VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

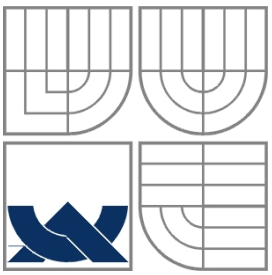
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

PROBLEMATIKA EMAILOVÉ KOMUNIKACE

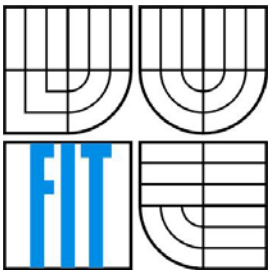
BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE KAREL TLUSŤÁK
AUTHOR

BRNO 2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

PROBLEMATIKA EMAILOVÉ KOMUNIKACE

EMAIL CUMMUNICATION EPROBLEMATICS

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR

KAREL TLUSŤÁK

VEDOUCÍ PRÁCE
SUPERVISOR

MGR. KAMIL MALINKA

BRNO 2008

Zadání:

1. Seznamte se s problematikou autentizace emailů, spamů, phishingu.
2. Nalezněte a diskutujte právní rámec a hlediska těchto problémů.
3. Implementujte nástroj na analýzu dat o phishingu, nebo kombinaci spam databáze s phishingem.

Licenční smlouva

Licenční smlouva je uložena v archívu Fakulty informačních technologií Vysokého učení technického v Brně.

Abstrakt

Tato práce popisuje aktuální problematiky emailové komunikace. Uvádí technické pozadí principů samotného vyměňování emailů a z toho vyplývající možnosti autentizace. Dále se práce zaměřuje na největší současné problémy spojené s emaily, a sice spamy a phishing. V oblasti spamů se tato práce zabývá především možnostmi filtrování a detekce těchto nevyžádaných emailů. Phishing je zde názorně ukázán pomocí provedení demonstračního phishingového útoku, dále je pozornost věnována rovněž možnostem ochrany proti takovýmto útokům. Další nosnou částí práce je popis emailové problematiky z právního pohledu. Je zde především rozebráno posuzování a postihy spamů a phishingu z pohledu české legislativy, Evropské unie a dalších zemí. Samotný phishing je, jakožto nejzávažnější trestná činnost zneužívající emailové komunikace, rozebírán na demonstračním právním procesu a precedenčních případech, které se staly nejen v zahraničí, ale i u nás. Poslední částí práce je popis a implementace jednoduchého emailového filtru využívajícího databázi serveru phishtank.com pro analýzu phishingových emailů.

Klíčová slova

phishing, email, spam, model OPT-IN, model OPT-OUT

Abstract

This work describes actual problems regarding to email communication. It shows how emails technically work and on these bases describes today's possibilities of email authentication. Next to it, the paper focuses on the biggest problems connected to emails – spamming and phishing. As far as spam is concerned, this work is dealing with methods of detection and filtering spam. Phishing is demonstratively shown on virtual case of phish-attack and attention is paid to anti-phishing tools as well. Other key-part of this work is low view of email problematic. This part covers judgement and eventual punishment of spamming and phishing in accordance to Czech, European Union and other countries' legislation. The phishing, considered to be the most serious problem concerning to emails, is demonstrated by the virtual court case which shows how related organs works and what are the problems about it. Some precedential cases are discussed there as well. The last part of this work describes the implementation of simple program which uses database in the Phishtank server to analyse phishing emails.

Keywords

phishing, email, spam, OPT-IN model, OPT-OUT model

Citace

Karel Tlusťák: Problematika emailové komunikace. Brno, 2008, bakalářská práce, FIT VUT v Brně.

Problematika emailové komunikace

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Mgr. Kamila Malinky.
Další informace mi poskytl Mgr. Jiří Mikulenka (advokát).
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Karel Tlusťák
1. 5. 2008

Poděkování

Rád bych tímto poděkoval mému vedoucímu bakalářské práce, panu Mgr. Kamilu Malinkovi, za cenné rady a připomínky. Dále bych chtěl poděkovat panu Mgr. Jiřímu Mikulenkovi, advokátovi a jeho synovi Pavlu Mikulenkovi, se kterými jsem mohl konzultovat právní otázky týkající se emailové komunikace.

Obsah

Úvod

Emailová komunikace je v dnešní době jedním z nejrozšířenějších způsobů, kterým si lidé vyměňují informace. Lze říci, že pro spoustu lidí je tento způsob komunikace nenahraditelný. Emailová komunikace je relativně snadná, rychlá a nejsou s ní spojeny prakticky žádné přímé náklady, právě díky těmto vlastnostem, rozvoji počítačové gramotnosti a internetu všeobecně se logicky emaily staly určitým standardem nejen v osobní komunikaci, ale i v obchodní sféře. Bez nadsázky se dá říci, že každý uživatel internetu má svůj email a aktivně jej využívá.

Růst této technologie je tedy zcela logickým důsledkem, nicméně právě díky tomuto aspektu by se měly dostat do popředí zcela aktuální otázky bezpečnosti a dalších problémů tohoto druhu komunikace. Budeme-li postulovat standardního uživatele internetu, pro kterého emailová komunikace představuje významný zdroj business/resource potenciálu, mohou se z jeho pohledu jevit v této komunikaci následující problémy:

- stráví zbytečně mnoho času tříděním pošty, kdy je potřeba rozdělit nevyžádanou poštu (spam) od užitečné pošty. Z vlastní zkušenosti vím, že pokud se člověk z hlediska svého podnikání potřebuje pohybovat po anglicky mluvícím internetu a přijímat anglické emaily různého typu, může mu právě toto redundantní třídění pošty zabrat až čtvrt hodiny denně.

- ve většině případů si nemůže být zcela jist autentičností emailu (pokud není email digitálně podepsán) a může se tedy stát obětí phishingu či dalších druhů podvodu

Myslím si, že uvedené problémy jsou velmi aktuální, obzvláště zmíněné zcizení identity metodou označovanou jako phishing, lze považovat jako vrchol emailové kriminality.

Statistickým pohledem tvoří spamy téměř polovinu veškeré SMTP komunikace a odhaduje se, že emaily v různých fórech nebo zveřejněné na stránkách, sklidí přes 90% spamerských skupin během jednoho roku [1]. Tento fakt je poměrně alarmující, nicméně spamy jsou již známou věcí a metody jejich eliminace jsou poměrně pokročilé. Co je však v poslední době velmi nebezpečným trendem, je tzv. phishing. Například v roce 2004 byly téměř 2 miliony občanů USA vystaveny phishingovému útoku na jejich běžné účty. Celkové ztráty, které byly takto způsobeny, dosáhly zhruba 2 miliardy dolarů, přičemž průměrná výše škody na jednom případu byla 1200 dolarů [2].

Je zcela prediktibilní, že tyto druhy internetové kriminality budou v následujícím časovém horizontu stále populárnější a je tedy důležité věnovat jim odpovídající míru pozornosti. Právě proto jsem se rozhodl zabývat se problematikou emailové komunikace.

V této bakalářské práci bych chtěl tedy představit problematiku emailů a spamů s tím, že se chci podrobně zaměřit na phishing a implementovat metodu ochrany před phishingovými emaily pomocí databáze dostupné na serveru www.phistank.com. V neposlední řadě bych chtěl tyto problémy zastřešit příslušnými právními rámci nejen v ČR ale i z právního pohledu EU a jiných zemí.

Tato bakalářská práce se tedy skládá ze čtyř částí. V první části (kapitola 1-2) jsou popsány základní principy emailové komunikace se zaměřením na možnosti ověření autentičnosti emailů. Následující část (kapitola 3 - 4) rozebírá problematiku spamů a phishingu. Jelikož o této problematice byla již napsána spousta odborných článků, snažil jsem se na otázku spamů a phishingu nahlížet spíše prakticky. Proto se u spamů věnuji především metodám obrany včetně zabezpečení samotných webových stránek proti sběru emailových adres. Phishing je v této práci popisován z pohledu samotných phisherů, demonstruji zde tedy ukázku celého průběhu phishingového útoku i s autentickými skripty. Jsou zde rovněž rozebrány současné metody obrany proti takovýmto útokům. Další nosnou částí mé bakalářské práce (kapitola 5) je popis právního pozadí emailové komunikace a souvisejících problémů. Zde jsem se zaměřil jak na českou legislativu, tak na právní normy jiných států a související směrnice Evropské unie. Poslední částí je popis vlastní implementace nástroje na rozpoznávání phishingových emailů.

