Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Internetová kriminalita

Svatopluk Vácha

! ! !

Místo této strany vložíte zadání bakalářské práce.
(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Internetová kriminalita" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 10.března 2013 _____

Svatopluk Vácha

Poděkování

Rád bych poděkoval Ing. Čestmíru Halbichovi CSc. za pomoc, podnětné připomínky, vstřícný přístup a čas, který mi věnoval při konzultacích.

Internetová kriminalita

Internet Criminality.

Souhrn

Bakalářská práce Internetová kriminalita je zaměřena na problematiku kriminality páchané prostřednictvím Internetu. V práci jsou uvedeny základní informace a obecný popis struktury Internetu, historie vzniku Internetové kriminality, její dělení a informace o pachatelích.

V další části jsou pak detailně rozebrány jednotlivé druhy Internetové kriminality a způsob obrany proti každému z nich. Vše je doplněno názornými příklady a událostmi, které se v minulosti odehrály.

Práce se dále věnuje prevenci a obecným zásadám bezpečnosti na Internetu. Je zde uveden přehled institucí, které se touto problematikou v ČR zabývají a na které se lidé mohou v případě problémů obrátit. Dále je zmíněn trestní zákon platný pro ČR, včetně uvedení některých postihů při jeho porušení.

Na základě získaných zkušeností jsou stanoveny možné příčiny, které mají podíl na zvyšování Internetové kriminality. Na závěr je uveden její budoucí vývoj.

Klíčová slova: Internet, internetová kriminalita, internetový útok, autorská práva, trestný čin, pachatel, email, spam, cracker, phishing, pharming, zásady bezpečnosti, výhled do budoucna

Summary

Bachelor thesis internet crime is focused on the issues of crime commited thrrough the Internet. The paper presents the basic information and a general description of the structure of the internet, history of internet crime, its division, and information on the perpetrators.

In the next part are discussed in detail the variol type sof Internet crime and method of defensse against each of them. Is accompanied by illustrative examples and events that occurred in the past. The work i salso dedicated to the preventiv and general principles of security on the internet and an overview of the institutions dealing with this issue in the Czech Republic, including putting some penalties for its violation.

In conclusion, on the basis of the exprerience gained can be established pillars that have a negative impal on the growing internet crime and determined its future development.

Keywords: Internet, internet crime, internet attack, copyrights, offense, offender, email, spam, cracker, phishing, pharming, the principles of safety, future outlook

Obsah

Seznam obrázků

1 Úvod

S Internetem se v dnešní době setkáváme téměř na každém kroku. Jeho hlavními, nejdůležitějšími a nejvíce oceňovanými výhodami jsou především velmi snadná, rychlá a levná komunikace. Pro mnoho lidí je také důležitým zdrojem informací při práci i zábavě. Přes Internet vyřizujeme obchody, spravujeme své finance, komunikujeme s přáteli, hrajeme hry ap.

Je třeba si uvědomit, že tato nová technologie má kromě pozitivního přínosu také negativní stránku. Jedná se o čím dál tím více diskutované a probírané téma Internetové kriminality, s nímž je používání Internetu velice úzce spojeno. Internetovou kriminalitu jsem si vybral jako téma své bakalářské práce zejména proto, že se s ní dnes setkáváme téměř v každodenním životě a představuje poměrně vysokou míru rizika bezpečnosti pro každého z nás. Internetová kriminalita každoročně narůstá a je proto třeba se proti ní efektivně bránit.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je hlouběji popsat problematiku internetové kriminality od historie až po současnost. První část práce se zabývá seznámením s Internetem a dále popisem a analýzou internetové kriminality. Druhá část pak zásadami bezpečnosti a prevencí. Závěrem je na základě studia materiálů a osobních zkušeností uveden možný budoucí vývoj internetové kriminality.

2.2 Metodika

Metodika řešené problematiky je založena na studiu a analýze odborných informačních zdrojů. Praktická část je zaměřena na využití získaných znalostí při hodnocení internetové kriminality. Na základě syntézy teoretických poznatků a výsledků provedeného hodnocení budou formulovány výsledky bakalářské práce.

3 Internet

3.1 Co je Internet

Internet je celosvětový systém navzájem propojených počítačových sítí, ve kterých mezi sebou počítače komunikují pomocí protokolů TCP/IP[1].[2] Lidé využívají internet především jako prostředek komunikace a výměny dat. Internet stále více roste a rozvíjí se.

3.2 Struktura Internetu

URL – Uniform Resource Locator

Jedná se o řetězec znaků, který se používá pro přesné umístění informací či zdrojů na Internetu. Například webový portál Seznam má URL http://www.seznam.cz.

Paket

Slouží k přenášení dat mezi počítači. Data se přenáší tím způsobem, že se rozdělí na menší datové jednotky – tzv. pakety. Každý paket je označen číslem a obsahuje adresu cíle a adresu zdroje. Pakety server posílá různými trasami a nemusí být vždy doručeny stejnou cestou.

Router

Router neboli směrovač provádí přenos paketů. V podstatě jde o počítač, který určuje, jaký paket pošle kterou cestou. Při procesu posílání paketů,vyhledává různé spoje, kterými lze pakety co nejrychleji poslat. Při neprůchodnosti spojů hledá další možné varianty jejich poslání.

[1] Transsmition Control Protocol/Internet Protocol – sada protokolů pro komunikaci v počítačové síti
[2] Dostupný z WWW: <http://cs.wikipedia.org/wiki/Internet>

IP adresa

IP adresa je adresa, kterou vlastní každý počítač, pokud je připojen k Internetu. Jedná se o 32bitové číslo, které má tvar čtyř dekadických čísel oddělených tečkami, např. 62.84.148.230. Každý počítač má svoji jedinečnou IP adresu.

Doména

Doména vyjadřuje IP adresu ve slovní podobě. IP adresy jsou složité na zapamatování a doména právě tento problém řeší. V 90.letech minulého století byl uveden do provozu tzv. DNS – Domain Name System. Pomocí něho lze vyjádřit IP adresu slovní podobou a naopak ze slovní podoby je možno určit IP adresu.

Protokoly

Internet obsahuje 3 různé druhy protokolů. Prvním je TCP (Transmission Control Protocol), který zajišťuje řízení přenosu. Rozděluje data do malých balíčků – již zmiňovaných tzv. paketů a dbá na jejich správnou cestu. Druhým protokolem je IP (Internet Protocol) – dohlíží na to, aby se všechny pakety dostaly na určené místo v korektním pořadí a tam se zpět poskládaly. Velmi často je možné se setkat s označením protokolů TCP a IP dohromady, tedy jako protokol TCP/IP. Posledním protokolem je aplikační protokol (Aplication Protocol), který je charakteristický pro samostatné služby Internetu – například pro FTP[3] (File Transfer Protocol), HTTP[4] (Hypertext Transfer Protocol), SSH[5] (Secure Shell), DHCP[6] (Dynamic Host Configuration Protocol) a jiné.

[3] File Transfer Protocol – protokol pro přenos souborů mezi počítači pomocí počítačové sítě
[4] Hypertext Transfer Protocol – protokol pro výměnu hypertextových dokumentů ve formátu HTML
[5] Secure Shell – program a zároveň zabezpečený komunikační protokol v počítačových sítích, který používají TCP/IP
[6] Dynamic Host Configuration Protocol - síťový protokol založený na modelu klient-server, který zajišťuje automatické přidělení IP adresy a ostatních parametrů potřebných k připojení do sítě jako je adresa brány, maska podsítě a adresa DNS serverů

3.3 Co je internetová kriminalita

Internetová kriminalita (označována někdy také jako počítačová kriminalita, kybernetická kriminalita či kyberkriminalita) je označení takových trestných činů nebo přečinů, které jsou páchány pomocí počítače, resp. prostřednictvím Internetu. Jde o nelegální, nemorální a neoprávněná konání, která zahrnují zneužití údajů získaných prostřednictvím výpočetní techniky nebo jejich změnu.

3.4 Dělení internetové kriminality

Internetovou kriminalitu lze rozdělit podle několika hledisek. Mezi nejzákladnější dělení patří kriminalita páchaná na počítači = přímá počítačová kriminalita, a trestný čin s využitím počítače = nepřímá počítačová kriminalita. U přímého typu je subjektem trestného činu přímo počítač. Jedná se například o nepovolené kopírování počítačového programu, neoprávněné použití zařízení výpočetní techniky, odcizení dat uložených na počítačových médiích atd.

U druhého případu se jedná o využití počítače pro trestný čin, jakým může být například připisování fingovaných plateb, účtů inkasa, falešných objednávek zboží nebo i přípravu a plánování různých neplánovaných demonstrací a dalších trestných činů.

3.5 Pachatelé internetové kriminality

Mezi časté pachatele patří z větší části mladí lidé, ale jsou známy i případy, kdy se internetových útoků dopouštěly i děti. Pachatele můžeme rozdělit do dvou skupin na tzv. hackery[7] a crackery[8].

