Pokud je uživatel napaden spamem, může využít těchto možností:

a) Zkusit se odhlásit ze seznamu adres odesílaných zpráv („unsubscribe“)

- *m*ožnost, aby nevyžádaný email obsahoval adresu na odhlášení (unsubscribe) je velmi nízká. Pokud spam tuto možnost obsahuje, většinou jde o neplatnou adresu, kterou se snaží Spammer zvýšit věrohodnost svého „produktu“.

b) Zkusit odpovědět se žádostí o ukončení zpráv

- úspěch této metody je velmi nepravděpodobný. Adresa, ze které je spam posílán není pravá, často se mění a možnost, že zpráva se žádostí doručí je velmi nízká.
- Pokud by vaše zpráva našla cíl, pak už záleží na svědomí Spammera, jestli výzvu uposlechne a přestane emaily posílat.

c) Kontaktovat svého administrátora

- poskytovatel konkrétní emailové schránky by měl být schopen vyhovět požadavku svého zákazníka a spamy ze schránky odfiltrovat

d) Vytvořit si na svém poštovním klientovi filtr

- filtr, který dnes už většina emailových schránek obsahuje, umožňuje doručené zprávy třídit a oddělit tak legitimní poštu od nevyžádaných spamů.

4) Hlavní znaky Spamu: [4]

a) Neznáma adresa

- v 90% se stává, že nevyžádaná zpráva přichází z adresy, kterou uživatel nezná. Tato adresa většinou pochází z freemailových serverů, má často nesmyslné tvary, např. asdsdtrikes @yahoo com. [zdroj Tykvon]

b) Předmět

- předmět je u Spamu zvýrazněn a bývá zpravidla v angličtině. Obsahuje výzvu, že jde o mimořádně výhodnou akční nabídku apod.

c) Obsah

- mimo nečekaně výhodných nabídek, obsahuje Spam informaci, která se snaží uživatele přesvědčit o legálnosti celé zprávy.

3.2.2.3 Warez

Tento pojem pochází z anglického slova wares neboli zboží. Pojmem warez se obecně rozumí nelegálně šířený software tedy pirátsky šířený software. Softwarem není myšlen pouze program samotný. Tento název je souhrnný pro hry, filmy, nebo hudbu.Většina laické veřejnosti se domnívá, že tento pojem zahrnuje nelegální vypalování CD.

Správná definice termínu warez je tato: *Warez je termín počítačového slangu označující autorská díla, se kterými je nakládáno v rozporu s autorským právem.* [23]

Osoba, která se zabývá warezem bývá nazývána warezák nebo také počítačový pirát. Warez nebývá doménou jednotlivce, zabývají se jím celé skupiny. Ve skupinách (podobně jako u crackerů) vládne vnitřní hierarchické rozdělení, kde má každý člen své přesně dané postavení a specializuje se pouze na svoji činnost. Skupiny si vytvořily svůj vlastní slangový jazyk. Je typický například nahrazováním písmene “s“ znakem “z“.

Příklady slangu:

- náhrada písmene S za $: Compu$erve, Micro$oft;
- nahrazení písmene 's' v množném čísle písmenem 'z' (passwordz, passez, utilz, MP3z, distroz, pornz, sitez, gamez, crackz, serialz, downloadz, FTPz, ...)
- nahrazení písmene 'o' číslicí 0 (c00l, l0zer, b00t, d00d …)
- využívání fonetického čtení/zápisu (You are => u R, For You => 4U…);
- použití zdůrazňující předpony k (snad jako kilo) (k-cool velice chladnokrevný, k-awesome – hrozně děsivý, k-korun – drahý);
- vzájemná záměna ph a f (phone => fone, freak => phreak);
- používání znaků #!$ při doplňování textů ("Hey Paul!#!$#$!#!$");
- nadměrné používání VELKÝCH PÍSMEN;
- používání jednoduchých obrázků v tzv. „znakové grafice“ nebo „ASCII grafice“ (některé ukázky viz závěr článku);
- pro českou komunitu je typické nepoužívání diakritiky a používání anglických (i méně obvyklých) zkratek [14]

Každá skupina je zaměřena na určitý druh činnosti. Specializace skupin bývají následující:

- zaměření na filmy (moviez)
- zaměření na hry (gamez)
- zaměření na aplikace (apzz)
- zaměření na cracky (crackz)

V čele skupiny stojí tzv. Leader (Vůdce), řídí chod celé skupiny, zhaní nové členy a je dominantní postavou celé skupiny. Velmi důležitým členem skupiny je Suplier (Zásobovač), který opatřuje pro skupinu nový, ještě nevydaný software a proto je pro skupinu nezbytně důležitý.

Dále ve skupině pracují Crackeři a Cardeři. Cracker překonává ochrany produktů a Carder se zabývá napadáním databází kreditních karet. Tímto způsobem získává finanční prostředky pro chod a vybavení skupiny. Posledním důležitým článkem skupiny je Tester. Náplní jeho práce je otestování výsledného produktu před jeho uvedením na server.

Výsledný produkt, který skupina vytvoří, se nazývá RELEASE. Po uvedení produktu na server se na scénu dostávají kurýrské skupiny, jejichž úkolem je co nejrychlejší šíření dat mezi jednotlivé servery. Prostřednictvím FTP serverů nebo P2P (peer to peer) sítí se data dostanou mezi obyčejné uživatele. FTP servery umožňují sice bezplatné stahování dat, ale na druhou stranu neposkytují velkou rychlost stahování. Proto se více využívají P2P sítě, kde spolu přímo komunikují jednotlivý klienti. Jejich výhodou je velká přenosová rychlost, řádově až desítky MB/s. [23]

V současné době existují programy, které pracují na principu výměnné sítě. Jsou to např. Strong DC a BitTorent. Slouží ke sdílení a stohování dat. Uživatelé jsou napojení na speciální server tzv. HUB, kde si mezi sebou vyměňují data. Díky takovým programům je cesta k Warezu opravdu snadná. Méně známý uživatelé internetu používají k vyhledání Warezu namísto výměnných programů přímo internetového vyhledavače. Takovýto způsob vypadá velmi jednoduše, ale často nevede k hledanému cíli. Uživatel se prokliká spoustou odkazů, ale místo hledaného produktu dojde k tomu, že si do počítače nevědomky natáhne škodlivý kód v podobě Malware. Pojem Malware je souhrnným označením pro škodlivé programy, které běží na počítači bez vědomí uživatele a tak ohrožuje jeho funkci. Tyto programy slouží nejčastěji k šíření spam, nebo ke sběru adres.

V březnu 2007 uveřejnil jeden z předních výrobců bezpečnostního software, firma McAfee studii, týkající se rizikovosti webových stránek.

Průzkum zobrazuje žebříček stránek seřazených podle pravděpodobnosti výskytu víru. Studie ukazuje, že mezi nejbezpečnější patří domény severských zemí. *Doména .fi* obsahuje pouze 0,1 % nebezpečných stránek. Naopak mezi nejnebezpečnější stránky patří domény ostrovních států, zejména *domény .tk* (pacifické ostrovy Tokelau).