1 Základy emailové komunikace

1.1 Historie

Za počátky komunikace pomocí emailů lze považovat přibližně rok 1965, kdy byla zpráva přenášena mezi sálovými počítači na univerzitě MIT pracujících v režimu sdílení času.

Od této doby prošla emailová komunikace značným vývojem. Emaily, tak jak je známe dnes, jsou definovány standardem specifikace RFC 822 a jsou přenášeny pomocí protokolu SMTP (Single Mail Transfer Protocol), který byl uveden v roce 1982 specifikací RFC 821. Jelikož jsou však tyto normy poměrně zastaralé a neodpovídají požadavkům moderního internetu (převážně z hlediska zabezpečení), byly tyto standardy revidovány do současných standardů RFC 2822 a RFC 2821.

1.2 Struktura emailu

Každý email se skládá ze 2 částí – z tzv. hlavičky (leader) a těla emailu (body), přičemž hlavička předchází tělu a tyto části jsou vzájemně odděleny prázdným řádkem (tedy znaky <CR><LF>).

1.2.1 Hlavička emailu

Hlavička emailu je generována automaticky při vytvoření emailu a jsou do ní postupně vkládány informace od serverů, přes které zpráva prochází (tzv. MTA). Pro běžné uživatele jsou z hlavičky nejdůležitější tyto údaje: předmět zprávy, čas odeslání zprávy, emailová adresa odesílatele a emailová adresa příjemce, proto většinou ostatní údaje emailový klienti (označování též jako MUA[1]) ani nezobrazují.

Emailová hlavička však obsahuje velmi důležité údaje, kterými se řídí samotné MTA servery a pomocí nichž lze dopátrat původ emailu. Tato část je tedy z našeho pohledu klíčová.

Hlavička smí obsahovat pouze tisknutelné znaky 7-bitového ASCII kódu (33-126), proto se emaily kódují do sedmi bitů (neuvažujeme-li rozšíření normy). Každá informace, kterou hlavička obsahuje, začíná na novém řádku a má syntaxi <Název>: <hodnota>, přičemž hodnota může být

[1] MUA – Mail User Agent, program, který používá uživatel na rozesílání a přijímání emailů (např. Outlook), tento program komunikuje s MTA (Mail Transfer Agent), který se stará o přenos emailů v prostředí veřejné sítě Internet.

zalomena na více řádků, kde každý takovýto řádek začíná mezerou nebo tabulátorem. Dvojici <Název>: <hodnota> označujeme jako záhlaví.

Při vytváření emailu emailovým klientem jsou většinou do hlavičky vložena tato záhlaví:

• **Date –** aktuální čas počítače, který vložil toto záhlaví

• **From** – adresa odesílatele

• **Cc** (carbon copy) – specifikuje další adresáty

• **Bcc** (blind karbon copy) – umožňuje rozesílání zprávy mezi více adresátů, přičemž je zpracován prvním MTA, kam email dorazí. Ten postupně rozesílá emaily adresátům jednotlivě a bez Bcc. Konečný adresát tedy nevidí další adresáty, pro které byl email určen.

• **Priority** – záhlaví priority emailu. Interpretace tohoto záhlaví je v různých MUA rozdílná

• **Reply-To** – specifikuje adresu, na kterou je zaslána případná odpověď

• **Subjekt** – předmět zprávy daný uživatelem

• **To** – udává adresu příjemce zprávy

• **Message-Id** – unikátní identifikátor, který je přiřazen MTA. Zpráva, jejíž Message-Id neodpovídá zápisu v doméně svého původu, je s vysokou pravděpodobností falešná.

Do emailové hlavičky přidávají záhlaví i průchozí MTA. Jedná se nejčastěji o tato záhlaví:

• **Return-Path** – toto záhlaví zpravidla zapíše cílový SMTP server. Jedná se o přepis adresy z obálky emailu (ta je poskytnuta serveru příkazem MAIL TO). Může obsahovat prázdnou adresu, jestliže se jedná o chybové hlášení ze strany serveru (například o tom, že zprávu nelze doručit)

• **Received –** jedná se o záhlaví, které je přidáváno všemi průchozími MTA. Ti jej přidávají vždy na začátek hlavičky před ostatní záhlaví Received od jiných MTA serverů, kterými email prošel dříve. Záhlaví received jsou pro účely získání reálného původu emailu zcela klíčové, jelikož díky nim lze usuzovat, kudy přesně email procházel.

Emailová hlavička může obsahovat ještě spousty dalších záhlaví. Jedná se například o celou rodinu tzv. X-záhlaví, které jsou využívány antivirovými programy a spam filtry. Tato záhlaví většinou obsahují výsledky testů atp. Prakticky v každém emailu jsou též tzv. MIME[2] záhlaví, které obsahují podpůrné informace pro správnou interpretaci samotného těla dané zprávy.

Pro naše účely je však nejzajímavější záhlaví Received. Syntaxe zápisu tohoto záhlaví je:

Received: from <doména klienta> **by** <doména serveru>
with <protokol> **id** <id zprávy>
for <příjemce> ; <časové razítko>

Díky tomuto záhlaví se můžeme dozvědět IP adresu stroje, ze kterého byl email odeslán.

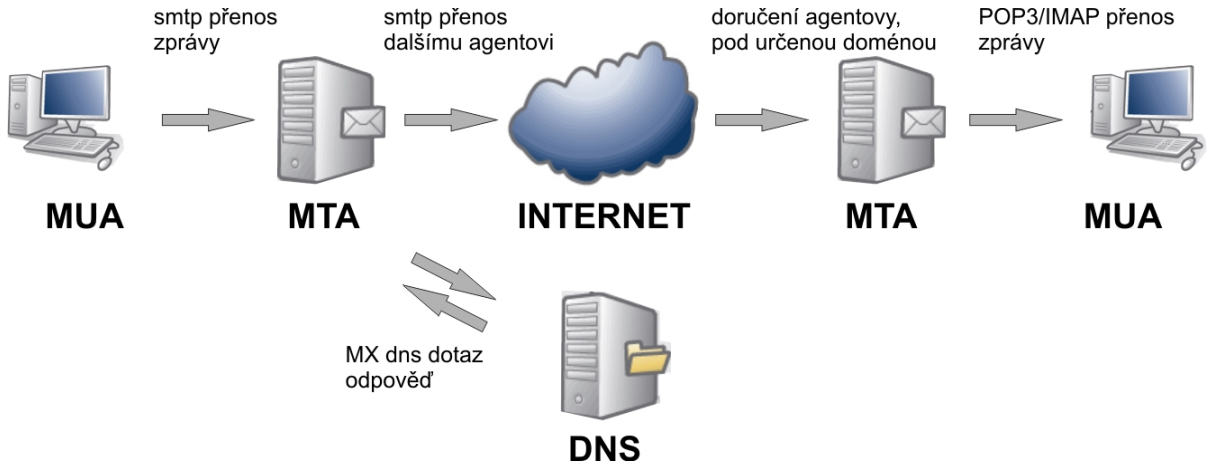
[2] MIME – Multipurpose Internet Mail Extension, jedná se o rozšíření definice dat v těle emailové zprávy, kdy je možné původní 7 bitová ASCII data interpretovat například jako 8mi bitová (to umožňuje zachování speciálních jazykových znaků či interpretaci obrázků, videí atd.). Toto rozšíření je komentováno v RFC 2045 – RFC 2048.

1.2.2 Tělo emailu

Tělo emailu obsahuje samotná data určená pro adresáta. Toto tělo má několik omezení: musí být kódováno v 7 bit ASCII kódování, délka řádku smí být maximálně 998 znaků a znaky <CR> a <LF> nesmí být v textu odděleně, ale pouze jako pár, přičemž tímto označují konec řádku. Interpretace národních znaků a všeobecně souborů v příloze je realizována pomocí výše zmíněného rozšíření MIME.