Hackeři vnikají do informačních a počítačových systémů za účelem hry či výzvy a mohli bychom říci, že jsou zdánlivě neškodní. Přesto je ovšem jejich vnikání a nebourávání se do systému jednoznačně nezákonné a navíc tím podrývají autoritu samotných firem a institucí, kde tuto nezákonnou činnost páchají. Ale mohou být i užiteční při odstraňování programátorských chyb a detekci vadného hardwaru.

Oproti tomu crackeři se cíleně nabourávají do počítačových sítí a své schopnosti využívají k nelegálnímu získávání informací, k destrukci programů, ovládnutí bankovních účtů atd. V současnosti se tento termín již moc nepoužívá a média často označují oba dva typy pachatelů pod „nesprávným“ označením hacker.

Pachatelé se často sdružují do skupin a tím jsou jejich činy promyšlenější a hůře řešitelné. Jednotliví členové skupiny se často ani neznají, jelikož veškerá jejich komunikace probíhá elektronickou formou.

[7] Hacker (White Hat) – je označení pro počítačového specialistu s perfektními znalostmi fungování systému, dokáže ho velice dobře používat a upravit si ho dle svých potřeb

[8] Cracker (Black Hat) – člověk, který zneužívá svých vědomostí při průnicích do software, často bývá špatně označován jako hacker

4 Historie

4.1 Historie internetové kriminality

Existuje mnoho materiálů a zdrojů, které se zabývají historií Internetové kriminality. Nejvíce mě zaujal postoj a výklad pana Michala Matějky, který ve své knize[9] rozděluje historii internetové kriminality do třech období: pravěk, středověk a novověk.

4.2 Období pravěku (do roku 1981)

Pravěkem nazýváme období od vynálezu telefonu do roku 1981, kdy byl poprvé na trh uveden první počítač. Jako první zločin v tomto období je považován případ, který se stal ve Francii roku 1801. Tehdy bylo v jedné firmě vyrobeno zařízení, které umělo automatizovat a opakovaně vykonávat úkony při tkaní látek. Zaměstnanci této firmy se však báli ztráty pracovních míst, a proto opakovaně sabotovali další vývoj tohoto zařízení, až bylo od jeho dalšího vývoje ustoupeno.

Dalšími zločiny v tomto období byly například přerušování a záměrné spojování k sobě nepatřících telefonních hovorů, vyměňování a kopírování počítačových programů mezi uživateli, porušování autorských práv apod.

S tímto obdobím je také spjato sestrojení BBS[10], díky kterému každý vlastník vybaveného počítače s telefonní linkou měl možnost být součástí kyberprostoru[11].

Se zrodem prvního elektronického počítače vzniká i pojem hacker. První hackeři však tenkrát měli zcela odlišnou funkci, než jim přisuzujeme dnes. Snažili se zejména o odstranění chyb a vylepšení prvních programů.

[9] MATĚJKA, Michal. Počítačová kriminalita, s. 17
[10] BBS - Bulettin Board System je systém elektronických nástěnek, které jsou rozděleny podle témat, do kterých mohou uživatelé přispívat. Tento systém předcházel Internetu a uživatelé se k němu připojovali pomocí vytáčení telefonní linky a modemu
[11] Kyberprostor je virtuální svět vytvářený počítači, telekomunikačními sítěmi apod.

4.3 Období středověku (1981-1994)

V tomto období se čím dál více počítačů připojovalo pomocí modemů do systému BBS. Důležitým rokem v tomto období je rok 1989, kdy došlo k tzv. floridskému skandálu. Jednalo se o přesměrování hovoru, který byl směřován na úřad kurátora na Floridě ale volající se opakovaně bez naúčtování poplatku dovolal na pornografickou linku ve státě New York. Tento „žertík“ pracovníka telefonního operátora umožnil vznik operace Sundevil, která proběhla v roce 1990. Policie si začala uvědomovat, že hrozba podobných útoků se může rozrůstat a dala patřičně najevo, že trestná činnost v kyberprostoru nebude tolerována. Tato akce se zaměřila hlavně na BBS s podezřelým obsahem a potlačování podvodů s kreditními kartami. Bylo zabaveno velké množství serverů, na kterých běželo BBS.

Za zmínku ještě stojí jména dvou hackerů: Roberta Morrise a Kevina Poulsena. Robert Morris byl strůjcem viru InternetWorm, kterým upozornil na novinku v podobě průniku do systémů za pomoci cílené infekce počítačovým virem. Kevinu Poulsenovi se zase podařilo proniknout do telefonních linek rozhlasové stanice a ovlivnit probíhající soutěž o automobil Porsche, který se mu podařilo tímto podvodem vyhrát. Oba dva hackeři byli odsouzeni a zatčeni.

Zajímavostí tohoto období je počátek používání kompaktních disků tzv. CD a s ním spojené nedovolené kopírování a rozšiřování. CD se nejdříve používala jako nosič hudebních nahrávek, postupně pak také k uchovávání dat. V tomto období začíná vznikat velké množství pirátských dílen, kde se CD nelegálně kopírovala a poté distribuovala.

4.4 Období novověku (1994 - současnost)

Charakteristickým znakem tohoto období je rozšíření sítě Internet a to hlavně jejího grafického prostředí WWW[12]. S tím bohužel přicházejí i počítačoví podvodníci, kteří se snaží této situace využit ve svůj prospěch. Začínají se rozšiřovat podvody s ukradenými kreditními kartami, útoky na bankovní systémy, zjišťování přístupových údajů a hesel do vládních systémů apod.

Zajímavým případem tohoto období je případ bankovního ústavu Citibank, kde se ruskému matematikovi Vladimiru Levinovi a jeho skupině hackerů podařilo prostřednictvím podvodných mailů a webových stránek vylákat z lidí přístupová hesla do internetových bankovnictví a obohatit se tak o značnou finanční částku,kterou si posílali na svůj účet z bankovních kont jednotlivých majitelů účtů.Mezi další případy patří například hackerská skupina CzERT, která měnila stránky různých serverů a opatřovala je svým emblémem v podobě zubatého čerta.

V současné době dochází ke stálému růstu internetové kriminality po celém světě. Přes již velice pokročilé metody, které se snaží s kriminalitou bojovat, se často nedaří podobným případům zabránit. Důvodem je značná vynalézavost a přizpůsobivost jednotlivých hackerů a podvodníků.

[12] World Wide Web je jedna ze služeb Internetu umožňující přenos webových stránek.

5 Nejznámější druhy internetové kriminality

V této kapitole jsou popsány nejznámější druhy Internetové kriminality, jejich princip fungování, možnosti odhalení a informace, jak se proti nim bránit.

5.1 Spamy a hoaxy

5.1.1 Spamy

Spamy jsou nevyžádaná sdělení, která jsou rozšiřována po Internetu a zaplavují nám ve velkém naše emailové schránky. Mezi nejčastější patří zejména reklamy na různé výrobky a služby, pornostránky, řetězové dopisy atd. Spameři je odesílají masově na obrovské množství adres, které zjišťují pomocí programů, které automaticky prohledávají internetové stránky a hledají v nich napsané emailové adresy, také však z různých pochybných formulářů na různé soutěže apod. Spamy pak většinou rozesílají ze smyšlených adres z cizích a špatně zabezpečených serverů, případně hacknutých počítačů, aby nebylo možné rozpoznat kdo a z jaké adresy tyto nevyžádané maily zasílá.

Proti spamu se lze bránit používáním dobrého antivirového programu, osobního firewallu[13] a nastavením nejvyšší úrovně zabezpečení internetových prohlížečů. Důležitá je i obezřetnost při instalování programů a nastavení parametrů Internetu. V případě nutnosti je možné se obrátit na Úřad pro ochranu osobních údajů[14], kterému problematika spamů přísluší.

[13] Firewall je síťové zařízení sloužící k tomu aby nikdo nebyl schopen proniknout zvenku internetu do našeho počítače, chrání uživatele před útokem virů a umožňuje volný a bezpečný přistup do Internetu
[14] Úřad pro ochranu osobních údajů (ÚOOÚ) – úřad dohlížející na ochranu soukromí a osobních údajů, vyřizuje také stížnosti na šíření spamu.

5.1.2 Hoaxy

Jedná se o anglické slovo, které označuje podvod či mystifikaci. V počítačovém světě takto nejčastěji označujeme poplašnou zprávu, která nás varuje před nějakým nebezpečím, nejčastěji před smyšlenými počítačovými viry, různými nereálnými nebezpečími (i mimo oblast výpočetní techniky) atd. Může se jednat i o falešné prosby o pomoc, fámy o mobilních telefonech, petice, výzvy, řetězové dopisy štěstí apod.