Velmi nebezpečné jsou také rumunské a ruské domény, konkrétně doména .ro (5,6 %) a *doména.ru* (4,5 %). Nejriskantnější domény mají přípony. *info* (7,5%).

České republice patří v průzkumu 36 místo, její domény obsahují 1 % nebezpečných stránek. [15]

Hlavním důvodem rozmachu warezu je neúměrná cena, kterou výrobci požadují za své produkty. Distributoři argumentují tím, že cena jejich produktů roste spolu se zvyšujícími se náklady na výrobu či vývoj. Na druhou stranu odpovídají zase běžní uživatelé tím, že se distributoři nestarají o potřeby běžného konzumenta a za své produkty požadují nekřesťanské peníze. Např. pro studenta, který programy využívá převážně pro studijní účely, nikoliv k podnikání je koupě originálního software drahá. Proto se stalé více uživatelů uchyluje k warezu. Takto ilegálně získaná aplikace má své „výhody“ i „nevýhody“.

Výhodou je to, že k získání produktu nevynaložil uživatel téměř žádné finanční prostředky.

Nevýhodou je ztráta technické podpory výrobce a již zmíněná možnost infekce počítače škodlivým malwarem, která velmi často provází stahování ilegálních aplikací.

Warezové skupiny fungují na principu NON-PROFIT, tzv. svoji práci berou jen jako koníček a neusilují o osobní obohacení. Samozřejmě i zde se najde pár jedinců, jejichž hlavním cílem je finanční zisk. Ve většině případu je však skupina dobře organizovaná a tak drtivá většina provozuje Warez opravdu jako zábavu bez vidiny vlastního ekonomického prospěchu. Hlavním hnacím motorem skupin je získání respektu od konkurence s, kterou soutěží. Soutěživost spočívá v počtu releasů, jejichž kvalita se boduje a sleduje v různých žebříčcích. Čím více kvalitních releasů skupina vytvoří, tím je lepší. [23]

Je jasné, že tvorba a následná distribuce Warezu je nelegální. Najdou se ale i země, kde se tato problematika přehlíží, anebo je dokonce legální. Jedná se nejčastěji o země třetího

světa (Asie, Čína) nebo země, kde vládne komunismus. V České republice je kopírování a šíření autorských děl bez povolení autora (tedy Warez) trestným činem. Trestá se podle § 152 TZ. Pachatel může být potrestán dvěma lety vězení, peněžitým trestem nebo propadnutí věcí. Délka trestů se odvíjí také od toho, v jakém rozsahu pachatel čin spáchal. Spáchá-li tento trestný čin opakovaně, tak se trestní sazba pohybuje v rozmezí od šesti měsíců do pěti let.

3.2.2.4 Cracking

Cracikng je provázán s pojmy warez a hacking. Název pochází z anglického slova crack-lámat. Podstatou této metody je zásah do programu, který umožní obejít jeho ochranu proti kopírování nebo neoprávněnému užití. [1]

Obecná definice crackingu je následující: Crackingem bývá označován soubor mnoha postupů, při kterých dochází k úpravám nebo zkoumání a pozorování funkcí, metod a principů programového kódu bez možnosti užití zdrojových kódů programovacího jazyka, v němž byl program vytvořen. [5]

Lidé zabývající se touto metodou se nazývají crackeři neboli lamači, pracují ve skupinách. Jednotlivé skupiny se dělí podle pole svého působení. Specializují se buď na herní oblasti, weby nebo aplikace. Ve skupině vládne hierarchické rozdělení, každý její člen má na starost nějakou specifickou činnost. Základními členy skupiny jsou dodavatelé, programátoři a distributoři. Úkolem dodavatele je opatřit nový software ještě před jeho oficiálním uvedením na trh. Programátoři jsou nejdůležitějším článkem skupiny, jejich úkolem je prolomení ochrany proti kopírování. Distributoři poté program rozšíří po celém světě.

K prolamování ochrany programu používají crackeři různé metody. Mezi nejvyspělejší metodu patří tzv. reverse engineering (reversní inženýrství). Je to zpětný překlad programu do určitého programovacího jazyka (nejčastěji do assembleru). Přesnost překladu se odvíjí od vyspělosti programu požitého při dekompilaci. Čím je úroveň použitého programu nižší, tím je přesnější výsledný překlad. Proto se nejčastěji překládá právě do assembleru. Při tomto zpětném překladu pak cracker zkoumá kód programu, snaží se ho pochopit a zaměřuje se na jeho ochranné nedostatky. Cracking se však nevyužívá jen jako prostředek pro porušování autorských práv. Existuje i skupina crackerů, která se specializuje také na prolomení bezpečnostních ochran systému.

Motivací většiny pachatelů zaměřujících se na cracking není vlastní obohacení. Touží po slávě a svou činnost provozují hlavně pro zábavu. Výsledky své činnosti dávají k dispozici zdarma. Existuje ale i určitá skupina lidí, která výsledky své práce prodávají dalším uživatelům za účelem finančního zisku. Takovéto jednání nemá s posláním opravdových crackerů nic společného.

Vlivem malé informovanosti, často způsobené i špatnou interpretací novinářů se stává, že pojmy hacking a cracking, respektive hacker a cracker bývají k nelibosti hackerů spojovány dohromady. Opak je ale pravdou a tyto dvě skupiny se od sebe zásadně odlišují.

Jedna z definic dokonce říká, že základní rozdíl je v tom že hackeři věci vytvářejí a crackeři je ničí. [16]

Crackeři se rádi řadí mezi hackery, jejich znalosti v oblasti programovacích technik a síťových protokolů však zdaleka nedosahují takových kvalit, aby se hackerům mohli vyrovnat. Vzhledem k tomu, že se cracker pracuje již s hotovým programem, který se snaží prolomit, spočívá jeho činnost spíše ve vytrvalosti než v excelentních znalostech. Pronikají-li crackeři do systémů využívají k tomu již zveřejněných slabin.

Naproti tomu hackeři disponují velmi kreativním myšlením, jejich činnost spočívá v hledání děr a slabin, které využijí pro průnik do systému za účelem zisku informací.

3.2.2.5 Phishing

Pojmem Phishing se označuje technika, která se využívá k získávání osobních údajů, jako je krádež hesla nebo krádež údajů o platební kartě. Phishing je vlastně určitou formou krádeže identity. Metoda funguje na principu zasílání emailových zpráv, ve kterých se při působení na uživatele používá již zmíněných metod sociotechniky. Tyto emailové zprávy vypadají věrohodně, jakoby je odesílala skutečná instituce.

Velmi často se používá podvodný formulář bankovního účtu, který je přesnou kopií formuláře, který používá banka. Formulář vyzívá uživatele k zadání uživatelského jména a hesla. Tím že uživatel zadá své jméno a heslo prozradí své přihlašovací údaje útočníkům, kteří je poté zneužijí a s účtem mohou manipulovat a připravit tak svou oběť o finanční hotovost. Uživatel je pomocí emailu vyzván, aby se například přihlásil do svého účtu za účelem zkvalitnění služeb nebo provedení změn. Uživatel navštíví formulář svého internetového bankovnictví, ale ve skutečnosti je přesměrován na stránku, která je podvodnou kopií formuláře opravdové banky.