1.3 Životní cyklus emailu

Životní cyklus je znázorněn na obrázku 1-1. Emailová komunikace tedy probíhá v několika krocích. Nejdříve je daná zpráva vytvořená uživatelem pomocí MUA (např. programem Outlook), jakmile si uživatel přeje zprávu odeslat, MUA naváže spojení se známým MTA (většinou poskytovatel připojení). Zde pomocí SMTP příkazů oznámí MTA, pro koho je uvedený email určen a identifikuje se. MTA server zpravidla do hlavičky zprávy připíše své Recived záhlaví a podívá se do jaké domény je email určen. Pokud se přímo nejedná o jeho vlastní doménu, provede dotaz na MX záznam DNS serveru, kterým zjistí IP adresu MTA serveru, kterému danou zprávu odešle. Ten postupuje obdobně, dokud se zpráva nedostane na MTA server, pro nějž je určena. Na tomto serveru je zpráva uložena do té doby, než si ji adresát pomocí protokolu POP3, IMAP nebo pomocí webového rozhraní MTU vyzvedne respektive vymaže. Celý proces přenosu emailu demonstruje obrázek 2-1.



Obrázek 1-1 demonstrující životní cyklus emailu

2 Autentizace emailů

2.1 Relaying

Přenos elektronické pošty je většinou zprostředkován několika servery MTA, velké podnikové sítě mohou mít například více lokálních MTA a jeden nadřazený hlavní server (tzv. Mailgate), můžeme dále uvažovat průchod emailu přes kontrolní firewally či servery třetích stran. Při přenosu emailu tedy může docházet ke způsobu přenosu, který nazýváme *mail relaying* (občas překládáno jako předávání pošty). Jedná se o proces, kdy poštovní server obdrží zprávu, jejíž odesílatel ani příjemce nejsou lokálními uživateli, které by server znal. Znamená to, že příjemce i odesílatel jsou z jiné domény (mimo lokální rozsah IP adres), a proto by měl být server zabezpečen a poznat, jestli je daná zpráva z hlediska k němu relevantní.

Pokud však server takto zabezpečen není, lze pomocí něj poslat zprávu, u níž není ověřena identita uživatele. Ve zprávě může být tedy podvrhnut odesílatel a uvedeny nesprávné odesílací údaje v hlavičce emailu. Tyto servery se nazývají *open relay* a jsou často zneužívány právě phishery a spamery.

Takto může vypadat hlavička zfalšovaného emailu, který prošel přes open relay server:

```
Received: from relayserver.com (relayserver.com [194.114.111.12])
 by smtp.skola.cz (8.8.5) id 001C16 for <sekretariat@skola.cz>;
 Thu, Nov 12 2007 22:25:40 +0100 (CET)
From: nobody <nobody@nobody.com>
To: (seznam prijemcu potlacen)
Message-Id: <dc3148x-121107@relayserver.com>
Subject: YOU HAVE WON!!!
...
```

Všimněme si, že relayserver zcela zahodil hlavičku původního odesílatele, nelze tedy dopátrat skutečného odesílatele. Jedná se o pomyslně nejhorší případ – server je označován jako tzv. spam zombie.

Open relay servery jsou velmi nebezpečné a proto je v dnešní době snaha o jejich eliminaci. V době, kdy ještě nebyl zaznamenán takový boom internetové kriminality spojené s rozesíláním emailů, byly tyto servery běžně využívány, jelikož existovalo hodně domén bez asociovaného SMTP serveru. Nyní však existují tzv. black listy, kde jsou tyto open relay servery uvedeny a podle této databáze lze poštu odeslanou právě těmito servery filtrovat. Problémem takovýchto serverů je však

většinou špatné zabezpečení především malých firemních SMTP serverů, jejichž administrátoři ani netuší, že je jejich server snadno zneužitelný.

2.2 Metody ověřování autentičnosti emailů

Jelikož lze poměrně jednoduše podvrhnout původ emailu, je potřeba ověřovat, jestli je odesílatelem opravdu ten, za kterého se vydává. Tohoto faktu většinou využívají jak spameři, tak phisheři, kteří se tímto například mohou tvářit, že email byl odeslán bankovním institutem či podobnými organizacemi. Je tedy esenciální zajistit znemožnění takového typu podvrhu.

Pro tuto činnost existuje několik komerčních a volně dostupných přístupů. Mezi placené produkty lze zmínit např. Sender Score Certified, které je založeno na DNS whitelistu, pomocí něhož jsou emaily ověřovány. Nevýhodou je, že za zápis do tohoto whitelistu se musí platit. V této práci se však chci zaměřit na nekomerční řešení. Za nejznámější technologie autentizace emailů lze považovat SPF (respektive SenderID) a Domain Keys. Tyto metody se vyznačují minimálními změnami na straně uživatelů.

2.2.1 SPF a SenderID

SPF (Sender Policy Framework) a SenderID jsou 2 velmi podobné metody ověřování autentičnosti emailů. SenderID prakticky vychází ze SPF, jedná se pouze o upravenou verzi s drobnými odlišnostmi, kterou se snaží prosadit společnost Microsoft.

SPF je otevřeným standardem (poslední verzí je SPFv1, též označovaná jako SPF Classic). Tato technologie umožňuje správci domény publikovat svou poštovní politiku, neboli které servery v rámci své domény používají pro přenos emailové komunikace. SPF vyžaduje pro svou funkci spolupráci 2 stran: (1) správce domény musí vystavit tyto informace v tzv. SPF záznamech v DNS zónovém souboru. Jakmile jiný poštovní server příjme email, který vypovídá, že jeho původ je právě z této domény, (2) server přijímající tento email se může dotázat DNS serveru na SPF záznam týkající se dané domény a pomocí něj určit zda je IP adresa odesílatele relevantní. Znamená to tedy, že pokud server přijímá email z neznámého serveru, lze s vysokou pravděpodobností předpokládat, že tento email je falešný.

Uvažujme tento příklad, který demonstruje, jak SPF (potažmo SenderID) pracuje. Uživatel vlastní doménu example.com, nicméně příležitostně používá svůj poštovní účet na www.volny.cz, jelikož však obdržel několik upozornění na zprávy z jeho účtu, který nikdy neposlal, rozhodl se publikovat svůj SPF záznam – ten v tomto případě může vypadat takto:

```
examle.com. IN TXT "v=spfl mx a:server.example.com include
volny.cz –all"
```

Vysvětlení jednotlivých částí SPF záznamu:

- **v=spfl** - uvádí verzi SPF, v tomto případě se jedná o verzi 1
- **mx** - příchozí emailové servery dané domény jsou autorizovány také k odesílání pošty z domény example.com
- **a:server.example.com** – tento server je též autorizován
- **include:volny.cz** – cokoliv, co je v tomto kontextu považováno za legitimní pro volny.cz je považováno za legitimní též pro example.com
- **-all** - všechny ostatní poštovní servery jsou považovány za neautorizované

Koncepce SPF je velmi nadějná, klíčem je fakt, že pro jeho funkčnost stačí pouze záznam v DNS a příjemce může email odmítnout již po příkazu MAIL FROM: v rámci SMTP komunikace, k tomu mu stačí jen jeden dotaz na DNS server. Na rozdíl od technologie SPF je v SenderID ověřována shoda s PRA (Purported Responsible Address), čili adresu, která je v emailu publikována v záhlaví (určeno výběrem) Resent-Sender, Resent-From, From, Sender. Bohužel však samotná koncepce nestačí – je potřeba především aby ji podporovaly MTA přijímající emailovou korespondenci.