Šíření těchto zpráv obtěžuje příjemce, jelikož se v jeho schránkách objevují tyto zprávy několikrát denně, přitom také dochází ke zbytečnému zatěžování linek a serverů. Mezi další nebezpečí patří vyzrazení důvěrných informací a to především tak, že pokud uživatel přepošle hoax na další adresy, ponechává většinou adresy všech příjemců ve zprávě a šíří se tím velký seznam adres pro další cizí lidi. Některé typy hoaxů také poskytují nebezpečné rady, návody a postupy, které mohou mít fatální následky. Pro zajímavost bych uvedl v poslední době velice známý hoax informující přijemce emailu o použití svého PINU[15] k platební kartě. Adresát se po rozkliknutí mailu dozví informaci, že pokud se při výběru vlastních peněžních prostředků ocitne v nebezpečí má svůj PIN zadat pozpátku a přivolá tím policii. Je jasné, že tato zpráva je naprosto mylná a pokud skutečně dojde k zadání PINU uvedeným způsobem docílíme tím zabavení karty příslušným bankomatem. O této skutečnosti již informovaly bankovní ústavy a varovaly své klienty, aby tento mail ignorovali a nereagovali na něj.

Hlavními důvody vytváření hoaxů je vyvolání strachu, šíření již zmiňovaných falešných rad, manipulace s názory lidí, poškození institucí, firem a výrobků, vylákání peněžních prostředků, přilákání pozornosti nebo jen vystřelení si z důvěřivých uživatelů.

Důležitou ochranou proti hoaxu je především nevěřit všem informacím, které nám přijdou z neznámých zdrojů do emailových schránek a informace vždy nejprve prověřit. Nikdy nesdělovat neznámým osobám naše osobní informace (PIN, datum narození atd.) a za

[15] Personal Identification Number – je osobní identifikační číslo, pomocí něhož je možné se autorizovat (např. u platebních karet, vstupních kódů, mobilních telefonů apodob.)

žádných okolností nedůvěřovat zprávám, které nám zasílá naše bankovní instituce, jelikož ty s klienty v případě důležitého sdělení tímto způsobem většinou nekomunikují.[16]

Obrázek č.1: Varianta jednoho ze známých hoaxů na sociální síti Facebook

Zdroj: http://i.iinfo.cz/images/323/hoax-proti-falesnym-uctum-na-facebooku-1-prev.png

[16] Dostupný z WWW: <http://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25>. 18.5.2010

5.2 Phishing

Jedná se o metodu, při které je odeslán falšovaný e-mail příjemci, který klamavým způsobem napodobuje legální instituci s úmyslem dozvědět se od příjemce důvěrné informace jako je nejčastěji číslo platební karty nebo heslo k bankovnímu účtu. Takový email, většinou navádí uživatele, aby navštívil nějaké webové stránky a zadal zde tyto důvěrné informace. Tyto stránky mají podobný a téměř nerozeznatelný design jako instituce, za kterou se pachatel vydává, aby získal důvěru. Stránky této instituci samozřejmě nepatří a výsledkem je získání důvěrných údajů za účelem finančního zisku. Označení phishing je evidentně variací na slovo fishing (rybaření), kde pachatel nahazuje „háčky" v naději, že se do nich pár jeho obětí „zakousne". [17]

Základní typy phishingových útoků

Falšování identity – je nejoblíbenější a nejčastěji vyskytovaná metoda podvodu. Jedná se o plně funkční falešnou webovou stránku na kterou je uživatel nalákán. Stránka má obrázky ze skutečné webové stránky a může s ní být i propojena.

Přesměrování – je většinou spojeno s útoky na zákazníky eBay[18] a PayPal[19]. Příchozí emaily obsahují grafiku a přihlašovací rubriky, které se v emailových zprávách prodejců normálně vyskytují.

Vyskakovací okna – jedná se o odkaz, na který se klepne ve phishingovém e-mailu a vyskočí útočné okno, za vyskakovacím oknem se skrývá skutečný cíl, ze kterého se pachatelé snaží ukrást data.

Všechny typy phishingových útoků jsou velmi propracované a vždy se jedná o aktivní útok. Samotné vytvoření phishingové stránky trvá zhruba několik hodin. Během 1-2 dní je phisher schopný nakonfigurovat phishingový server včetně anonymní schránky a zrealizovat statisíce útoků a pak se vytratit.

[17] LANCE, James. Phishing bez záhad, s. 28
[18] eBay – je nejznámější americká internetová aukční síň, pomocí které lze provádět nákupy i prodeje
[19] PayPal – je internetový platební systém, umožňuje přesuny peněžních prostředků mezi účty, které jsou identifikovány emailovými adresami. Každý účet je spojen s jednou a více platebními kartami.

Nejznámější phishingové útoky

Technika phishingového útoku byla známa již v roce 1987 a termín phishing byl poprvé použit v roce 1996. K prvnímu reálnému útoku došlo v roce 1995 v síti giganta AOL[20] ve Spojených státech. Další útoky jsou známy z roku 2001, kdy byla napadena finanční instituce E-gold. Nedošlo však k velkému rozšíření tohoto problému díky včasnému zastavení útoku. Masivní útoky začaly přicházet v druhé polovině roku 2003.

V ČR byl zaregistrován první případ v března roku 2006. Jednalo se o falešnou zprávu bankovního ústavu Citibank. Zpráva informovala klienta, že na jeho účtě došlo k přijetí částky a pro připsání této částky na účet je potřeba tuto transakci potvrdit. Odkaz v emailové zprávě pak nevedl do Citibank, ale na webové stránky útočníka. Později byly uskutečněny útoky na Českou spořitelnu a Komerční banku. Poslední významnější útok byl veden v roce 2011 na Raiffeisenbank.

Obrázek č.2.: Podvodný email, informující klienty Citibank o příchozí platbě


Od: Citibank Online [alerts@citibank.cz]
Komu: Petr Nadenicek
Kopie:
Předmět: Important notice: Confirm Payment

citibank

Serial EM202-16

Vážený kliente Citibank Online®,

03/02/2006 na Váš běžný účet byl přijat převod v cizí měně na částku ve výši 2000 . Se shodou s *spotřebitelským souhlasem CitiBank® online*, je potřeba potvrdit tento převod pro jeho úspěšné zařazení na Váš běžný účet.

Pro potvrzení platby Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank® online a dále postupujte podle předloženého návodu. V případě nepřijetí potvrzení v průběhu 48 hodin, bude částka vracena odesílateli.

Pro vstup do programu CitiBank® online, **klikněte sem** >>>

S pozdravem
Služba CitiBank® Alerting Service

Zdroj: http://www.finance.cz/newsimg/Pavel_N/citibank_czphishing.GIF

[20] America Online – je poskytovatel internetových služeb, sídlo této společnosti je v New Yorku

Prevence proti phishingu

Základem je používání antiviru (např. Ad-Aware Pro, AVG Anti-Virus apod.) a antispamového programu (např. Cloudmark DesktopOne, SPAMfighter Pro apod.), který umí ochránit počítač před nevyžádanou poštou. Je také nutné mít na paměti, že banky a podobné instituce nikdy nepožadují v emailových zprávách po klientovi přihlášení k účtu.

Dále je potřeba provádět kontrolu, zda hypertextové odkazy ve zprávě nevedou na jinou adresu než je uvedena v textu, zda není přítomna podezřelá příloha ke spuštění či zpráva není napsána v netypickém jazyce. Podvodná emailová zpráva většinou odkazuje na stránky, které jsou velice podobné jako ty správné. Adresa podvržené stránky (URL) je však naprosto rozdílná. Například http://www.paypa1.com s jedničkou v názvu se tváří naprosto stejně jako správná doména http://www.paypal.com.

5.3 Pharming

Základem slova pharming je anglické slovíčko farming, což v překladu znamená pěstovat nebo farmařit. Pharming je velice úzce spjatý s phishingem a jeho princip je téměř totožný jako u phishingu, který jsem již ve své práci popisoval. Jediným rozdílem je to, že zatímco u phishingu si uživatel může všimnout rozdílu v názvu domén a útok ještě stihnout odhalit, u pharmingu je již tato nedokonalost odstraněna a jeho odhalení je tedy velice náročné.

Principem pharmingu je infikování uložených DNS[21] záznamů. Útočníci napadnou nedokonale zabezpečený DNS server a poté přidělí nějaké stránce zadané ve vyhledávači IP adresu stránky falešné. V praxi to znamená, že uživatel si ve vyhledávači zadá například URL adresu internetového bankovnictví. Útočník však pozměnil záznam DNS serveru a stránce je tudíž přiřazena podvržená IP adresa, která uživatele přesměruje na falešné stránky. URL adresa zůstává nezměněna a podstrčená stránka se tváří jako originál. Uživatel pak nemá důvod k žádnému podezření.

Jedinou účinnou ochranou je detailní prostudování SSL certifikátu. Ten hacker neumí zcela předělat a pouze ho trochu upraví, aby nebylo na první pohled jasné, že jde o podvod.