Phishingu lze předcházet použitím SSL certifikátu. Služba SSL (Secure socket layer) je rozšíření klasického protokolu http o bezpečnostní vrstvu. Z protokolu http tak vznikne zabezpečený protokol https. Data jsou tím pádem zašifrována a chráněna proti odposlechu hackerem. [25]

SSL certifikáty se používají všude tam, kde je uživatel vyzván k zadání osobních dat, jako jsou například hesla, nebo čísla platebních karet. Právě užitím SSL certifikátu při vyplňování přihlašovacích údajů jsou odesílaná data maximálně zabezpečena proti případnému úniku a následnému využití jinou nepovolanou osobou. Ne všechny weby však umožňují ověřování informací pomocí služby SSL. [24]

Phishing lze poměrně snadno odhalit zkontrolováním správnosti webové adresy (URL), na které se má považovaná schránka či formulář nacházet. Niance webových adres spočívá byť jen v jediném písmenku. Například správná stránka, kterou uživatel míní navštívit má tvar secubank.com, ale uživatel bez povšimnutí navštíví stránku securbank.com, kterou má hacker připravenou ke svému podvodu. Díky vlastní nepozornosti tak nevědomky poskytne své osobní údaje pirátovi, který má poté snadnou práci. Existují i některé weby, zabývající se nebezpečím Phishingu, např: www.antiphishing.org

3.2.2.6 Pharming

Základem pojmu Pharming je anglické slovo farming, což znamená farmařit nebo pěstovat. Kvůli hackerskému slangu vzniklo ze slovíčka farming slovo pharming. Výraz farming, neboli pěstovat proto, že si útočník (hacker) na vyhlédnutém počítači vypěstuje podmínky pro svoji ilegální činnost.

Pharming velmi úzce souvisí s Phishingem. Stejně jako u phishingu je jeho princip založený na tom, že se uživateli podstrčí falešná webová stránka. Ta je věrnou kopii originální stránky, kterou měl uživatel původně v úmyslu navštívit. Pomocí této vykonstruované stránky pak hacker získá od nic netušícího uživatele osobní data.

Jaký je vlastně rozdíl mezi Phisingem a Pharmingem? U Phisingového útoku si může uživatel zkontrolovat správnost webové adresy požadované stránky, na které se nachází.

Například kdyby existoval web s názvem www.ceskabanka.cz, hacker podstrčí uživateli stránku s názvem *www.ceskabankaonline.cz.*

U zkušeného uživatele může rozdíl v názvu domén vzbudit pozornost a útok tak čas odhalit. Právě tuto nedokonalost Pharming odstraňuje, nelze ho tedy tak snadno odhalit a je

tak mnohem nebezpečnější. Pracuje na principu „otrávení“ uložených DNS záznamů. Tato technika se nazývá DNS „cache poisoning“.

DNS (DOMAIN NAME SYSTEM) překládá doménová jména (URL) na IP adresy a opačně. Jména domén (*www.seznam.cz*) poskytují uživateli lepší schopnost zapamatování, ale adresy pro počítač musí být zadávány ve formátu IP.

Útočníci si vyberou špatně zabezpečený DNS server a přidělí stránce zadané do vyhledávače IP adresu stránky falešné. [26]

Například uživatel zadá do vyhledávače URL adresu internetového bankovnictví. Útočník změnil záznam DNS serveru, takže stránce je přiřazena falešná IP adresa, která přesměruje na uživatele na předem připravenou falešnou stránku. URL adresa zadávané stránky se nezměnila a podstrčená stránka odpovídá originálu. Uživatel tak nenabude žádného podezření o napadení.

Odhalit Pharming by mohl zkušenější uživatel prostudováním vlastností SSL certifikátu. Všechny náležitosti SSL certifikátu není schopen hacker předělat, pouze ho poupraví tak, aby při běžném zkontrolování nebylo možno odhalit nějaké podivnosti.

4 OCHRANA PŘED POŘÍTAČOVOU KRIMINALITOU

Přínos prevence v boji s počítačovou kriminalitou je zcela nezastupitelný, už proto, že působení represe je díky mnoha těžkostem při vyšetřování počítačových zločinů velmi často omezené. Prevenci lze dále rozdělit na psychologickou a technologickou. [1]

Psychologická prevence je souborem takových opatření, která napomáhají vytváření povědomí o nemorálnosti a společenské nepřijatelnosti činů, které jsou právem zakázány a sankcionovány. Touto prevencí se zabývají zejména softwarové firmy a jejich zájmová sdružení (např. BSA).

Sdružení vzniklo v USA roku 1998. Hnutí se podílí na přípravě zákonů autorských práv. Spolu s výrobci informuje veřejnost o výhodách použití originálního software. Podle právního řádu postihuje jednotlivce i organizace, které se podílejí na vzniku ilegálního software a porušování autorských práv. BSA sdružuje významné evropské firmy jako je např. Adobe, Autodesk či Novell. [27]

Základem v technologické prevenci je zabezpečení. Jde o neustálý boj mezi tvůrci ochran a útočníků. Neustálá snaha tvůrců programů o dokonalou ochranu vede v niveč, neboť se ukázalo, že v oblasti výpočetní techniky žádná dokonalá ochrana neexistuje. Jakákoliv nová ochrana je v zápětí prolomena.

Tvůrci programů se proto snaží doplnit technickou ochranu zákonnými omezeními, která zakáže uživatelům prolamovat či jinak obcházet nedokonalou ochranu. I tyto snahy se však brzy ukázaly jako zbytečné, pokud je ochrana prolomitelná, pachatel toto využije bez ohledu na zákon.

Jedinou cestou jak nelegální kopírování produktu omezit je nabídnout uživateli takové produkty, které budou výhodné jak po stránce finanční tak obsahové.

5 VLIV VÝVOJE KYBERNETIKY A VÝPOČETNÍ TECHNIKY NA POČÍTAČOVOU KRIMINALITU

Jednoznačným trendem v současné počítačové kriminalitě je neustálá profesionalizace. Dnešní hackeři již netouží po překonání systémových bariér nebo po získání slávy mezi svou komunitou. Jejich hlavní motivací se stávají peníze a majetek. Stále častěji tak dochází k tomu, že do počítačové komunity prorůstá organizovaný zločin.

5.1 Trendy vývoje počítačové kriminality

Vývoj počítačové techniky přinesl následující trendy: [2]

a) Nové delikty, které lze spáchat pouze on-line. Jsou to trestné činy proti integritě a důvěryhodnosti (hacking).

b) Tradiční útoky na okolní počítače a informační systémy jsou prováděny prostřednictvím vydírání, podvodů a metod sociálního inženýrství.

c) Vzrůstající ohrožení mobilních komunikačních systémů ukázalo, že ani mobilní zařízení nejsou před útoky z venčí dokonale chráněna. Počet útoků na mobilní zařízení vzrostl v průběhu roku až desetinásobně.

d) Zneužívání WIFI sítí, WIFI sítě jsou napadány viry, které spouštějí lokalizované útoky.

e) Masové rozšíření Spamingu za pomocí trojských koní a automatických programů (botů). Pomocí těchto botů lze napadený počítač ovládat na dálku.

f) Nárůst Phishingu (viz. kap 3.2.2.5)

g) Nárůst Spyware motivovaný finančním ziskem pachatelů. Spyware poté využijí například ke krádeži identity

5.2 Copyright a Copyleft

V oblasti porušování autorských práv je patrná výrazná tendence, která bývá označována jako posun od copyrightu k copyleftu. [1]

Nástup nových technologií umožnil masové porušování autorských práv (tedy copyrightu) na celém světě. Na druhou stranu není možné, aby autoři poskytovali k využití svá díla zadarmo. Hlavním problémem je to, že část finančního zisku uskutečněného mezi autorem

a koncovým uživatelem končí v kapsách vydavatelských společností, které mají z celé transakce nejvyšší výnos.