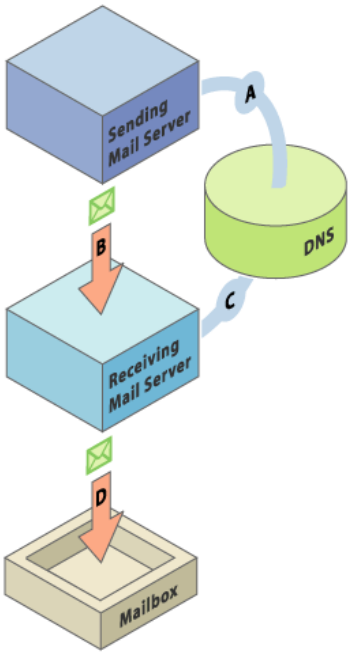
2.2.2 Domain Keys

Do určité míry lze říci, že Domain Keys je zkráceným názvem pro technologií Domain Key Identified Message. Jedná se o protokol, který vychází z původních Domain Keys navržených společností Yahoo a Internet Identified Message (vyvinuto společností Cisto). Tato technologie je poměrně rozšířená a to především díky podpoře velkých emailových serverů jako je GMail, AOL, Yahoo, atd. Podle tiskové zprávy Yahoo z roku 2005 počet přijatých emailů, které tato společnost verifikovala pomocí Domain Keys, přesahoval 300 miliónů za den.

Princip autentizace pomocí Domain Keys spočívá v tom, že je do emailové hlavičky přidáno záhlaví DomainKey-Signature, které obsahuje digitální podpis kontextu, který je v emailu obsažen. Pro samotné šifrování se používá algoritmus RSA, přičemž šifrovaný výsledek je následně převeden metodou BASE64. Proto, aby takovýto podpis mohl být vygenerován, musí daný poštovní server znát pár veřejný – soukromý klíč, platný pro uvažovanou doménu, přičemž veřejný klíč je publikován jako záznam na DNS serveru. Pro každou zprávu je tedy použit privátní klíč, kterým je vytvořeno záhlaví

DomainKey-Signature. Příchozí server rozeznává autentičnost emailu na základě DNS dotazu, kterým získá veřejný klíč pro doménu, ze které email pochází. Tímto pozná, zda byl podpis vygenerován na základě odpovídajícího soukromého klíče a může tedy odfiltrovat případné podvržené emaily. Jednotlivé kroky samotné autentifikace pomocí Domain Keys jsou znázorněny na obrázku 2-1.

Domain Keys je z hlediska boje proti zneužívání emailů velmi zajímavá a účinná technologie. Obzvláště pokud budeme uvažovat cílené podvržení adresáta a následný phishing, je tato metoda prakticky esenciálním způsobem, jak by se měly banky či jiné potenciálně napadnutelné instituce bránit. Jako určitou nevýhodu můžeme brát fakt, že signatura je pro každý odeslaný email počítána zvlášť, což může být hardwarově náročné, nicméně tato nevýhoda zůstává v pozadí oproti skutečnosti, že Domain Keys lze za určitých podmínek obejít pomocí tzv. „replay attacks“[3].



Obrázek 2-1 princip fungování systému autentifikace emailů pomocí Domain Keys

[3] Replay attack je metoda podvržení emailu, která se snaží využít faktu, že Domain Keys nekontrolují relevanci tzv. obálky emailu. Jedná se o to, že útočník pošle zprávu sám sobě, čímž vytvoří platný DomainKeys-Signature a následně tento dopis opětovně odešle, nicméně již s pozměněnou obálkou, což mu umožní tento email poslat prakticky kamkoliv.

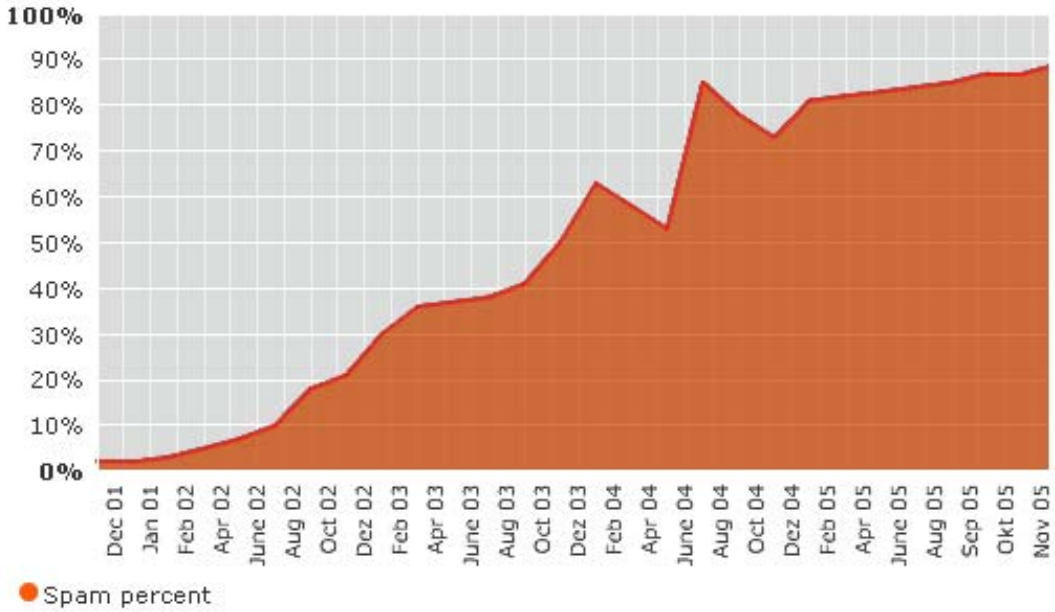
3 Spam

3.1 Definice spamu

Spam je vžitý název který nelze definovat jednoznačně, jelikož to, co jeden uživatel může požadovat za spam je pro jiného uživatele za určitých okolností cenná informace. Nicméně lze považovat za spam emailovou zprávu, která je nevyžádaná a zároveň hromadná. Z hlediska antispamové související legislativy platné nejen v rámci EU, ale i např. v USA je však podstatný fakt, že spamem je anonymní email splňující podmínky nevyžádanosti a hromadnosti. Slovem anonymní je zde myšleno podvržení adresy odesilatele či další maskování pravého původu emailu.

Za klíčovou společnou vlastnost většiny spamů lze považovat fakt, že jejich cíleným účelem je finanční zisk. Tato skutečnost je zcela pochopitelná, uvážíme-li vstupní investice do emailové kampaně. Relativní ignorace spamů z pohledu cílových adresátů je zde totiž velmi dobře vyvážena dostatečnou masivností uvažované emailové kampaně. Na internetu lze nalézt spousty firem nabízejících tzv. mail listy, které lze použít jako zdroj emailových adres. Podle jejich kvality a cílové skupiny se pochopitelně odvíjí jejich cena, nicméně je poměrně alarmující, že podle [3] lze pořídit list 500.000 emailů již za 29 dolarů.

Z výše uvedeného je zcela pochopitelné, že je stále větší obliba použití právě takovéto formy propagace, tedy emailové kampaně – spamu. Vývoj procentuálního zastoupení spamu na celkové emailové komunikaci za 4 roky znázorňuje obrázek 3-1 vycházející ze statistik [4].



Obrázek 3-1 vývoj procentuálního zastoupení spamu mezi emaily

3.2 Techniky sběru emailových adres

Jak již bylo řečeno, emailové listy jsou poměrně snadno a levně dostupné na internetu. Existují přímo programy, které mají v sobě tyto listy a navíc dokáží hromadnou poštu rozesílat hned přes několik SMTP serverů[4].

Existuje mnoho metod, pomocí kterých se spameři dostanou k emailovým adresám. Může se na k tomuto účelu dokonce použít slovník, pomocí něhož se generují pravděpodobné názvy emailů a ty se pak zkouší tzv. „hrubou silou“. Nebo lze využít přímo kontaktů v adresáři běžného poštovního klienta, zde je pochopitelně potřeba, aby uživatelův počítač dostatečně ovládl příslušný virus.

Nejúčinnější metodou sběru emailových adres je však použití programu pracujícího tak, že prohledává postupně html kód webových stránek a hledá v nich klíčová slova jako *mailto* či hledají znak zavináče. Tímto objeví veškeré emailové adresy nacházející se na daných stránkách. Jako zdroj url adres se zde používá katalogových služeb internetových vyhledávačů. Dá se tedy říci, že potenciální zdroj emailových kontaktů je téměř nevyčerpatelný.