[21] Domain Name System – slouží k překladu doménových jmen (URL) na IP adresy a opačně

5.4 Sniffing

Tímto slovem se označuje neoprávněný monitoring elektronické komunikace. Jde o techniku, při které se ukládají a následně čtou TCP pakety. Používá se především pro odposlouchávání datové komunikace a jeho cílem je získat přístup k veškerému obsahu nešifrované komunikace, např. k přístupovým heslům a jménům, obsahu e-mailů a dalším souborům, které se posílají po internetu. Lze ho také použít při diagnostice sítě či zjišťování používaných služeb. Tuto techniku může používat i například zaměstnanec firmy a odposlouchávat tím veškerou firemní komunikaci, např. mezi vývojovým oddělením a vedením firmy. Získané informace může pak zpeněžit u konkurenční společnosti. Obdobně však může i vedení firmy odposlouchávat své zaměstnance a kontrolovat tak jejich činnost.

V každém případě se však jedná o trestnou činnost podle paragrafu o porušení tajemství dopravované zprávy. V případě, že pachatel využije získané informace pouze pro svoji potřebu je bohužel jeho odhalení velice komplikované a často se na něj ani nepřijde.

Základním ochranou je v tomto případě odeslat data tak, aby si je mohl přečíst pouze jejich adresát. Data, která odesíláme, lze zabezpečit vhodným šifrováním. Používá se šifrování dat pomocí SSL[22] certifikátů. Na trhu je také k dostání celá řada softwarových systémů, které jsou schopny ochránit a prověřit počítač před neoprávněným odposlechem.

[22] Secure Sockets Layer - je identifikační průkaz serveru, který obsahuje šifrovací klíč, který chrání data proti zneužití během jejich přenosu po Internetu.

5.5 Dialer

Tato problematika se týká připojení k síti Internet pomocí vytáčeného připojení přes modem. Jde o program, který umí změnit současné připojení k internetu nebo rovnou nastavit kompletně nové připojení, aniž by uživatel vůbec něco zjistil.

V praxi celý princip funguje tak, že během surfování na internetu uživatel může narazit na stránku, kde povolí instalaci programu, který se tváří například jako komponenta pro správné zobrazení stránky, a tím dojde ke spuštění samotného dialeru a hned je zaděláno na velký problém. Nejčastěji se jedná o pornografické stránky nebo stránky se sexuální tématikou ale může se jednat i o zdánlivě nevinné stránky. Místo klasického čísla pro internetové připojení pak dojde k automatickému přesměrování vytáčení na čísla se zvláštním tarifem, kde jsou velice vysoké sazby za každou minutu spojení a u poskytovatele internetu pak poškozenému uživateli nabíhá vysoký účet, který se může vyšplhat až na desetitisíce či statisíce korun.

Některé dialery však mohou být i legální. Představte si, že na internetu najdete server, jenž nabízí nějaký speciální (typicky erotický) obsah. Pro majitele serveru je (adult) dialer jednou z metod, jak umožnit přístup ke svým službám a zároveň mít jistotu, že za ně patřičně zaplatíte. Část telefonních poplatků jde – vedle telefonní společnosti – do kapsy právě majiteli. Zásadní problém však spočívá v tom, že drtivá většina podobných stránek neinformuje o použití dialeru dostatečně průhledně. Oznámí sice, že obrázky jsou zcela free, avšak pro jejich prohlížení si musíte nainstalovat zákaznickou aplikaci (samozřejmě dialer). Zmínku o tarifech pak najdete třeba někde v koutku milimetrovým písmem, v ujednání na straně x dole, černým písmem na tmavomodrém podkladu, apod.[23]

Účinnou obranou proti dialeru je používání antiviru, firewallu a úprava bezpečnostních nastavení v internetových prohlížečích. Další ochranou mohou být tzv. antidialery, při jejichž nastavení dochází k připojení pouze na ta čísla, která dáme do seznamu povolených. V případě podezřelého čísla dojde k zablokování modemu a upozornění uživatele. Možným řešením je i u poskytovatele telefonického připojení zablokování čísel s vysokou tarifikací.

[23] Co jsou to dialery a jak se proti nim bránit [cit. Ousmane Keita 16.11.2005]. Dostupný z WWW: < http://computerworld.cz/securityworld/muj-isp-je-na-kajmanskych-ostrovech-co-jsou-to-dialery-a-jak-se-proti-nim-branit-46399>. 27.2.2013

Obrázek č.3.: Ukázka dialeru, v případě odsouhlasení dojde k přesměrování.

Zdroj: http://trojanhelp.wz.cz/dia/dialer2.jpg

.

5.6 Zakázaná pornografie

Pornografie a sexuální tématika je bohužel v dnešní době na Internetu nejvyhledávanější a nejžádanější. Pornografický průmysl je nejvíce rozvíjející se odvětví, jehož obrat činí ročně desítky miliard amerických dolarů. Lidé, kteří pomocí Internetu sledují pornografickou tématiku, však vystavují svůj počítač vážným bezpečnostním rizikům. Nejčastěji bývá k pornografickým materiálům přistupováno z domova, daleko méně pak ze zaměstnání nebo internetových kaváren. Řada firem pochopitelně blokuje přístupy na stránky s pornografickou tématikou a představa, že by vedení společnosti zjistilo, že jejich zaměstnanci místo pracovního nasazení tráví čas u sledování porna by jistě nedopadla jinak, než kázeňským napomenutím či výpovědí.

Za obsahově rizikové jsou především pornografická videa zdarma ke zhlédnutí. Některá se zobrazují on-line, ale řada z nich vyžaduje stažení a spuštění na počítači. K tomu počítačoví piráti samozřejmě přidávají známé triky, jako např., že video nelze přehrát a přidají rovnou odkaz na stažení nového přehrávače popř. sad různých kodeků apod. a tím dochází samozřejmě k napadení počítače. Mnoho nabídek erotického obsahu na Internetu také požaduje autorizaci přes e-mailovou adresu. Uživatelé jsou pak atakováni spamem a jejich e-mail se dále šíří Internetem. Příslušný spam je samozřejmě cílený. Uživatelé pak většinou na odkazy v těchto e-mailech klikají a tím samozřejmě dochází k dalším problémům v podobě vyzrazení citlivých údajů apodob.

Nejvážnějším problémem je však šíření dětské pornografie. Tento druh pornografie se objevuje od osmdesátých let stále více jako téma mezi odborníky, kteří se touto problematikou zabývají. Dětská pornografie se bohužel stává velice lukrativním zbožím a to jak pro její tvůrce, tak i pro její distributory. Děti jsou navíc ohroženy i tím, že se samy nedokážou bránit a neuvědomují si plně důsledky svých činů a stávají se tak lehce manipulovatelnými. Vzhledem k novým technologiím, snazší dostupnosti Internetu a určité míry anonymity dochází tak k jejímu poměrně rychlému šíření. Děti přicházejí do styku s pornografií na Internetu již od 11 let. O rok později se z nich pak stávají pravidelní uživatelé. Jakýkoliv dohled rodičů bohužel tento problém neřeší, jelikož děti vyhledávají pornografii například v době, kdy si rodiče myslí, že si dělají své domácí úkoly nebo hrají oblíbené hry. Další fintou pornografického průmyslu je registrace dětských hrdinů do

internetových vyhledávačů a poté následné propojení s erotickým obsahem. V dobré víře pak děti hledají svého bojovníka a místo toho se dostanou na pornografické stránky.

Šíření pornografie, je v právním řádu ČR postihováno dle § 205 TrZ[24], který se týká ohrožování mravnosti. Tento paragraf je dělen do dvou odstavců. První odstavec zakazuje uvádění do oběhu, rozšiřování, výrobu či dovoz pornografických děl, v nichž se projevuje neúcta k člověku a násilí, zobrazení sexuálního styku s dítětem, se zvířetem nebo jiné sexuálně patologické praktiky. Ve druhém odstavci se zakazuje nabízení, přenechávání nebo zpřístupňování pornografických děl osobám mladším osmnácti let.

Obranou před nevyžádanou internetovou pornografii jsou především softwarové programy. Velice účinné jsou tzv. filtry. Jedná se o software, který dohlíží nad naším operačním systémem a sleduje všechny internetové stránky, které si uživatel na počítači zobrazuje. V případě, že se na stránkách vyskytne slovo, které je v jeho databázi označeno jako závadové, stránku a její obsah vůbec nezobrazí. Samozřejmě používání filtrů má také své nedostatky jako jsou například falešné poplachy, kdy nedojde k zobrazení podezřelé stránky jen z toho důvodu, že byla použita špatná sémantika ale stále i přes zdokonalující se vynalézavost autorů pornografických stránek patří k nejúčinnější ochraně.