Řešením by mohlo být použití copyleftu, tzv. zvláštního požití autorského práva. Z nesvobodného software se stane systém svobodný a všechny jeho další modifikace mohou být šířeny taktéž svobodně. [28]

Společnosti, které ze současné situace profitují, by přišly o finanční zisky a tak apelují na zpřísnění právní úpravy, která by šíření zakázala. Takové jednání vyvolává negativní ohlasy z řad veřejnosti, která naopak požaduje právní úpravu umožňující volné užití autorských děl.

Současná legislativa ale kráčí opačným směrem, což spolu se zvyšováním cen produktů vede k velké míře nelegálního kopírování. Situace začíná být neudržitelná. Celý systém je třeba nastavit tak, aby na jedné straně autoři dostávali dostatečnou kompenzaci za svá díla a odstranit vysoké ceny způsobené přístupem vydavatelů.

6 TERORISMUS V IT – KYBERTERORISMUS

Terorismus samotný představuje jednu z aktuálních globálních hrozeb. V dnešní době se pojmem terorismus neoznačuje pouze politicky motivovaný atentát či útok proti skupině lidí.

Nástupem IT a zejména Internetu dostal terorismus úplně nový, snad ještě nebezpečnější význam. Ze spojení klasických teroristických útoků a nových metod vznikl pojem Kyberterorismus.

6.1 Teroristické aktivity související s IT

1) Mediální terorismus

   Tento pojem se objevil v souvislosti s metodami vedení psychologické války a mediální manipulací. Jako hlavní metody útoku se využívají masová média, mezi která patří i Internet. Teroristé využívají toho, že důvěra v elektronická média je daleko vyšší než důvěra v běžná sdělovací média jako jsou televize nebo noviny.

Mezi základní druhy mediálního terorismu patří: [3]

a) Vydávání internetových novin a časopisů:

   teroristé manipulují pomocí vlastních příspěvků s názory čtenářů ve svůj prospěch

b) Kybertronika:

   tento druh mediálního terorismu je založen na zneužití podprahového vnímání, kde útočník vloží například extrémisticky zaměřený text do nevinně vyhlížející reklamy propagující zubní pastu

c) Haktivismus:

   Označuje provozování internetových stránek a serverů. Které obsahují prvky aktivismu

2) Procesní terorismus

   Tento druh terorismu zneužívá prvky demokracie, je postaven na sebezničujícím efektu demokratického řešení sporů. Základem je zneužití zákonných ustanovení nebo soudní moci za účelem vyvolání soudního řízení, které vede k narušení bezpečnostních prvků státu. Procesní terorismus využívají hlavně mezivládní organizace a spolky, které se snaží zviditelnit.

3) IT governance

   Je to soubor manažerských metod a nástrojů zaměřených na řízení oblasti IT. Hlavním cílem je maximalizace přidané hodnoty informačních systémů a technologií pro realizaci strategie organizace. [29]

Hlavním znakem kybernetických útoků je stále vzrůstající složitost a rafinovanost, se kterou si útočníci počínají.

Mezi hlavní cíle kyberteroristů patří servery a sítě, jejichž narušení má kromě psychických dopadů i finanční a politické důsledky. Nejpravděpodobnějším útokem teroristů se stávají informační systémy spojené s důležitou infrastrukturou.

7 VÝBĚR A ROZBOR NĚKTERÝCH PŘÍPADŮ POČÍTAČOVÉ KRIMINALITY

7.1 Světové případy

7.1.1 Případ Skljarov

Hlavním aktérem této kauzy je ruský programátor Dmitrij Skljarov nar. 18. prosince 1974. Vystudoval moskevskou univerzitu, specializoval se na počítačovou bezpečnost. Pracoval v moskevské firmě ElcomSoft, kde spolu se svými spolupracovníky vyvinul program Advanced eBook Proccesor (dále jen AeBP), který umožňoval převod elektronických knih (eBooků) z chráněného formátu Adobe E-book do nechráněného formátu.

Právě kvůli tomuto převáděcímu programu vznikl zásadní problém. Mezi 11. a 16. červencem se Skljarov zúčastnil hackerské konference DEFCON na níž se schází přední počítačový odborníci. Prezentoval zde svou přednášku, která se věnovala bezpečnostním slabinám firmy Adobe pro produkt eBook. Přímo na konferenci byl zatčen americkými orgány FBI na základě iniciativy firmy Adobe. [30]

Samotný Skljarov a spolu s ním i celá firma ElcomSoft byli obviněni právě kvůli distribuci programu AeBP, který umožňoval porušovat autorská práva a překračoval tak paragrafy zákona DCMA.

Zákon DCMA (Digital Millennium Copyright Act) byl přijat kongresem Spojených států amerických v roce 1998, za účelem vymezení a upřesnění ochrany autorských práv ve vztahu k Internetu. [31]

Za nedlouho po zatčení Skljarova začali probíhat mohutné demonstrace, které ho podporovali. Protesty vyvolaly velký zájem veřejnosti, přilákaly spoustu medií, které se postaraly o velikou medializaci celého případu. Začali se podepisovat petice za jeho osvobození a především petice proti organizaci DMCA.

Paradoxní na celém případu je to, že Dmitrij Sklarov je Rus a firma ElcomSoft sídlí rovněž v Rusku, přesto jsou zatčení a souzeni na základě amerických zákonů, které mají platnost pouze v USA. Podle ruských a evropských zákonů je totiž počínání Skljarova legální. Americká strana argumentovala tím, že fy. ElcomSoft nabízela svůj software na

Internetu, mohl být tedy zakoupen i občany USA. Američané poukazovali na fakt, že pro ruský ElcomSoft platí stejné zákony jako pro firmy americké, které své produkty nabízejí v rámci zemí USA, tedy v zemích, kde zákon DCMA platí, tudíž je distribuce nelegální.

Internetová distribuce AeBP trvala 10 dní, během kterých se prodalo do světa 20 kopií, z toho celkem 9 kopií do USA. V Americe si program opatřila Národní laboratoř v Los Alamos nebo bankovní ústav Credit Suisse First.