Proti této metodě je velmi vhodné webové stránky již při vývoji kódu chránit. Jedná se o to, že webdesigner co nejvíce upraví emailovou adresu, aby ztížil takovýmto programům práci. Tradiční ochranou může být nahrazení znaku zavináče za jeho slovní popis (např. milt(zavináč)volny.cz, milt[at]volny.cz, atd). Tento popis emailu je však velmi nevýhodný pro samotné návštěvníky stránek, jelikož musí většinou ručně slovní popis zavináče přepsat do jeho znakové podoby.

Myslím si, že nejpokročilejší a uživatelsky nejvýhodnější metoda, jak zabránit sběru emailu, je pomocí pokročilé modifikace samotného html zápisu. Může se tedy jednat například o takovouto transformaci:

Původní email: *milt@volny.cz*

Zápis vhodný proti sběru adres:

```
&#105;<!--<!--n@spam--&#109;&#108;<!--&#64;;&#64;--&#62;<!--nospam--
>&#109;&#105;&#108;<!--&#64;;&#64;-->&#116;&#64;&#118;&#111;<!--
falsemail@mail.cz--> &#108;&#110;&#121;&#46;&#99;&#122;
```

Na tomto příkladu jde dobře vidět, že robot hledající emailovou adresu, by musel být poměrně pokročilý, aby bezpečně odstranil všechny vložené komentáře a vydělal z nich správný řetězec, který

[4] Jako demonstrující příklad lze považovat např. 123hiddensender (dostupný na www.123hiddensender.com). Tento program nejen že umí odesílat emaily tak aby bylo velmi obtížné vystopovat odesílatele, ale ještě navíc k němu kupující obdrží list 100 000 000 emailových adres – to vše již od 179$.

ještě musí interpretovat pomocí html kódovací tabulky. Navíc je velmi obtížné pro takovýto robot vůbec určit, od kterého místa v html kódu má spustit své parserovací algoritmy.

Pravděpodobně nejúčinnější metodou obrany proti takovýmto robotům je však použití javascriptu. Ten může vypadat například takto:

```
<SCRIPT type="text/javascript">
<!--
Antispam=('milt' + '@' + 'volny.cz')
Dokument.write('<a tref="mailto:' + antispam + '" >' +
antispam + '</a>')
//-->
</SCRIPT>
<NOSCRIPT>
     Emailová adresa nemůže být zobrazena, jelikož Váš
     prohlížeč má zakázán javascript
</NOSCRIPT>
```

Nevýhodou této metody je fakt, že někteří uživatelé mají javascript z bezpečnostních důvodů vypnutý, nicméně kombinací dvou předchozích metod lze dosáhnout velmi dobrého zabezpečení emailu proti zneužití. Všeobecně lze říci, že takto komplikovaně zapsaný email by prakticky žádný robot nesklidil, jelikož toto zabezpečení je zatím poměrně málo rozšířené a většina robotů s ním jednoduše nepočítá.

3.3 Možnosti filtrování spamů

Pro filtrování spamu se používají programy, které jsou spuštěny buď na straně serveru nebo na straně klienta. Všeobecně lze říci, že účinnější a efektivnější je antispamová ochrana implementovaná na samotném serveru. Nejenom že je díky tomu snížena zátěž spamů na lokální síti, ale poštovní server je takto schopen odmítnout zprávu již v rámci relace SMTP (lze využít speciální metody jako například greylisting a SPF). Na druhou stranu je v tomto případě koncový uživatel zcela závislý na tom, jak kvalitní zabezpečení v tomto ohledu jeho ISP poskytuje. Proto je též výhodné bránit se i při samotném procesu příjímání elektronické pošty (protokolem POP3 nebo IMAP).

Jedním z možných přístupů, jak rozlišit, zdali se jedná o spam či nikoliv, je pomocí určení autentičnosti odesílatele. Existuje spousta nástrojů a technologií, které toto provádějí, nejznámější jsou SPF a Domain Keys (viz kapitola 3.1.1 a 3.1.2). Výhodou těchto řešení je především fakt, že ve své základní verzi nejsou zpoplatněna. Existuje též několik komerčních řešení, která jsou založena na tom, že majitel emailu si zaplatí za svůj DNS záznam, vůči kterému je následně daný email ověřován (např. řešení Sender Core Certified[5]). Jiný princip využívá například firma Habeas [6], která prodává licence, které umožňují ověření na základě vloženého kusu kódu do hlavičky emailu (tzv. haiku). Nevýhodou všech těchto metod je fakt, že musí být podporovány samotným MTA a úspěšnost je tedy značně závislá na jejich rozšíření.

3.3.1 Analýza obsahu emailu

Tato metoda patří mezi jednu z nejstarších. Vychází z faktu, že spousta spamů jsou v podstatě komerční sdělení, které se snaží propagovat určitý produkt. Lze tedy vypozorovat závislost na určitých slovech (např. viagra) či slovních spojeních (např. výhodná koupě).

Na základě analýzy textu těla emailu se dá tedy určit rozsah výskytu takovýchto slov a dát jim odpovídající rozhodovací váhu. Jednou z prvních metod, jak se spameři snažili obejít tyto filtry byla modifikace takovýchto slov do jiné znakové podoby, která je však stále dobře čitelná pro člověka (např. místo VIAGRA se dá použít V|@GR@). V poslední době jsou velmi oblíbené filtry, podporující regulární výrazy. Ty jsou schopny lépe rozlišovat takto zkomolená slova; uvedený příklad by se dal vyřešit například tímto regulárním výrazem: (v(i,|)(a,@)gr(a,@)). Jedním z nejsofistikovanějších přístupů současnosti je však tzv. Bayesovský filtr. Ten vychází z principu, že slova i slovní spojení, která se vyskytovala v předchozích známých spamech se budou vyskytovat i ve spamech budoucích. Porovnává tedy jednotlivé části zprávy s databází spamů a na základě množství shod vyhodnocuje pravděpodobnost, že daný email je spam. Tato metoda většinou ignoruje běžně používaná slova (spojky, částice, atd.), nicméně se zaměřuje na slova používaná ve spamech s co největší citlivostí. Rozlišuje se zde například podezřelé použití interpunkce, velkých písmen či jiných znaků (například zápis „SLEVA!!!“ je mnohem podezřelejší než zápis „sleva“, u kterého lze předpokládat běžné použití ve větě). Bayesovský filtr se nedívá jen na samotný výskyt slov, ale porovnává i další příznaky, které by mohly být směrodatné při samotném rozhodování. Jedná se především o výskyt url, kde se dá následně prozkoumat obsah odkazované stránky, dále použití html značek v emailu, přítomnost obrázků a dalších aspektů. Pokud tyto filtry disponují dostatečnou znalostní bází, dokáží filtrovat spamy s účinností přes 95% [7].

3.3.2 Signatury a jejich porovnávání

Filtry založené na metodě porovnávání signatur využívají kontrolní součty těl emailů (signatury), které následně porovnávají s distribuovanou databází těchto součtů. Tyto filtry vycházejí z filosofie, že spamy jsou rozesílány hromadně a tudíž množství emailů se stejnou signaturou bude velké.

Jestliže tedy zpráva byla zaznamenána dostatečným počtem serverů, lze říci, že se s vysokou pravděpodobností jedná o spam. Problém této metody spočívá v tom, že spamy mohou být generovány tak, aby měly alespoň částečně dynamický obsah. Některé filtry tuto skutečnost řeší tak, že zprávu rozdělí na několik částí a u těch jednotlivě počítají signatury. Nejznámější implementace tohoto filtru jsou Virpul's Razor a Distributed Checksum Clearinghouse (DCC). Obě řešení jsou do značné míry podobná, nicméně se liší v přístupu k legitimním hromadným zprávám (například emailové konference). Jelikož je metoda porovnávání signatur založena na tom, že porovnává množství výskytu emailů, může se velmi snadno stát, že takto vyfiltruje právě emailové konference či další hromadně rozeslané emaily, které však nejsou spamem. Virpul's Razor tento problém řeší pomocí mechanismu, kdy tzv. autorizovaní přispěvovatelé mohou odeslat informaci, že daná zpráva není spam. Jiný mechanismus používá DCC, který rozeznává legitimní poštu na základě whitelistu. Největší nevýhoda těchto metod je však jisté zpoždění, které vzniká tím, že spam musí obdržet a nahlásit spousta serverů, než jej lze takto filtrovat. Používá se tedy spousta nastražených adres (honeypotů), které se snaží zmírnit náskok spamerů.