[24] Trestní zákoník – zákon, který obsahuje skutkové podstaty jednotlivých trestných činů

5.7 Extrémistické projevy

Extrémismem označujeme ideologii skupin, která stojí mimo hlavní proud společnosti. Porušují a neuznávají základní etické, právní a další důležité společenské standardy, zejména ve spojení s násilím, historickým revizionismem, verbální případně fyzickou agresivitou, sociální demagogií, navíc motivované rasovou, náboženskou, národnostní či jinou sociální nenávistí. Pro tyto extremistické skupiny, ať už se jedná například o neonacisty, anarchisty, komunisty či různé sekty se Internet stává ideálním prostředím, kde mohou prezentovat své názory a také ho využívat jako prostředek rychlé a efektivní komunikace při domlouvání provedení nějakého útoku například na romskou či přistěhovaleckou komunitu v určitém městě apod.

Extremistickými projevy na internetu se nejčastěji pachatelé mohou dopustit podle platného trestního zákoníku následujících trestných činů: § 403 založení, podpora a propagace hnutí směřujících k potlačení práv a svobod člověka, § 404 projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka, § 352 násilí proti skupině obyvatelů a proti jednotlivci, § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob a § 356 podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod. [25]

Většinu závadných obsahů s podtextem extremismu obsahují webové stránky, jejichž poskytovatelé nemají sídlo v ČR. V mnoha případech jde o USA a Rusko, tedy domény s koncovkami .com, .org, .net, .ru a další. Pokud tedy chce česká policie informace o osobě, která umístila texty na webových stránkách, které jsou však umístěny v zahraniční, obrací se na orgány daného státu pomocí institutu právní pomoci. Základní podmínkou pro poskytnutí těchto informací však je, aby v žádaném státě platila tzv. oboustranná trestnost, tzn., že nestačí, aby byl daný skutek trestný jen podle českého práva, protože musí být také trestný i v dožádaném státě.

Problém oboustranné trestnosti, který se týká hlavně Spojených států amerických, na kterých se většina závadových stránek nachází a velice komplikuje a v podstatě znemožňuje odhalování a potlačování extremistických projevů v ČR, neboť pojetí americké svobody slova a projevu je bohužel velice rozdílné od evropského pohledu.

[25] Projevy extremismu na internetu [cit. Odbor bezpečnostní politiky 25.11.2010]. Dostupný z WWW: < http://www.mvcr.cz/clanek/projevy-extremismu-na-internetu.aspx>. 28.2.2013

Americké orgány činné v trestním řízení pak nemají právní titul, na základě kterého by mohly ČR sdělit potřebné informace. Problém neřeší jen ČR, ale i další státy. Tomuto tématu je v rámci Evropské unie věnována velká pozornost.

5.8 Doménové pirátství

Doménové pirátství neboli cyberasquatting vzniklo kombinací dvou slov, cyber (ze slova kybernetika) a squatting (obsazení prázdného domu bez povolení vlastníka objektu). Jedná se tedy o zaregistrování domény znějící identicky na název známého subjektu, případně registraci doménového jména, podobné již existujícímu názvu (například přidané či odebrané písmeno v názvu domény). Také však může jít o registrování domén, kterým již vypršela expirace, a tudíž jí opět může kdokoliv znovu zaregistrovat. Cybersquatteři pak danou doménu koupí a pokud byla například z nedbalosti původního majitele smazána, nezbývá nic jiného původnímu majiteli, aby se s novým vlastníkem dohodl na případném odkupu. Cybersquatteři pak samozřejmě nasadí vysokou cenu za účelem osobního obohacení, či v případě neodkoupení původním majitelem provozují tuto doménu a parazitují na dobré pověsti původní firmy.

Spory s doménovým pirátstvím se nejčastěji řeší soudní cestou a v ČR se ročně řeší až tisíc doménových sporů. Nevýhodou soudních procesů je však jejich značná pomalost a případ se tak často vleče dlouhou dobu. Proto často obchodní společnosti sahají po možnosti mimosoudního vyrovnání a doménu si od prodejce odkoupí.

Jedním z nejznámějších sporů v Česku byla rozepře o doménu Oskar.cz. Jednalo se o vleklý několikaměsíční spor společností Český Mobil a Comfor, majitele společnosti Oskar. Po vstupu nového mobilního operátora, jehož majitelem byla společnost TIW z Kanady, na český trh se hledal nejlepší název nové značky. Z několika možností byl Českým Mobilem vybrán název Oskar. Problém však byl v tom, že doménu oskar.cz měla registrovanou firma Oskar, s. r. o., ta však již nepoužívala ochrannou známku Oskar, tak jak měla. Český Mobil se potom dohodl s pardubickou firmou Oskar na převodu domény. Obě společnosti se pak ale rozešly v názoru, co mělo být kompenzací za převod. Český Mobil se tehdy nechtěl dohadovat o ceně a obrátil se na soud. Jedna žaloba byla vedená proti Comforu a druhá již "tradičně" proti CZ.NIC. Vleklý spor byl rozřešen až v dubnu roku 2003, kdy Český Mobil doménu oskar.cz koupil. Šlo o jakési mimosoudní vyrovnání mezi Českým Mobilem a bývalou firmou Comfor, jehož cena byla tehdy obchodním tajemstvím.

Vrchol tohoto typu pirátství je již na ústupu a celá problematika ustupuje do pozadí. V budoucnosti by však mohla mít význam převážně spojený s uváděním nových produktů na trh, nebo také při vzniku nových subjektů.[26]

[26] Cybersquatting: když jsou internetové domény v ohrožení [cit. Jiří Kocourek 7.4.2008]. Dostupný z WWW: < http://www.itbiz.cz/spory-domeny-cesko>. 28.2.2013

5.9 Zneužití kreditních a platebních karet

Se zneužíváním platebních karet, tzv. cardingem se můžeme v dnešní době setkat stále častěji. Možnost uskutečňování plateb pomocí těchto karet je pro nás dnes již samozřejmostí a pro většinu se stala nepostradatelnou součástí života podobně jako mobilní telefony. Narůstající je zvlášť objem plateb pomocí karet v on-line shopech, kde si zákazník může danou věc okamžitě zakoupit, čímž se i zároveň vyhne zbytečnému placení poplatků za bankovní převody.

Z počátku pachatelé této trestné činnosti úplně jednoduše platební karty kradli a opisovali si jejich čísla, která pak dále zneužívali pro zjištění čísla účtů jejich obětí. Často se také vydávali za pracovníky bankovních ústavů, kteří kartu vydali a předstírali vážnou chybu jejich vnitřního systému, díky které musí znovu zadat veškeré údaje o kartě. Majitel jim v dobré víře všechny požadované informace sdělil a tím se také velice často připravil o veškeré své úspory na svém účtu.

Postupem času došlo ke značnému zdokonalení metod zneužívání karet, k čemuž jistou mírou přispělo především umožnění plateb za služby a zboží právě přes Internet. Především se jedná o nestandardní služby typu online kasin, pornografických stránek, placených seznamek apod., kde obchodníci ve skutečnosti strhávají zákazníkům větší částky než uvádějí na svých stránkách. Pokud na to zákazník přijde, většinou se nedomáhá svých práv, díky choulostivým službám, které na internetu vyhledával. Toto se ve většině případů netýká plateb za zboží, které si kupujeme přes různé on-line shopy. Zde však platí, že se musíme mít na pozoru a kontrolovat si, zda nám z účtu opravdu byla strhnuta správná částka za nakoupené zboží.

Za novinku v této oblasti patří tzv. skimming, který umožňuje získání dat z magnetického proužku karty a dokonce i PINu. V praxi celá věc probíhá tak, že k bankomatu je připevněna kamera a čtečka karet, která je v oblasti, kam se vkládá karta do bankomatu. Pomocí čtečky pachatelé zjistí důležitá data a kamera zase odhalí vložený PIN při výběru z bankomatu. Poté již nic nebrání tomu, aby mohlo dojít k neoprávněnému výběru peněžních prostředků z účtu poškozeného. Tento postup je ale možný pouze pro starší typ karet, které nemají čip. Banky již v současné době vydávají kvůli lepší bezpečnosti karty s čipem.

5.10 Warez

Warez je označení pro nelegální distribuci filmů, softwaru, počítačových her apodob. Díky rozvoji Internetu se podařilo vytvořit jednoduchý distribuční kanál, který usnadňuje distribuci těchto médií. Výsledem tohoto šíření jsou pak situace, kdy nový film nebo kniha, jsou ke stažení už týden před očekávanou premiérou a vydáním.

Warezové verze software jsou distribuovány ve dvou podobách a to plné nebo ořezané (tzv. rip verze). Rip-verze jsou především menší, jsou zde vynechány zbytečné části a některé části jsou zkomprimovány. Plné verze jsou obsáhlé a kompletní, obvykle se jedná o obrazy DVD či CD disků.

Warez je distribuován tak, že osoba, která soubory poskytuje ostatním, pošle tyto soubory na nějaký server, který poskytuje úložiště pro data, v současné době je nejoblíbenější RapidShare. Servery však mají nastavená omezení většinou velikosti jednoho souboru, proto dojde k jejich rozdělení pomocí komprimačních programů typu WinRAR či WinZIP na menší části a celý zabalený soubor je chráněn heslem, které znemožňuje se správcům podívat, co soubor obsahuje ani ho smazat.