Sílící akce demonstrantů přiměli firmu Adobe k jednání. 23. července se uskutečňuje schůzka vedení firmy s nadací EFF (Electronic frontier foundation). Tato nezisková organizace se zabývá ochranou občanských práv a svobod v oblasti IT. Po tomto jednání, probíhajícího za stálého nátlaku demonstrantů vydala firma Adobe tiskovou zprávu, požadující okamžité propuštění Skljarova z vazby. V tiskovém prohlášení bylo uvedeno, že byl uvězněn nesprávný člověk (zaměstnanec), nikoliv ředitel firmy a jednak to, že DMCA splnilo svoji úlohu, protože program AeBP už není v USA k dispozici. Proto není žádný důvod Skljarova déle věznit. [31]

Tento výsledek však neznamenal po Skljarova právní osvobození, protože se ukázalo, že Adobe nemůže svou žalobu stáhnout. V celé kauze vystupuje Adobe pouze v roli hlavního svědka. Už nešlo o civilní žalobu, celý případ byl posunut do oblasti trestního práva, kdy proti sobě stojí USA vs. Skljarov.

Dne 6. srpna byl Skyljarov propuštěn na kauci 50 000 USD, nadále musel zůstat v USA a navíc však musel slíbit, že bude svědčit proti svému bývalému zaměstnavateli. Další soudní zasedání se uskutečnilo 11. Prosince. Americká strana u soudu tvrdila, že ElcomSoft vytvořil program AeBP s cílem se obohatit. Naopak ruská firma se hájila tím, že hlavním důvodem proč AeBP vlastně vznikl, byla podpora legálních držitelů eBooku.

Dimitrij poukázal na to, že program vytvořil hlavně proto, aby upozornil na jeho slabiny, ostatně to dokládá i jeho přednáška. Program navíc obsahoval dodatek, který apeloval na jeho legální a férové používání. Definitivní rozsudek byl vynesen 18. prosince, porota rozhodla, že Skyljarov a firma ElcomSoft jsou nevinní ve všech bodech obžaloby a mohou být tedy propuštěni na svobodu.

Celý tento případ má velký význam proto, že pokud by soud uznal stížnost amerických orgánů za oprávněnou, změnil by se způsob trestání jednotlivých států. Už by nebyl trestán stát nebo pachatel, ze kterého ilegální aktivita pochází. Nově by byl trestán stát, ze kterého se k dané aktivitě přistupuje. V praxi by to potom mohlo vést k tomu, že

pokud by se poskytovatel nepřesvědčil o legálnosti programu, který poskytuje ve všech zemích, mohl by být někde žalován.

7.1.2 Gary Mckinnon aneb největší vojenský hack historie

Obr. 3 Gary Mckinnon

Gary se narodil v Glasgow roku 1966. Ve 14 letech dostal svůj první počítač, na kterém se stal brzy závislý. V 17 letech opouští školu a začíná pracovat jako kadeřník. Toto povolání ho příliš neuspokojovalo a tak na radu přátel začal studovat IT. Po úspěšném dostudování proměnil svou závislost na počítačích v zaměstnání a začal rozvíjet své hackerské schopnosti. Kromě hackingu se zajímal také o UFO, tento koníček se mu stál osudným. [32]

Celý případ začal nevinně, při vyhledávání důkazů o existenci UFO nalezl Gary na jistém serveru nové informace, které dosud neznal. Po překonání zaheslovaného serveru vnikl do amerického armádního počítače ve virginijském městě Fort Meyer. Z počítače získal práva správce systému, zkopíroval si přísně tajné data obsahující uživatelské kódy, některá data vymazal a nakonec zašifroval přístupová hesla.

Dále pronikl do počítačů amerického letectva a námořnictva na námořní základně Eagle. Celkově napadl 97 vládních počítačů. Z toho bylo 53 počítačů armádních, 26 námořních, 16 počítačů patřilo organizaci NASA a 1 počítač ministerstvu obrany a oddělení US Air Force. Z provozu vyřadil celou armádní síť v oblasti Washingtonu po

dobu jednoho týdne. Hacker byl dopaden britskou policejní jednotkou Hi-Tech Crime Unit, která se specializuje na kybernetické zločiny. Celková škoda, kterou svými průniky způsobil, dosáhla výše 700 000 USD. Byl obviněn ze 14 trestných činů, které spáchal na území 14 států USA. [33]

Velká Británie rozhoduje, zda se bude soudit doma v Anglii nebo ho vydá zemi, proti které byly útoky namířeny (USA). Velká Británie by hackera propustila bez trestu, zatímco v USA by mu hrozilo 70 let vězení a pokuta 1,75 mil. dolarů.

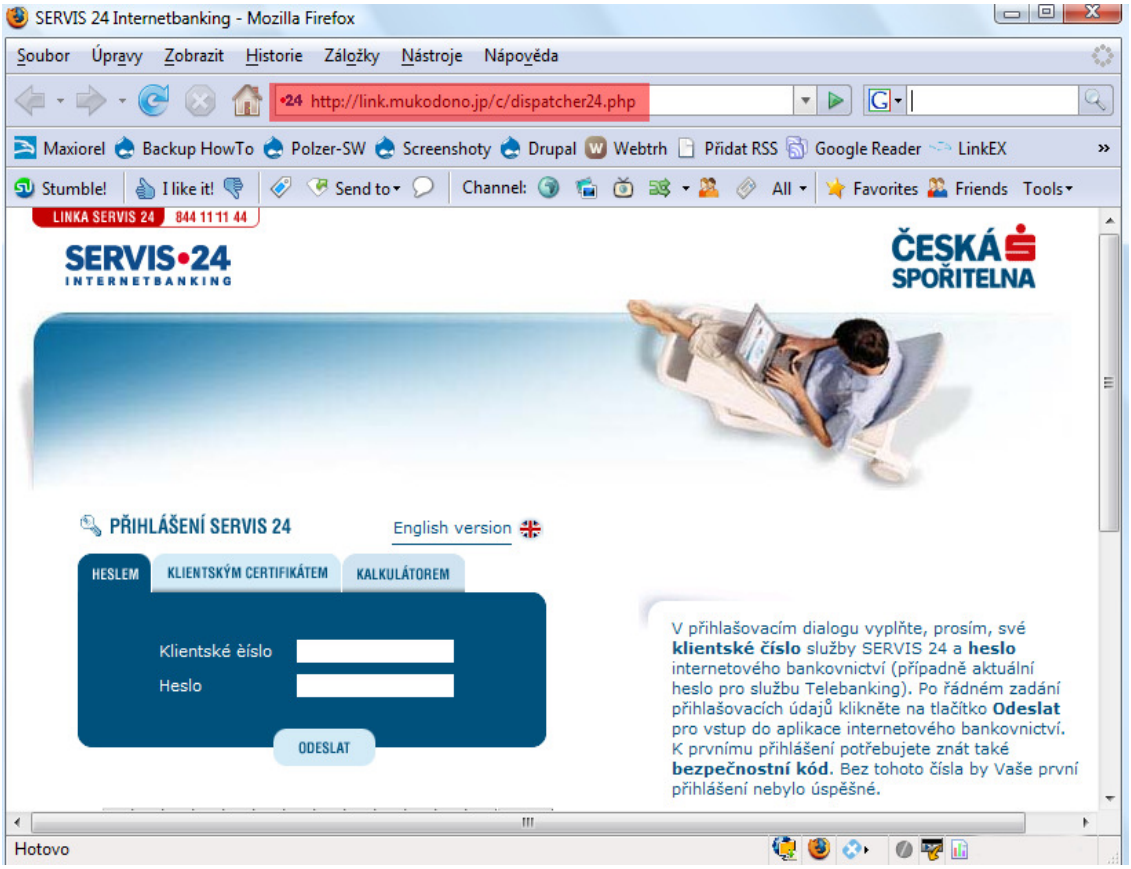
Advokát Edmund Lawsson vyjednal Garrymu propuštění na kauci ve výši 5 000 liber, přičemž mu byl odepřen přístup počítače s internetem a každý den se musel hlásit na policii. Gary se u soudu hájil tím, že nabouráním do systémů nechtěl způsobit žádné škody, toužil pouze po objevení mimozemského života. Poukazoval na nedostatečné zabezpečení systému, tvrdil, že zabezpečení armádních počítačů nebylo nízké, ale že nebyly zabezpečeny vůbec.