3.3.3 Black list

Black list je v podstatě distribuovaná databáze, která obsahuje zdroje (IP adresy, DNS záznamy), ze kterých již alespoň jednou prokazatelně pocházel spam. Black listů je v síti internet mnoho – ať už komerčních či veřejně přístupných.

Dají se rozlišit 2 typy blacklistů. Buď je na základě blacklistu porovnávána shoda IP adresy odesílatele uvedené v hlavičce Received, nebo blacklist uchovává záznamy o doménových jménech či IP adresách, na které jsou v těle emailu uvedeny url odkazy. Největším problémem blacklistů, který byl velmi závažný obzvláště v minulosti, je vysoký počet tzv. false-positive detekcí. Tehdy se mnoho i velmi významných serverů dostalo nechtěně do blacklistů (např. podle serveru lupa.cz to určitou dobu byl i www.seznam.cz [8]). V takovýchto případech, kdy se do blacklistu dostane adresa nechtěně, může její majitel po odstranění své bezpečnostní díry požádat o vymazání svého záznamu v blacklistu. Ten si však většinou nechává nějaký čas, po který sleduje, jestli neobdrží zprávy o dalších spamech z této adresy. Jelikož se občas vyskytují útoky typu DoS proti provozovatelům blacklistů a

vzhledem k zrychlení odezvy na dotazy směřující na tyto servery, je celosvětovou snahou vytvořit síť takovýchto DNS serverů. Následující obrázek 3-2 zobrazuje geografické rozložení serverů, které si mezi sebou vzájemně zrcadlí (tzv. mirror-servery) blacklist provozovaný organizací Spamhaus [9].

Obrázek 3-2 geografické rozložení blacklist serverů spamhaus.org

3.3.4 White list

Whitelist je v podstatě také databáze emailů či doménových jmen. V porovnání s blacklistem se většinou nejedná o velkou distribuovanou databázi, ale spíše o lokální seznam emailů, které nemají být filtrovány, jelikož jsou to známé emaily, se kterými se již pravidelně komunikuje, nebo jsou dostatečně věrohodné.

Tímto lze například zabezpečit bezproblémový chod emailových konferencí. Další výhodou může být fakt, že na takto označené emaily již není potřeba provádět sérii antispamových testů. Zajímavým přístupem k provozu whitelistu je řešení označované jako Chalenge-Response. To vychází z faktu, že spamy jsou odesílány strojově a není tedy možné, aby byly dodatečně potvrzeny. Využívá se zde například interakce s odesílatelem, kterému je poslán zpět email s odkazem na webovou stránku, kde musí do formuláře vypsat vygenerovaný kód (tuto metodu používá například produkt Merak Mail Server). Nevýhodou tohoto systému však je, že jsou takto odfiltrovány automaticky vygenerované emaily, které jsou však pro uživatele důležité (například faktury z e-shopů či informace o účtech).

3.3.5 Greylisting

Greylisting je technologie používaná na MTA, která využívá možnosti tzv. dočasného odmítnutí definovaného protokolem SMTP (chyba s kódem 450-459). Toto odmítnutí se v rámci snížení zátěže provádí pouze u odesílatelů, kteří se nenacházejí v lokálním whitelistu. Jestliže je emailová adresa legitimní, server, z něhož byl email odeslán, jej s vysokou pravděpodobností odešle znovu. MTA se odesílajícímu serveru jeví, jako by byl příliš zaneprázdněn a v danou dobu email nemohl přijmout, jakmile však uplyne určitý čas, email přijme.

MTA vybavený greylistingem většinou obsahuje tyto trojice záznamů o každé emailové adrese, se kterou se setkal:

- IP adresu odesílatele (respektive MTA, který se pokouší zprávu odeslat)
- Emailovou adresu odesílatele, který je zaznamenán v SMTP obálce
- Emailovou adresu příjemce z SMTP obálky

Každý přicházející email je porovnáván s těmito záznamy. Pokud zde není, je zaslána chyba o dočasném odmítnutí, nicméně pokud po stanoveném čase server opět odesílá uvažovanou zprávu, dostane se i on do tohoto whitelistu (expirační doba takovéhoto záznamu je většinou několik desítek dnů). Tyto záznamy obsahují doménová jména (emailovou adresu) z toho důvodu, že mnoho společností používá pro odesílání emailů hned několik serverů, které se podle zátěže mohou střídat.

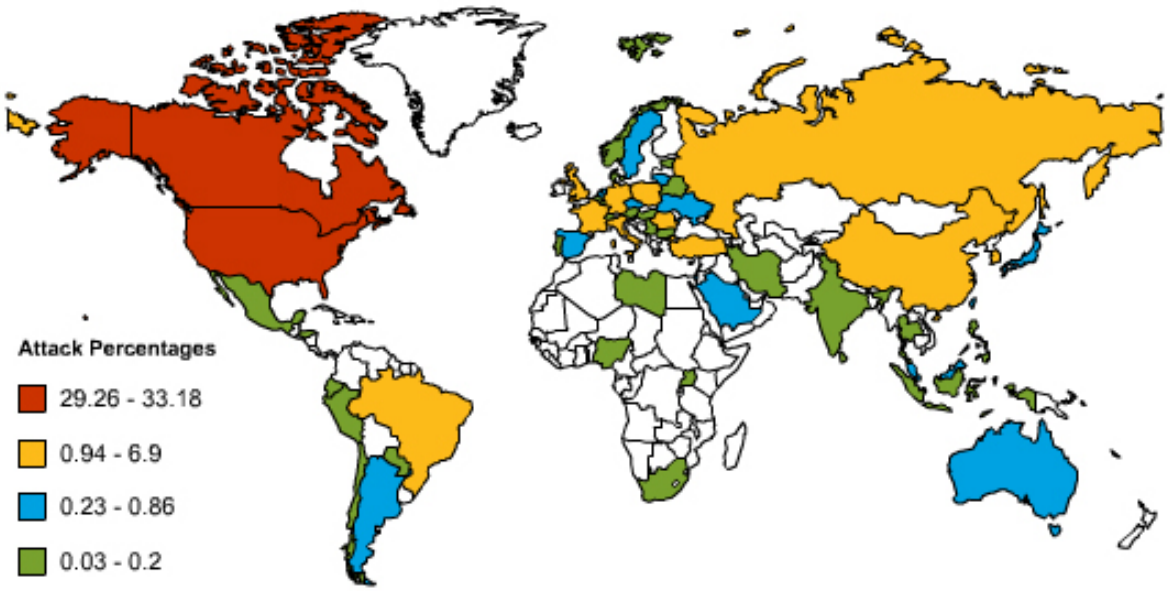
Tato metoda je poměrně účinná obzvláště v kombinaci s blacklisty, jelikož se tímto spam pozdrží a pokud byl odeslán dostatečnému počtu uživatelů, může se během této doby dostat do blacklistu a být pak úspěšně vyfiltrován. Na druhou stranu ještě stále bohužel existuje spousta MTA které nemusí striktně dodržovat všechna doporučení RFC a nemusí mít chybu s kódem 450-459 dostatečně ošetřenou. Všeobecně lze říci, že tato metoda je vhodný doplněk dalších metod, na který by se mělo vždy myslet při plánování antispamové politiky.

4 Phishing

4.1 Úvod do problematiky phishingu

Phishing, známý též jako carding či brand spoofing má mnoho podob a definic. Podstatou phishingu je oklamání uživatele podvrženým emailem za účelem získání osobních údajů.