Při tomto nelegálním šíření obsahu se pachatelé dopouštějí trestného činu porušení autorských práv podle § 270 trestního zákoníku a soud jim může za spáchání tohoto činu uložit trest odnětí svobody ve výši až 8 let.

5.11 DoS útok

DoS (Denial Of Service = odepření služby) útoky se dají zařadit mezi velice nepříjemné útoky, které nás mohou v oblasti informační bezpečnosti potkat. Provedení tohoto typu útoku je poměrně jednoduché avšak obtížně se proti němu brání. To samé platí i pro jeho zaznamenání.

Ve své podstatě jde o to, udělat vybrané zdroje nedostupnými aby se k nim nedostali ani oprávnění uživatelé. Tento útok má obvykle dvě základní formy. V té první, útočník přinutí počítač k restartu, případně k zahlcení vlastních zdrojů takovým způsobem, aby nadále nebyl schopen poskytovat své služby. Ve druhé pak obsadí komunikační média mezi uživatelem a obětí tak, že mezi nimi nebude nastolena odpovídající vazba.

Tento útok bychom mohli v realitě přirovnat k vyčerpání zdrojů (například vyprodání všech vstupenek na určité představení). Pro představu, jaký následek takový útok může mít, použijme tento příklad. Každý z nás má jistě svou emailovou schránku. Útočník se rozhodne nám tuto schránku vyřadit z provozu právě DoS útokem. Začne do ní tedy nepřetržitě zasílat proud emailů ze svých schránek. Příval emailů začne sílit a náš server ho přestane zvládat, jelikož není v jeho silách přijmout tak obrovské kvantum emailů, které se do naší schránky hrnou. A o to útočníkům jde. Přestože se našeho počítače ani nedotkli, podařilo se jim email vyřadit z provozu.

V současné době známe čtyři základní způsoby provedení DoS útoků, s kterými je možné se setkat.

Prvním z nich je obsazení přenosové kapacity, kdy dojde k blokování přístupu k určité službě. Ze strany útočníka dojde k vytvoření takového provozu, který naprosto zatíží přístupovou cestu a tím odřízne ostatní uživatele. K zahlcení přístupových cest většinou použije několik slabších linek, zkušenější útočníci jsou schopni použít i jednu silnější linku ale tento výskyt je ojedinělý.

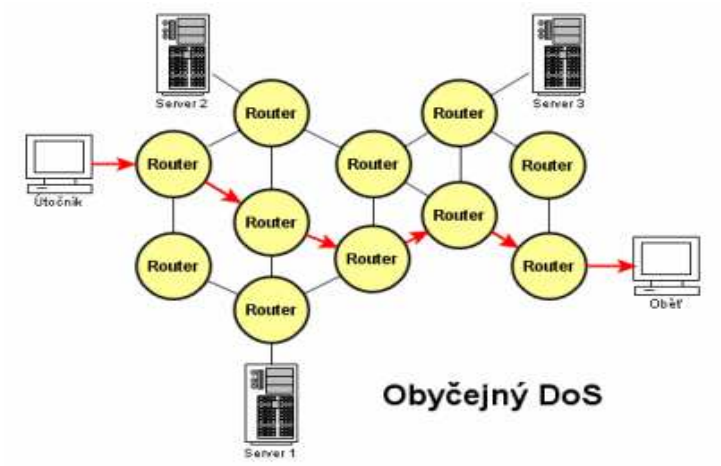
Dalším způsobem útoku je přisvojení si systémových zdrojů. Cílem je spotřebovat limitované zdroje oběti. Tedy například paměť serveru, procesorový čas nebo volná kapacita na disku. Útočník vytvoří takový stav, kterým získá značnou část systémových zdrojů a na oprávněné uživatele zbude pak jen pouze zanedbatelná kapacita.

Třetím způsobem je zneužívání chyb v programech. Tyto chyby mohou být jak známé, tak i nově objevené. Většinou jsou napadány servery, u kterých správci zanedbávají záplatování. Díky chybě pak program nedokáže reagovat na zvláštní situaci a může tak dojít k jeho zhroucení, pádu, zacyklení apod. V důsledku toho se pak regulérní uživatel nemůže dostat tam, kam potřebuje.

Napadení systému směrování paketů a DNS je pak posledním způsobem provedení tohoto typu útoků. Na DNS serverech dojde po zásahu útočníka ke změně záznamů o IP adresách. Ty jsou samozřejmě měněny ve prospěch útočníka. Ten pak poměrně snadno umístí nekorektní informaci do odkládací paměti jmenného serveru. Všem žadatelům jsou poté poskytovány mylné informace, které se týkají směrování.

Ochrana před DoS útoky je poměrně složitou záležitostí ale je možné se s ní vypořádat. V každém případě se jedná o celý komplexní soubor opatření a nejde jen o jedinou poučku. Základem je pravidelná kontrola instalace bezpečnostních záplat. Router by měl být nastaven tak, aby první paket z různé IP adresy nebyl vpuštěn dál. Dále by měly být vypnuty nepoužívané služby, znemožněna možnost zápisu na disk, existence záložních zdrojů a provádění pravidelných záloh, aby byly v případě odstavení systému ihned k dispozici. Samozřejmostí by měl být i připravený a krizový plán, včetně zajištění dobrého kontaktu na poskytovatele připojení, se kterým lze případný incident vyřešit jednodušeji a rychleji.

Obrázek č.4.: Schéma principu klasického DoS útoku



Zdroj: http://i.iinfo.cz/urs/obycejny-116039658405511.GIF

6 Prevence a zásady bezpečnosti na Internetu

Informační prevenci bychom mohli rozdělit na dvě části, a to na prevenci technologickou a psychologickou. Jedna část doplňuje druhou a nemohly by existovat samostatně. Prevence je bohužel velkým problémem, jelikož bývá často přehlížena a zanedbávána a díky tomuto faktu dochází ke stálému nárůstu internetové kriminality. Přitom by si stačilo uvědomit, že s jejím použitím by nám mnohdy odpadlo řešení nemalých problémů.

6.1 Technologická prevence

Technologická prevence zabezpečuje programy proti nelegálnímu užití a sítě proti neoprávněným přístupům a průnikům. Útoky hackerů jsou nesmírně rychlé a někdy útočníkům stačí pouze několik hodin, než překonají nově nastavenou ochranu či nově vyvinutý antivirový program. Neustále tak musí docházet k vývoji nových typů ochran proti kopírování či vniknutí do systémů. Antivirové programy procházejí denními aktualizacemi a veškeré druhy ochran a zabezpečení (např. firewall, antispyware[27] atd.) jsou velice rychle vyvíjeny ve všech směrech, aby se podobným útokům co nejvíce předcházelo.

Nelze však na stoprocentně tvrdit, že by tento druh prevence byl tak dokonalý, že by jeho použitím nedocházelo k žádným útokům. Pachatelé internetové kriminality jsou vždy o krok napřed. Vyvíjení technologické prevence jim velice komplikuje jejich trestnou činnost a zvyšuje její náročnost. Tím i částečně dochází ke zúžení okruhu pachatelů. V podstatě jde o jakýsi nekonečný boj mezi vývojáři ochranných prvků a útočníky.

[27] Antispyware - je program, který má za úkol odstranění či blokování spywaru.
Spywarem je pak označen program, který bez vědomí uživatele odesílá prostřednictví internetu data z počítače za účelem využití údajů pro budoucí reklamní účely, může jít však i útok a získáni citlivých údajů

6.2 Psychologická prevence

Oproti tomu psychologická prevence pak působí proti tomuto druhu kriminality vytvářením povědomí o společenské nepřijatelnosti a nemorálnosti protiprávních činů, které s internetovou kriminalitou souvisí a informuje uživatele využívající informační technologie o následcích porušování zákonů. Jejím úkolem je tedy zvyšovat povědomí o tom, co je povolené a co se naopak nesmí.

Využívá širokého spektra reklamních spotů, upoutávek či krátkých filmů. Také se jedná o různé internetové diskuze s odborníky, zabývající se touto problematikou. Mnohdy si uživatelé Internetu ani neuvědomují, jak se velice snadno mohou sami dopustit trestného činu například již používáním nelegálních počítačových programů apod. Proto je tato část prevence velice důležitá a neměla by se zanedbávat.

6.3 Zásady bezpečnosti na Internetu

V této podkapitole bych rád uvedl základní a užitečné zásady při používání Internetu. Je zřejmé, že jejich používáním nelze zcela vyloučit riziko nějakého útoku, ale jejich dodržováním se jistě tato rizika minimalizují a je na každém z nás, jak se na Internetu budeme chovat a k čemu ho budeme využívat.