Britský soud nakonec doporučil vydání Mckinnova do Spojených států. Hacker se proti rozsudku neúspěšně odvolal a tak byl převezen do USA, kde se rozhodne o jeho dalším osudu. [32]

Tento případ vyvolal ve Velké Británii velikou vlnu publicity. Lidé podnikali různé aktivity směřujících ke Garyho záchraně. Tvrdili, že Mckinnon je obětní beránek a Američané se mu snaží pomstít za to, že odhalil slabiny v jejich bezpečnostním systému.

7.2 Případy v rámci ČR

7.2.1 Phishingové a Pharmingové útoky proti České spořitelně



Obr. 4 Phishingový mail napodobující stránky České Spořitelny

Česká spořitelna se stává již po několikáté terčem Phishingového (kapitola 3.2.2.5) respektive Pharmingového (kapitola 3.2.2.6) útoku. Podobným útokům musela čelit již v dřívějších letech.

Jeden z posledních útoků se odehrál v lednu 2008. Cílem Phisherů se stalo internetové bankovnictví Servis 24 České spořitelny. Pomocí podvodné emailové zprávy (obrázek č.4) se pokusili získat klientské číslo a heslo adresáta. Samotná emailová zpráva vyzývala adresáta, aby se z bezpečnostních důvodů či z důvodu zkvalitnění služeb přihlásil ke svému účtu prostřednictvím odkazu, který byl umístěn v těle zprávy. Pokud tak dotyčný učinil, dostal se sice na podobné stránky, ale pouze vzhledově. Namísto originální adresy

www.servis24.cz se klient dostal na podvrženou adresu www.servis24.us. Pokud se uživatel na této stránce ke svému účtu přihlásil, poskytl přihlašovací údaje Phisherům k potenciálnímu zneužití.

Česká spořitelna uvádí, že pokud by některý klient na email zareagoval a přes tuto stránku se k účtu přihlásil, nemělo by mu hrozit nebezpečí, neboť pomocí pouhých dvou údajů se nedá služba Servis 24 zneužít. Klientům, kteří na email reagovali ČS doporučuje, aby co nejdříve zkontaktovali její klientské centrum se žádostí o zablokování služby a vydáním nových přihlašovacích údajů. ČS se snaží klienty před Spaningem a Pharmingem varovat a vydává prohlášení.

„S klienty nikdy prostřednictvím emailu nekomunikujeme o tak zásadních záležitostech, jako je například zabezpečení. Nikdy nevyžadujeme zadání osobních bankovních údajů jako je například PIN ke kartě či klientské číslo a heslo. Skutečnost, že pachatelé na podvodné webové stránce tyto citlivé údaje vyžadují, jasně poukazuje na to, že se jedná o podvod.“ [34]

V březnu musí spořitelna čelit dalšímu útoku, tentokrát se nejedná o Phishing ale o Pharming. Pharming je sofistikovanější druhem podvodu, kdy je do počítače nahrán škodlivý software, který způsobí přepsání IP adresy a přesměruje klienta na falešné stránky.

Vzhledem ke vzrůstajícímu počtu útoků podala banka trestní oznámení na neznámého pachatele a poukázala na to, že při útocích byly použity údaje internetového bankovnictví 107 klientů ČS z roku 2004, které byly zkopírovány softwarem z veřejného počítače. Všech 107 klientů pocházelo z jednoho regionu.

V polovině března se ukazuje, že phishingové a pharmingové útoky mají své první oběti. Muž z Děčína obdržel email s nabídkou o vylepšení služeb Servis 24 ČS. Protože nevěděl, že se jedná o Phishing, na email zareagoval a poskytl tak údaje potřebné ke svému účtu. Poté zjistil, že přišel o 5 400 Kč. [34]

ČS apeluje na své klienty, aby nepodceňovali zabezpečení svých počítačů a používali antivirové programy. Na svých webových stránkách www.csas.cz varuje před nebezpečím Phishingu a Pharmingu. Poskytuje zde základní informace a rady týkající se těchto podvodných praktik. Email je charakteristický tím, že je psán nesrozumitelnou češtinou. Za letošní rok se už objevilo 17 různých variant podvodných emailů.

7.2.2 Ostravský bankovní pirát

Tento případ se odehrál během září 2006 a jde zřejmě o dosud největší případ bankovního pirátství u nás.

Hlavní aktér Lumír Herič z Ostravy je podezírán z pokusu o zpronevěru více než 3 mil. Kč. Herič je člověk velmi znalý v práci s výpočetní technikou, studoval několik vysokých škol, žádnou však nedokončil. Jeho první problémy se zákonem přišly v roce 2004. Podařilo se mu nabourat do vnitřního počítačového systému Ostravské univerzity, kde získal výsledky přijímacího zařízení, které pozměnil. U soudu byl potrestán podmínkou.

Svůj druhý zločin uskutečnil v průběhu čtyř dnů v září 2006, jako student Vysoké školy báňské- Technické univerzity v Ostravě. K činu použil univerzitní počítač, do kterého nainstaloval speciální program, který vytvořil. Využil toho, že studenti počítače používali k ovládání svého bankovního konta prostřednictvím Internetu.

Program zaznamenával tlačítka stisknuta na klávesnici a získaná data pak posílal Heričovi na email. Z takto získaných dat byl Herič schopen vygenerovat přihlašovací údaje od člověka, který se přes počítač přihlásil ke svému účtu. Tímto způsobem nabourал 79 účtů, zfalšoval 800 platebních příkazů a na svůj účet se pokusil převést 3,2 mil. Kč. [35]

Bankovní příkazy prováděl pomocí wifi sítě, která znemožňuje identifikaci konkrétního odesilatele. Podvodně získaných peněz si ale neužil, peníze se mu podařilo převést pouze ze čtyř účtů a to jen na chvíli. 90 % podvodných příkazů Česká spořitelna odhalila ještě před převodem peněz na účet podvodníka. Spořitelna nakonec zareagovala i na 4 uskutečněné převody a provedla zpětnou transakci na účet skutečných majitelů. [36]

Následně podala trestní oznámení na neznámého pachatele a po této zkušenosti zvýšila svá bezpečnostní kritéria pro internetové operace.

Dnes lze provádět internetové transakce jen po potvrzení hesla zaslaného zprávou SMS.