První zaznamenaný phishingový útok byl proveden v roce 1995 na America Online (AOL). Phisheři zde napodobovali administrátora AOL, přičemž sdělovali uživatelům, že se vyskytnul problém s jejich vyúčtováním a vyžadovali, aby uživatel obnovil údaje o platební kartě a o svém účtu. Tehdy byl tento útok velmi úspěšný, jelikož spojení domácího počítače a internetu bylo relativní novinkou a lidé těmto emailům neměli důvod nevěřit. Tehdy však phishing nezasahoval takovou část populace jako je tomu dnes. Do současnosti bylo podle serveru phishtank.com [10] a podle firmy Millersmiles [11] zjištěno okolo 370 000 phishingových stránek, které byly použity k phishingovým útokům. Počet takovýchto útoků roste a dostává nové podoby. Nejčastěji napadené společnosti jsou americké banky, nicméně phishing se dostává již i do méně rozvinutých zemí. Geografické rozložení phishingu znázorňuje mapa na obrázku 4-1, která čerpá z údajů APWG [12].



Obrázek 4-1 geografické rozložení phishingu

4.2 Demonstrativní ukázka phishingového útoku

V této části bude ukázán jednoduchý postup, kterým phisher může realizovat svůj útok. Snahou tohoto textu je předvést životní cyklus takovéhoto útoku v jednoduché a názorné podobě metodou falešné identity. Pochopitelně, že v dnešní době jsou phishingové útoky značně sofistikovanější, nicméně se stále najdou phisheři, kteří uloví důvěřivé uživatele i poměrně malou modifikací této metody.

Jako cílová stránka bude použita pomyslná banka The First Bank of Phishing veřejně dostupná na adrese http://bank.securescience.net/bank[5] - viz obrázek 4-2.

Obrázek 4-2 stránka pomyslné banky určená pro demonstrativní phishingový útok

Metoda falešné identity začíná obvykle zrcadlením cílové stránky. Pro tyto účely lze použít např. volně dostupný linuxový nástroj wget. Odzrcadlenou stránku je třeba uložit na server a dostatečně pozměnit pro účely podvodného získání dat. Phisheři většinou propojí obrázky, CGI a HTML odkazy s původní stránkou. Jediný nepropojený odkaz v tomto případě povede na skript zpracovávající samotné přihlašovací údaje (Login.cgi). Tento soubor provede 2 akce: zaznamená přihlašovací údaje tím, že je odešle do naší anonymní schránky a dále odešle MIMT POST s uživatelskými údaji na původní originální stránku a přihlásí se místo něj. Tato technika byla použita

[5] Tato stránka je součástí projektu pro ukázku schopností antiphishingových nástrojů, pro znázornění phishingového útoku je však zcela dostačující.

například u případu, kdy se phiseři zaměřili na platební systém PayPal, nezkušený uživatel nepozná, že se vůbec něco stalo. Samotný kód takového skriptu může vypadat takto:

```
#!/bin/sh

PATH=/bin:/usr/bin:/usr/local/bin
URI=‘echo “${REQUEST_URI}“ | sed –e ‘s@.*/cgi/@/cgi/@‘ ‘

echo “Status: 301 Page moved
Content-Type: text/html
Location: http://bank.securescience.net/bank ${URI}
<html>
<body>
Stránka přesunuta na adresu:
<a href=\“ http://bank.securescience.net/bank
${URI}\“>http://bank.securescience.net/bank  ${URI}
</a>
</body>
</html>“
ZISKANADATA=‘echo “${URI}“ | sed –e ‘s/\/cgi\/Login.cgi?//‘‘
cat <<! | /usr/lib/sendmail –t
From: ziskanadata@phishing.cz
To: milt@volny.cz
${ZISKANADATA}
!
```

Tento kód je modifikovanou verzí skutečného kódu dostupného v knize 1 na straně 52 - 53.

Uvedený skript vezme URI z REQUEST_URI a z něj odmaže vše až k /cgi/ (v tomto příkladu se předpokládá, že /cgi/ je v URI obsaženo). V uvažované demonstrační bance vypadá URI například takto:

```
http://bank.securescience.net/bank/cgi/Login.cgi?username=kare
l&password=aaa&x=19&y=14
```

Takto jsou získány přihlašovací údaje zákazníka, které jsou pomocí aplikace sendmail odeslány na phisherův email. Tento email si většinou phisher založí u společnosti, která provozuje emaily zdarma a využívá jej jen po dobu nezbytně nutnou k získání kontaktů (většinou jen několik dnů).

Samozřejmě phisher může získané údaje ukládat přímo na server, na kterém běží daný skript, možností samotného odchycení a zpracování přihlašovacích údajů je mnoho. Na přesměrování podvedeného zákazníka používá tento skript návratového kódu 301 http protokolu. Popsaný postup je poměrně jednoduchý, nicméně se jedná pouze o demonstraci phishingových postupů a navíc je třeba si uvědomit, že phisheři mají svůj vlastní účet v bankovním ústavu, který chtějí napadnout a ví tedy přesně, co se děje před přihlášením uživatele i po něm. Díky tomuto mohou provést účinné přesměrování na originální stránky a vědí, na co se zaměřit při sběru dat.

Dalším esenciálním krokem, který phisher musí provést, je vytvoření samotného emailu pro rozesílání klientům banky. V této fázi většinou phisher spolupracuje s odborníky na psychologii, kteří pečlivě volí každé použité slovo s cílem, aby email vypadal co nejvěrohodněji. Dalším problémem je, jak email odeslat, aby phishera pokud možno nebylo možné vystopovat. V rámci tohoto příkladu bude použita poměrně nenáročná metoda, která je však velmi efektivní a byla použita v praxi rumunskými phishery. Jedná se o PHP skript, který zneužívá šířku pásma zneužitého serveru. Při použití této metody se předpokládá, že phisher buď vnikl na cizí server, nebo si server pro tyto účely zakoupil pomocí kradené platební karty (tu mohl získat například z předchozí phishingové výpravy). Zde je ukázka skutečného kódu použitého phisherem, který se snažil napadnout platební portál paypal.com. (tento kód phisher umístil na předem nastražený server v rámci projektu German Honeynet Project)[6].

```
<?php
  include("ini.inc");
  $mail_header = "From: support@Bank.com<support@Bank.com>\n";
  $mail_header .= "Content-Type: text/html\n";
  $subject="Zlepšení bezpečnosti Vašeho účtu";
  $body=loadini("seznamemailu.txt");
  if (!($fp = fopen("seznamemailu.txt", "r")))
       exit("nelze otevřít soubor s meily.");
  $i=0;
  print "Cas zacatku "; print date("Y:m:d H:i"); print "\n";
  while (!feof($fp)) {
       fscanf($fp, "%s", $name);
       $i++;
       mail($name, $subject, $body, $mail_header);
```

[6] Cílem tohoto projektu je dopadnout phishera ještě dříve, než se mu podaří uskutečnit jeho podvodný záměr. Principem je, že jsou provozovány a pečlivě monitorovány servery, které mají záměrně velmi špatné zabezpečení a umožňují odesílat neautorizovanou poštu (open relay). Těmto serverům se říká honeypoty a jsou často vyhledávány phishery. V rámci Honeynet Project bylo nastaženo několik takovýchto serverů s cílem nalákat phishery, aby takto monitorovaný server použili ke svým podvodným účelům.

```
}
print "Konečný cas "; print date("Y:m:d H:i"); print "\n";
print "$i"; print "emails sent."; print"\n";
?>
```

Tento kód je modifikovanou verzí skutečného kódu dostupného v rámci projektu Honeynet [13].

Po samotném odeslání emailů již jen phisher vyčkává několik dnů a postupně sbírá osobní údaje důvěřivých klientů. V rámci zahlazení stop pak obvykle phisher své stránky stáhne a případně zruší dočasně vytvořenou poštovní schránku. Nyní již má databázi přístupových údajů nebo čísla karet většinou nic netušících uživatelů a musí je využít ještě dříve, než uživatelé zjistí, že byli podvedeni a zablokují své účty. Phisher v tomto případě většinou ukradené údaje spíše prodá zločinecké organizované společnosti, která si jej pro tyto účely najala. Tyto společnosti jsou v dnešní době již tak vybavené, že jsou si dokonce schopny na základě čísel karet a jejich bezpečnostních symbolů a čísla pin vyrobit karty vlastní, které jsou zcela použitelné.

Pochopitelně, že výše ukázaný útok je příliš jednoduchý a nebylo by možné jej použít na dobře zabezpečené banky, nicméně podobných metod phisheři stále používají a lze vidět, že provést takový útok nestojí moc úsilí a z úhlu pohledu phishera se jedná o velmi rychle vydělané peníze.