Pravidla všeobecné prevence:

- V internetové komunikaci nikdy nesdělujeme citlivé informace (bydliště, telefonní kontakt, emailová adresa a podobně). Je nutné mít na paměti, že sdělení těchto údajů prostřednictvím sociálních sítí je podobné, jako kdybychom vyšli na veřejné prostranství a začali tam tyto informace rozkřikovat.
- Používáme výhradně legální software. Je zde totiž záruka pravidelné bezpečnostní záplaty. Užíváním nelegálního software se navíc zvyšuje problematika malwaru[28]. Samo o sobě je pak jakékoliv nelegální používání kvalifikováno jako protiprávního jednání.
- Nepodílíme se na jakémkoliv nelegálním dění na Internetu (sdílení nebo stahování nelegálního software, videa, hudby a pornografie).
- Neotvíráme soubory přiložené k emailům od neznámých osob.
- Užíváme kvalitní antivirové programy s dostatečnou aktualizací.
- Data z externích zdrojů (USB, email, CD-ROM atd.) vždy kontrolujeme vhodným antivirovým programem. Důležitá je pravidelná kontrola celého harddisku.
- Dáváme pozor na podivné hry a různý freeware[29].
- Pozor na spustitelné programy (koncovky *.com, *.exe a *.bat). Nenechat se zmást použitím dvou přípon souborů. Opravdová přípona je zcela na konci v názvu souboru, např. soubor fotka.jpeg.exe není obrázek ale pravděpodobně virus.
- Pozor na možnost přesměrování. Hlídat aktivní okna internetových stránek, která umožňují výběr mezi "ne" a "ano". Občas se i při volbě obou možností může stát,

[28] Malware – označení pro jakýkoliv software, jehož účelem je poškození počítače. Může jít například o krádež citlivých údajů z počítače, zpomalení jeho chodu apod.

[29] Freeware – jedná se o software, který je distribuován bezplatně. Bezplatné používání je definováno v licenční smlouvě, která je většinou specifická pro konkrétní druh freeware.

že účty za připojení budou astronomické části. Při podezření na přesměrování vypnout konkrétní okno a rovnou i celý prohlížeč.

- Pravidelně zálohovat cenná data.
- Zákaz přístupu k osobnímu počítači pro osoby, které nedodržují bezpečnostní pravidla
- Chránit svůj počítač bezpečnými a často obměňovanými hesly. Většina uživatelů sítě Internet si volí velice jednoduchá snadno prolomitelná hesla. Často se jedná o jména členů rodiny, jednoduchou posloupnost znaků či dokonce svoje vlastní jméno. Heslo by se nemělo skládat pouze z písmen nebo pouze z číslic. Ideální je, aby heslo obsahovalo kombinaci velkých a malých písmen a čísel. Optimálně pak do hesla přidat ještě nějaký symbol.
- V případě nalezení nelegálních či pochybných věcí na Internetu (extremistická propaganda, pornografie, podvodné maily apod.) ohlásit tuto skutečnost Policii České republiky.

7 Boj proti Internetové kriminalitě

7.1 Organizace bojující proti Internetové kriminalitě

Bojem proti internetové kriminalitě se zabývají různé organizace. Hlavní organizací, která bojuje proti tomuto druhu kriminality je stát a jeho složky, kteří určují hranice toho, co je etické, případně společensky přijatelné a co už není. Stát prostřednictvím parlamentu tyto hranice vytváří a pomocí systému policie, státních zastupitelství a soudu je pak vymáhá a jejich nedodržování trestá.

Dalšími organizacemi jsou nestátní subjekty, které chrání a informují veřejnost, také však dokáží vyvinout tlak na státní orgány, aby mohlo dojít k nárůstu intenzity boje proti ní. Jejich výhodou je schopnost pružně reagovat, a tímto mohou státu v určitých případech velice pomoci. Většinou se jedná o organizace nebo lobbistické skupiny, které se věnující prevenci, protože nemají na rozdíl od státu téměř žádné pravomoce.

7.2 Policie ČR

Internetovou kriminalitu vyšetřuje v České republice obdobně jako jinou trestnou činnost Policie ČR. V roce 2005 začaly vznikat při Krajských ředitelstvích tzv. Oddělení informační kriminality, která vyhledávají důkazy internetové kriminality a podporují tím útvar Úřadu služby kriminální policie a vyšetřování (ÚSKPV). Kriminalistickou počítačovou expertizu pak provádí Kriminalistický ústav Praha.

Novinkou, která vznikla v srpnu roku 2012 je možnost nahlášení internetové kriminality (například různé podvody, protiprávní jednání atd.) přímo pomocí on-line formuláře na oficiálních stránkách http://www.policie.cz.

Obrázek č.5.: Elektronický formulář PČR pro nahlášení internetové kriminality

Zdroj: http://aplikace.policie.cz/hotline/

7.3 BSA (Business Software Aliance)

Jedná se o mezinárodní organizaci, která v sobě zahrnuje velké množství známých firem jako např. Adobe, Intel, Microsoft, Corel, Apple a mnoho dalších. Její specializací je ochrana autorských práv jejích členů a zaměřuje se na boj proti softwarovému pirátství. Dále šíří osvětu v oblastech bezpečného používání Internetu a informačních technologií. Úzce spolupracuje s policií a poskytuje jí různá doporučení, včetně vytipovaných míst, kde by případně mohlo docházet k softwarovému pirátství. Mimo jiné je provozovatelem internetových stránek http://www.softwarelegalne.cz, kde lidé mohou online oznamovat případné softwarové pirátství.

Po přijetí oznámení používání nelegálního software odešle BSA dané instituci dopis, jehož součástí je i čestné prohlášení, že firma používá pouze legální software. Pokud firma vyplní prohlášení, pak je vše v pořádku a dále se již nemusí nic řešit. V případě, že instituce papír nevyplní a odmítá spolupracovat, BSA jako samotná organizace nic nezmůže, ovšem může vše předat policii ve věci používání nelegálního sofware a ta pak už danou situaci bude řešit dle zákona.

Obrázek č.6.: Formulář BSA pro nahlášení používání nelegálního firemního software

FORMULÁŘ PRO NAHLÁŠENÍ SOFTWAROVÉHO PIRÁTSTVÍ

(bez vyplnění červeně označených kolonek není možné podniknout řádné právní kroky)

Jméno společnosti/uživatele (kde se nachází nelegální software):

Předmět činnosti:

Adresa:

Odpovědná osoba za řízení firmy:

Provozovny, pobočky:

Počet zaměstnanců:

Kontakty na firmu (telefon,web):

Počet počítačů:

Počet serverů:

Nelegálně užívaný software:

Výrobce	Název	Verze	Počet nelegálních kopií

Kde se nachází nelegální software (např. podlaží, číslo místnosti, jaké počítače). Případně uveďte kontakt na Vás, pokud chcete vystoupit z anonymity (Vaši identitu uchováme v tajnosti).

Kdo je za užívání nelegálního softwaru odpovědný:

Zdroj: http://diit.cz/data/images/49019.png

7.4 CERT a CSIRT týmy

CERT (Computer Emergency Response Team) a CYRT (Computer Security Incident Response Team) jsou bezpečnostní týmy, které mají za úkol minimalizovat množství bezpečnostních incidentů v konkrétní přidělené síti. Incidenty jsou ve většině příkladů rozesílání spamu, pharming a phishing, znemožňování standardního fungování sítě a podobně.

Bezpečnostní týmy se utváří v jednotlivých organizacích, které připojení k Internetu buďto zprostředkovávají nebo ho využívají. V České Republice je nejznámější a největší tým CSIRT.CZ. Je provozován sdružením CZ.NIC z.s.p.o.[30]. Úkolem tohoto týmu je hlavně pomoc při vytváření dalších bezpečnostních týmů s nižší úrovní a koordinace jejich vzájemné komunikace.

7.5 NCBI (Národní centrum bezpečnějšího Internetu)

NCBI provádí osvětu o bezpečném a zodpovědném užívání Internetu. Pořádá vzdělávací akce, které jsou cíleny hlavně na děti a jejich rodiče, mladistvé a mladší generace. Spolupracuje s některými partnery, jako jsou, Google Česká republika, Telefónica O2 Czech republic, Centrum.cz, Policie ČR, Ministerstvo vnitra, Ministerstvo školství a Policie ČR. Zaměřuje se především na boj s extremismem, pedofilií a podvodným jednáním na Internetu. Provozuje také internetové stránky, na kterých mohou lidé nahlásit případné porušování zákona.

[30] CZ.NIC z.s.p.o. – je zájmové sdružení právnických osob. Jeho hlavní činností je provozování registru doménových jmen .cz

7.6 Trestní zákon v ČR a jeho postihování

Postihování počítačové a internetové kriminality se v ČR řídí novým trestním zákoníkem z roku 2009, konkrétně se jedná o zákon č.40/2009 Sb. Dá se říci, že tento trestní zákoník oproti předcházejícímu, č.140/1961 Sb. reaguje částečně na vývoj kriminality, osobnosti pachatelů a také díky nově nastaveným parametrům má alespoň malý vliv na snížení všech projevů počítačové a s tím související internetové kriminality.