Vyšetřování tohoto případu trvalo delší dobu, pouze zkoumání zabavených věcí trvalo 10 měsíců. Při domovní prohlídce policisté zabavili 7 počítačů a 500 CD a DVD disků. Po analýze všech zabavených materiálů, která skončila teprve v březnu 2008, se vyšetřovatelé rozhodli Heriče obvinit. Před zatčením však utekl a nyní se skrývá neznámo

kde. Na základě shromážděných důkazů byl mimo jiné obviněn z trestných činů padělání a pozměňování peněz. Za tyto trestné činy mu hrozí trestní sazba 10 až 15 let vězení. [36]

ZÁVĚR

Ve své bakalářské práci jsem se zabýval počítačovou kriminalitou a terorismem.

Nejprve jsem zpracoval poměrně rozsáhlou historii počítačové kriminality, kde jsem poukázal vůbec na první počítačový zločin, který spadá do počítačové kriminality. Je však podivné, že se v souvislosti se spácháním tohoto trestného činu mluví o počítačovém zločinu, když ve skutečnosti počítače vznikly až téměř o 150 let později.

Dále jsem popsal fungování prvních hackerských skupin, vznik prvních telefonních pirátů, kteří se zasloužili o vznik prvních BBS systémů- tedy prvních předchůdců Internetu. Velkým milníkem v celé historii počítačové kriminality byl vznik CD-ROMu, který umožnil počítačovým pirátům výrazně zvýšit jejich aktivity. V 90. letech došlo k velkému rozšíření osobních PC a tím pádem také Internetu, který dává větší prostor k páchání nelegálních aktivit. Pachatelem počítačových zločinu už není počítačový nadšenec nýbrž profesionál.

V kapitole ochrany před počítačovou kriminalitou jsem popsal některé opatření, která umožňují bojovat proti počítačové kriminalitě, ať už jde o psychologickou nebo technologickou prevenci. S vývojem kybernetiky souvisí i neustálá profesionalizace útočníků kdy do počítačové komunity stále více prorůstá organizovaný zločin, a tak postupně dochází ke vzniku kyberterorismu o kterém se v práci rovněž zmiňuji.

V závěru své práce jsem se věnoval rozboru konkrétních hackerských útoků, kde popisuji jednak osobnost pachatele, způsob provedení jeho útoku a následný trest.

Vzhledem k tomu, že útočníci mají k dispozici neustálé sofistikovanější a modernější vybavení a jejich metody útoku se neustále zdokonalují, je těžké předpovědět, co lze očekávat do budoucnosti pro běžného uživatele. V souvislosti s narůstající nebezpečnostní pachatelů a dopadem jejich činů nelze počítačovou bezpečnost a ochranu dat v žádném případě podceňovat. Naopak je potřeba se v této oblasti neustále vzdělávat na všech úrovních lidské společnosti, tj. ve školách ve firmách, úřadech atd.

Dalším problémem je to, že se o každém člověku sbírá čím dál víc osobních informací a údajů. To vede k nebezpečí například krádeže identity. Lidé by proto měli být obezřetní na to, komu svoje osobní a důvěrné údaje poskytují.

Mým hlavním cílem této práce bylo poukázat na aktuální a zajímavé projevy počítačové kriminality a vytvořit tak určitý přehled o této oblasti.

ZÁVĚR V ANGLIČTINĚ

I emloyed in my bachelor work to used computer criminality and terrorism.

At first I processed relatively wide history computer criminality, where I pointed at all on a first computer crime that fall to the computer criminality. It's however peculiar that in the context commitment hereof crime is talking about computer crime when in fact PCs arose as far as almost about 150 years later.

Further I'm described behaviour first hackers groups, inception first phone pirate that the deserved about rise first BBS system- so first predecessor of Internet. Big milestone in the whole story of the computer criminality was rise CD-ROM that the enable hacker markedly advanced their activities. In 90th years its get to large expansion personal PC thereby also expansion of Internet which gives bigger space to commission illegal activities. Offender of computer crime already isn't computer fanatic but professional.

In chapter of protection before computer criminality I described some steps that make possible fight against computer criminality, no matter what already is concerned psychological or technological prevention. With evolution cybernetics osculate also all the time professionalization attacker when into computer community increasingly grow through organized crime, thus step by step happen to rise cyberterrorism about which in work also I´m writing.

In the end of my work I devoted analysis concrete hacking attacks where describe partly person of the offender, facture of his attack and resulting punishment. Inasmuch as that attackers have to disposal all the time sophisticated and more modern equipment and their methods of attack all the time innovate, it is hard to predict what can be expect into the future for common user. In connection withaccruing offender´s hazardousness and fall their acts it is impossible computer security and data security least underestimate. On the contrary is need to edify in this area all the time on all levels of human companies, i. e. in schools in firm, office etc. Next problem is collection wherewith along more personal information and data about everyone . It leads to danger for example robberies identity. Therefore people should be heedful on it, who it´s their personal and confidential data providing.

My main aims those work was refer to actual and interesting manifestation computer criminality and set up so definite view about those areas.

SEZNAM POUŽITÉ LITERATURY

[1] MATĚJKA, M. *Počítačová kriminalita*. Praha : Computer Press, 2002. 165 s. Bakalářská práce.

[2] POŽÁR, J. *Informační bezpečnost*. Plzeň : Vykladatelství a nakladatelství Aleš Čeněk, s.r.o., 2005. 312 s. Bakalářská práce.

[3] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha 7 : Grada Publishing a.s., 2007. 288 s. Bakalářská práce.

[4] STŘIHAVKA, M. *Vaše bezpečnost a anonymita na Internetu*. Praha : Computer Press, 2001. 87 s. Bakalářská práce.

[5] [Zemánek, J. Cracking bez tajemství. Brno, Computer Press, 2002, s. 313]

ELEKTRONICKÉ ZDROJE

[6] Digitální underground. Martin.hinner.info [online]. 1996 [cit. 2008-05-13]. Dostupný z WWW: <http://martin.hinner.info/crackdown/czech/part2.html>.

[7] EMERY, D. About : Urban Legends and Folklore [online]. 2007 , 27. 4. 2007 [cit. 2007-05-13]. Dostupný z WWW: <http://urbanlegends.about.com/>.

[8] Co je to HOAX : Jak HOAX poznáme. Hoax.cz [online]. 2006 [cit. 2008-05-13]. Dostupný z WWW: <http://www.hoax.cz/cze/index.php?action=hoax_description>.

[9] Co je to HOAX : Jak HOAX škodí. Hoax.cz [online]. 2006 [cit. 2008-05-13]. Dostupný z WWW: <http://www.hoax.cz/cze/index.php?action= hoax_damages >.

[10] Co je to HOAX : Čím HOAX škodí. Hoax.cz [online]. 2006 [cit. 2008-05-13]. Dostupný z WWW: <http://www.hoax.cz/cze/index.php?action= hoax_damages >.

[11] První známý spam byl odeslán 3. 5. 1978. SecurityWorld.cz [online]. 2008 [cit. 2 008-05-13]. Dostupný z WWW: <http://www.securityworld.cz/sew.nsf/id/30-let-spamu>.

[12] Kauza Tvujdum.cz: ty adresy jsme koupili : Stručná historie kauzy Tvujdum.cz. Lupa.cz [online]. 2003 [cit. 2008-05-14]. Dostupný z WWW: <http://www.lupa.cz/clanky/kauza-tvujdum-cz-ty-adresy-jsme-koupili/>.

[13] Problém dneška? Spam! : Jak poznáte Spam ?. Tykvon.blogy.novinky.cz [online]. 2007 [cit. 2008-05-13]. Dostupný z WWW: <http://tykvon.blogy.novinky.cz/0706/problem-dneska-spam>.

[14] Hackeři, Crackeři, Rhybáři a Lamy? (2. díl) : Warez. Technet.idnes.cz [online]. 2004 [cit. 2008-05-13].

Dostupný z WWW: <http://technet.idnes.cz/hackeri-crackeri-rhybari-a-lamy-2-dil-d6y-/software.asp?c=A040812_5271894_bezpecnost>.

[15] Nebezpečné části internetu odhaluje studie McAfee. Technet.idnes.cz [online].2007 [cit. 2008-05-13]. Dostupný z WWW:

<http://technet.idnes.cz/nebezpecne-casti- internetu-odhaluje-studie-mcafee-fs5-/tec_denik.asp?c=A070314_143729_tec_denik_pka>.

[16] Co je to Hacker?. Zvon.org [online]. 1999 [cit. 2008-05-13]. Dostupný z WWW: <http://www.zvon.org/translations/hacker/Output/ch2_cs.html>.

[17] MIKO, K. NEBEZPEČÍ ZVANÉ HACKING : Bílé vs. černé klobouky. Dcit.cz [online]. 2003 [cit. 2008-05-13]. Dostupný z WWW: <http://www.dcit.cz/files/bezpecnost/BW_nebezpeci_hacking.pdf>.

[18] ČERVENÝ, L. Historie hackerství : Historie v datech. Fi.muni.cz [online]. 2003 [cit. 2008-05-13]. Dostupný z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2003/xcerveny.htm>.

[19] CD-ROM. Cs.wikipedia.org [online]. 2007 [cit. 2008-05-13]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/CD-ROM>.

[20] Hacking za hranicemi... : Phrack. Hysteria.sk/prielom/2/#1 [online]. 1998 [cit. 2008- 05-13]. Dostupný z WWW: <http://www.hysteria.sk/prielom/2/#1>.

[21] RYCHNOVSKÝ , L. Počítačová bezpečnost : Script kiddies. Ics.muni.cz/zpravodaj/articles/342.html [online]. 2005, č. 15 [cit. 2008-05-13]. Dostupný z WWW: <http://www.ics.muni.cz/zpravodaj/articles/342.html>.

[22] Script kiddies. somm.cz/ [cit. 2008-05-13]. Dostupný z WWW: <http://www.soom.cz/ >.

[23] JINDRA, M. Warez : Warez obecně. Ventum.net/items/warez [online]. 2005 [cit. 2008-05-13]. Dostupný z WWW: <http://ventum.net/items/warez>.

[24] SSL certifikáty. Mediaweb.cz/sluzby/ssl-certifikaty/ [online]. 2007 [cit. 2008-05-13]. Dostupný z WWW: <http://www.mediaweb.cz/sluzby/ssl-certifikaty/>.

[25] BITTO, Ondřej. Rhybaření střídá pharming. Lupa.cz/clanky/rhybareni-strida-pharming/ [online]. 2005 [cit. 2008-05-13]. Dostupný z WWW: <http://www.lupa.cz/clanky/rhybareni-strida-pharming/>.

[26] Definice základní metod kyberteroristického chovvání : Pharming. Specialista.info/view.php?cisloclanku=2006120205 [online]. 2007 [cit. 2008-05-13]. Dostupný z WWW: <http://www.specialista.info/view.php?cisloclanku=2006120205>.

[27] KUNEŠ, J. BSA se v nové kampani obrací na zaměstnance firem. Zive.cz/Bleskovky/BSA-se-v-nove-kampani-obraci-na-zamestnance-firem/sc-4-a-132027/default.aspx [online]. 2006 [cit. 2008-05-13]. Dostupný z WWW: <http://www.zive.cz/Bleskovky/BSA-se-v-nove-kampani-obraci-na-zamestnance-firem/sc-4-a-132027/default.aspx>.

[28] RADOMĚRSKÝ, V. Copyleft. Abclinuxu.cz/slovnik/copyleft [online]. 2004 [cit. 2008-05-13]. Dostupný z WWW: <http://www.abclinuxu.cz/slovnik/copyleft>.

[29] IT governance. Lbms.cz/Reseni/Tema/IT_Governance.htm [online]. 2008 [cit. 2008-05-13]. Dostupný z WWW: <http://www.lbms.cz/Reseni/Tema/IT_Governance.htm>.

[30] Dmitry Sklyarov. En.wikipedia.org/wiki/Dmitri_Sklyarov [online]. 2008 [cit. 2008-05-13]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Dmitri_Sklyarov>.

[31] ZAJÍČEK, L. Uvěznění ruského programátora vyvolalo protesty. Www.lupa.cz/clanky/uvezneni-ruskeho-programatora-vyvolalo-protesty/ [online]. 2001 [cit. 2008-05-13]. Dostupný z WWW: <http://www.lupa.cz/clanky/uvezneni-ruskeho-programatora-vyvolalo-protesty/>.

[32] Gary Mckinnon. Soom.cz/index.php?name=usertexts/show&aid=613 [online]. 2006 [cit. 2008-05-13]. Dostupný z WWW: <http://www.soom.cz/index.php?name=usertexts/show&aid=613>.

[33] Gary Mckinnon. Soom.cz/index.php?name=usertexts/show&aid=282 [online]. 2006 [cit. 2008-05-13]. Dostupný z WWW: <http://www.soom.cz/index.php?name=usertexts/show&aid=282>.

[34] Klient ČS přišel kvůli podvodnému e-mailu o 5400 Kč. Financninoviny.cz/index_view.php?id=302786 [online]. 2008 [cit. 2008-05-13]. Dostupný z WWW: <http://www.financninoviny.cz/index_view.php?id=302786>.

[35] Hacker zkusil z kont odčerpat tři miliony a uniká policii. Zpravy.idnes.cz/hacker-zkusil-z-kont-odcerpat-tri-miliony-a-unika-policii-pzv-/krimi.asp?c=A080229_135535_krimi_lpo [online]. 2008 [cit. 2008-05-13]. Dostupný z WWW: <http://zpravy.idnes.cz/hacker-zkusil-z-kont-odcerpat-tri-miliony-a-unika-policii-pzv-/krimi.asp?c=A080229_135535_krimi_lpo>.

[36] Bankovní pirát se pokusil ukrást přes tři miliony. Brnensky.denik.cz/z_domova/bankovni_pirat20080229.html [online]. 2008 [cit. 2008-05-13]. Dostupný z WWW: <http://brnensky.denik.cz/z_domova/bankovni_pirat20080229.html>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

LOD	Legion of Doom
BBS	Blue Board Systém
FBI	Federal Bureau of Investigation
FCFAAA	Federal Computer Frauf And Abuse Act
RE	Rada Evropy
P2P	Peer to Peer
NSA	National Security Agency
IT	Information Technology
AeBP	Advanced eBookl Processor

SEZNAM OBRÁZKŮ