Pro představu a zajímavost je zde z tohoto zákoníku uveden stručný výtah některých trestných činů a jejich trestněprávní postihy:

- Neoprávněné nakládání s osobními údaji - odnětí svobody na délku až 5 let
- Ohrožování mravnosti - odnětí svobody až na délku 1 roku, propadnutí věci nebo peněžitý trest
- Porušování tajemství dopravovaných zpráv - odnětí svobody až na délku 1 roku
- Porušování autorských práv - odnětí svobody až na délku 2 let, v případě velkého rozsahu až 5 let, propadnutí věci nebo peněžitý trest
- Podněcování nenávisti vůči skupině - odnětí svobody až na délku 2 let
- Podpora a propagace hnutí směřujících k potlačování práv a svobod člověka - odnětí svobody na délku až 5-8 let
- Nepoctivé provozování online sázek a her - odnětí svobody až na délku 5 let, případně peněžitý trest

8 Závěr

Problém internetové kriminality se stal v současnosti velmi diskutovaným a vyhledávaným tématem, který si v každém případě zaslouží velkou dávku pozornosti, ať už ze strany odborné či laické veřejnosti. Cílem mé bakalářské práci bylo co nejvíce a srozumitelnou formou přiblížit problematiku Internetové kriminality v ČR a upozornit na veškerá úskalí, která s používáním Internetu souvisí.

Následující možný výhled do budoucna a směr, kterým se bude internetová kriminalita ubírat lze jen těžko přesně předpovídat. Osobně se domnívám, že dle uplynulých let a díky stálému nárůstu této kriminality lze vyvodit určité dílčí závěry, které by mohly být platné i do budoucna.

Je pravděpodobné, že jednotlivci nebo skupiny útočníků, právě tak jako vyšetřovatelů budou dále existovat, bez jakéhokoliv ohledu na technologické prostředky používané k páchání protiprávní činnosti. Oba tyto tábory se budou ve svých činnostech stávat dokonalejšími, včetně modernizace svých technologií a postupů. Zlepšení postupů na jedné straně bude mít za následek stejně kvalitní posun na druhé straně. Útočníci budou ale vždy o malinký krůček napřed. Důkazem toho mohou být nedávné DoS útoky (o kterých jsem se již v předcházející kapitole zmiňoval) na začátku března 2013, kdy v průběhu čtyřech dní docházelo k masivnímu napadání a výpadkům hned několika zpravodajských webů, další den oblíbených webových portálů a následně několika internetových bankovnictví. Přesto však jejich boj bude téměř vyrovnaný bez větších šancí na potenciální zvrat.

Podle mého názoru snížení internetové kriminality lze dosáhnout zvýšením prevence, podrobnějším výzkumem a vzděláváním v této oblasti a v neposlední řadě systematickým sjednocením právních úprav v celosvětovém rámci.

Je nutné vytvoření takové právní výchovy a propagandy v boji s internetovou kriminalitou, která by zahrnovala širokou veřejnost. Celospolečenské zapojení do této problematiky by mohlo být velice přínosné. Pokud totiž společnost bude vědět, jakými způsoby ochránit svá data a změní se její přístup například k porušování autorských práv, může dojít k omezení nebo zpomalení nárůstu této kriminality. Zatím tomu tak není a tato nelegální činnost je společností běžně tolerována.

Výzkum by měl pružně reagovat na nově se vyskytující jevy a vyvíjení informačních technologií. Samozřejmostí by mělo být i postupné zvyšování kvalifikace složek, které vyšetřují tuto problematiku, odstranění jazykových bariér a zlepšení technického vybavení.

Posledním zmíněným problémem v boji s počítačovým zločinem je také problém s teritorialitou práva. Internet nemá hranice a připojit se k němu můžeme téměř ze všech koutů světa, ale vzhledem k neexistenci unifikovaných právních úprav, dochází k absurdním situacím, kdy v jedné zemi je povoleno to, co v jiné je striktně zakázáno.

Závěrem bych uvedl, že téměř s jistotou nebude docházet k poklesu internetové kriminality, pokud se nezlepší uvedené podmínky a nedojde ke sjednocení právních řádů jednotlivých zemí.

Seznam použité literatury

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

ENDORF, Carl. *Detekce a prevence počítačového útoku.* Praha: Grada Publishing, a.s., 2005. 355 s. ISBN 80-247-1035-8.

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

LÁTAL, Ivo. *Ochrana informací, dat a počítačových systémů.* Praha: Eurounion, 1996. 238 s. ISBN 80-85858-32-0.

YANG, Susan; AITEN, Dave. *The hacker's handbook : the strategy behind breaking into a defending networks.* Boca Raton : Anerbach, 2004. 860 s. ISBN 0-8493-0888-7.

HALBICH, Čestmír, BRECHLEROVÁ, Dagmar. *Bezpečnost informačních systémů: vybrané kapitoly.* Praha: Credit, 2003. 100 s. ISBN 80-213-1090-1.

ČANDÍK, Marek. *Základy informační bezpečnosti.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 107 s. ISBN 80-7318-218-1.

LANCE, James. *Phishing bez záhad.* Praha: Grada Publishing, a.s., 2007. 282 s. ISBN 80-247-1766-2.

SCAMBRAY, Joel, a další, a další. *Hacking bez tajemství.* Praha: Computer Press, 2001. 596 s. ISBN 80-7226-549-0.

SMEJKAL, Vladimír. *Internet a §§§* . Praha: Grada Publishing, a.s., 1999. 166 s. ISBN 80-7169-765-6.

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

SMEJKAL, Vladimír. *Internet a §§§* . Praha: Grada Publishing, a.s., 1999. 166 s. ISBN 80-7169-765-6.

Internetové zdroje

HORÁK, Vladimír. *Spam.* [on-line]. 9.1.2006 [cit. 2013-02-25]. Dostupný z WWW: <http://uvt1.cuni.cz/email/spam/index.html>.

KAMIL, Kopecký. *Co je hoax. E-bezpeci.* [on-line]. 18.5.2008 [cit. 2013-03-01]. Dostupný z WWW: <http://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25>.

OUSMANE, Keita. *Můj ISP je na Kajmanských ostrovech. Co jsou to dialery a jak se proti nim bránit? Computerworld.* [on-line]. 16.11.2005 [cit. 2013-02-27]. Dostupný z WWW: <http://computerworld.cz/securityworld/muj-isp-je-na-kajmanskych-ostrovech-co-jsou-to-dialery-a-jak-se-proti-nim-branit-46399>.

Kaspersky Laboratory. *Vulnerabilities and hackers.* [online]. 1997-2013 [cit. 2013-08-05]. Dostupný z WWW: <http://www.securelist.com/en/threats/vulnerabilities>.

POLZER, Jan. *PayPal Phishing stále zákeřnější.* [online]. 13.6.2006 [cit.2013-02-28]. Dostupný z WWW: <http://www.maxiorel.cz/paypal-phishing-stale-zakernejsi>.

OBR, Jiří. *Sniffing: Odposlech datové komunikace. IZBiz.* [online]. 6.3.2009 [cit.2013-03-03]. Dostupný z WWW: <http://www.itbiz.cz/sniffing-odposlech-datove-komunikace>.

PAUKERTOVÁ, Veronika. *Elektronická informační kriminalita*. *Ikaros*. [online]. 2.8.2006 [cit. 2013-03-06]. Dostupný z WWW: <http://www.ikaros.cz/node/3554>.

BEDNÁŘ, Vojtěch. *Pharming je zpět a silnější. Lupa.* [online]. 23.3.2007 [cit. 2013-08-03]. Dostupný z WWW: <http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi>.

POLZER, Jan. *PayPal Phishing stále zákeřnější.* [online]. 13.6.2006 [cit.2013-02-28]. Dostupný z WWW: <http://www.maxiorel.cz/paypal-phishing-stale-zakernejsi>.

PŘIBYL, Tomáš. *Zákeřný útok jménem DoS.* [online]. 1.11.2006 [cit.2013-02-28] Dostupný z WWW: <http://www.systemonline.cz/it-security/zakerny-utok-jmenem-dos.htm>.

Mvcr.cz [online]. [cit. 2013-2-25]. Dostupný z WWW: <http://www.mvcr.cz>.

Policie.cz [online]. [cit. 2013-2-25]. Dostupný z WWW: <http://www.policie.cz>.

Sofwarelegalne.cz [online]. [cit. 2013-03-04]. Dostupný z WWW: <http://www.softwarelegalne.cz>.

Epravo.cz [online]. [cit. 2013-03-09]. Dostupný z WWW: <http://www.epravo.cz>.

Ostatní zdroje

Zákon č. 140/1961 Sb., trestní zákon