4.3 Metody obrany

Existuje řada nástrojů, které se snaží zamezit působení phishingu. Ať už se jedná o samotné blokování phishingových emailů, tak odchytávání phisherů pomocí nastražených falešných emailových stránek či honeypotů. Většina z těchto nástrojů jsou poměrně drahé komerční aplikace, neboť se předpokládá, že zákazníkem je banka či ISP, nikoliv běžný uživatel.

Za jeden z nejúčinnějších antiphishingových řešení je považován nástroj od společnosti Symantec. Ten totiž využívá své zkušební sítě Brightmail, která obsahuje návnady v podobě emailových účtů. Jelikož phisher odesílá své phishingové emaily většinou poměrně hromadně, je zde slušná pravděpodobnost, že se jeho email dostane do laboratoří Symantec, kde je intenzivně prozkoumán a v případě potvrzení jeho škodlivosti je okamžitě vytvořen filtr, který se následně odešle samotným abonentům. Symantec rozesílá poskytovatelům internetu tyto aktualizace filtrů každé 4 minuty. Tyto filtry jsou pak schopny označit či zachytit podvodné emaily. Jakmile je takto

detekován útok, Symantec odešle svým zákazníkům z řad finančních institucí informaci o tomto útoku, která mimo jiné obsahuje i IP adresy útočníka.

Poměrně oblíbená technologie obrany proti phishingu je varování zákazníka v momentě, když vstoupí na podvržené webové stránky. Tuto metodu využívají např. firmy Billeo, Whole Security, Webroot, Netcraft, Earthlink a Phish Free. Podstatou této ochrany je většinou plug-in pro webový prohlížeč, který se snaží analyzovat navštěvované stránky a pokud je tato stránka vyhodnocena jako podezřelá, uživatel je patřičně varován (například obrázkem semaforu, který mění barvu). Tyto nástroje většinou fungují na principu porovnávání url se seznamem známých phishingových stránek. Některé z nich jsou však sofistikovanější - např. produkt firmy Whole Security (tuto firmu nyní koupil Symantec). Ten prozkoumává i obsah, text, rozvržení stránky atd. Na základě váženého průměru z dosažených výsledků pak rozhoduje, jestli je stránka pravá, nebo se jedná o phish.

Existují firmy, které se na otázku bezpečnosti dívají z co nejkomplexnějšího pohledu. Nejznámější je v tomto ohledu pravděpodobně RSA Security, který pomáhá firmám v přípravě na phishingové útoky, aby na ně uměly reagovat a případně se z nich zotavit. RSA Security disponuje hned několika nástroji a týmem odborníků, kteří se snaží sondovat sítě a analyzovat veškeré podezřelé aktivity, které by mohly poškodit jejich klienty. V případě odhalení phishingového útoku RSA ihned odhaduje jeho rozsah a ve spolupráci s ISP a orgány činnými v trestním řízení zablokuje danou stránku. Dále tato firma nabízí pomoc při vyšetřování a snaží se trestním orgánům poskytnout co nejvíce informací potřebných k soudnímu procesu.

Dalším zajímavým řešením, je produkt firmy Cyveillance. Ten nepřetržitě monitoruje registry domén za účelem rozpoznání neoprávněného použití jejich jmen. Nejenom, že tímto chrání identitu značky svých zákazníků, ale navíc se snaží zachytit a analyzovat co nejvíce spamů s cílem objevit snahy o zcizení osobních údajů. Jakmile Cyveillance objeví falešnou aktivní stránku, kontaktuje ihned trestní orgány, aby tato stránka mohla být zrušena.

Secure Science je též velmi významnou organizací, která vyvíjí řešení proti phishingu. Její filosofie je však poněkud odlišná. Snaží se totiž phishingu předcházet, nikoliv jej analyzovat a blokovat až v momentě, kdy je samotný phishingový útok zahájen. Tato firma nabízí softwarový balíček Daylight Fraud Prevention (DFP), který obsahuje spousty funkcí chráněných průmyslovými patenty, které jsou schopny detekovat a případně blokovat nepovolené přístupy k některým internetovým službám, které jsou specifické pro phishing. DFD se integruje do webových aplikací a serverů, přičemž používá notifikační službu kompatibilní se standardy SNMP, SOAP API a POSIX. Tato technologie je schopná odhalit použití podezřelého množství proxy serverů (proxy chaining), pokusy o zrcadlení stránky, mění systém přihlašování, který v zásadě omezuje použití keyloggerů, dokáže odhalit útoky přesměrování (tzv. man-in-the-middle), monitoruje použití obrázků stažených z originální stránky, atd.

5 Právní rámce emailové komunikace

5.1 Zákony v ČR a související směrnice EU

Emailová komunikace je ve většině států EU uznaným způsobem oficiálního předávání informací mezi fyzickými či právními osobami. Znamená to, že email je právně relevantní například jako důkaz u soudního líčení, v některých zemích může sloužit jako plnohodnotný prostředek pro komunikaci s úřady a dokonce lze digitálně podepsané emaily použít jako výraz bezesporné vůle vzhledem k právnímu úkonu (například podpis smlouvy)[7].

Tato rovina se blíží myšlence, kdy email je rovnocenným ekvivalentem klasického dopisu. Z hlediska práva se však jedná o zcela nový aspekt, jehož právní vývoj není moc dlouhý a ještě zdaleka není ustálen. Je třeba si uvědomit, že vývoj nejenom práva v chápaní legislativy, ale i rozlišení spravedlnosti je dlouhodobá záležitost mnoha generací lidí, kdy se nějaká nová věc ukotví v jejich myšlení a morálce. Vzhledem k tomu, že emailová komunikace je poměrně novou a vyvíjející se sférou, ve které se objevují stále nové možnosti zneužití a prokazatelnost je poměrně obtížná, je i legislativa v tomto ohledu ještě poměrně neucelená.

Jedná se především o to, že působnost emailu může být mezistátní záležitostí, kdy email byl poslán ze serveru země s odlišnou legislativou, než má stát příjemce. Vzniká pak poměrně dlouhý proces arbitráží, přičemž tato prodleva často způsobí pozdější nedopátratelnost případného pachatele. Na tento fakt často spoléhají phisheři, kteří využívají servery v zemích s nízkou právní kulturou. Tato problematika je velmi úzce spjata s mezinárodním právem, které bude probráno níže na modelovém případě.

Nejrozšířenějším trestným činem způsobeným zneužitím emailové komunikace, je rozesílání nevyžádaných obchodních sdělení (spamu), zde existují 2 rozdílné přístupy: OPT-IN (přijato jako vzorový právní model pro země EU) a OPT-OUT (zakotveno především v zákonech USA). Dále bude v této práci rozebráno právní pozadí nejzávažnějšího trestného činu, který postihuje emailovou komunikaci – phishingu.

[7] Elektronicky podepsané emaily jsou již zaběhlé například v celní sféře, kdy je potřeba efektivně vyměňovat ověřené dokumenty v rámci několika států. Tato skutečnost je u nás ošetřena těmito zákony: zákona o elektronickém podpisu (č. 227/2000 Sb.), celní zákon (č. 13/1993 Sb.) a správní řád (č. 500/2004 Sb.).

5.2 Emailová kriminalita z pohledu mezinárodního práva soukromého a veřejného

Jelikož se většina emailů, které svou formou poškodí jinou osobu či dokonce naplňují skutkovou podstatu trestného činu, zpravidla odehrává v rámci více než jednoho státu, je velmi problematická kvalifikace takovéhoto soukromoprávního deliktu či trestného činu.

Jako demonstrující příklad můžeme uvažovat phishera, který je občanem České republiky, nechal se však najmout ruskou phisherskou společností a ze serveru v Rumunsku odeslal klientům americké banky emaily, které způsobily finanční škodu jak samotné bance, tak několika jejím klientům, kteří jsou občany různých zemí světa. Je zcela zjevné, že phisher se dopustil trestného činu, nicméně je velmi obtížným úkolem rozhodnout, podle které legislativy bude tato skutečnost posuzována, který orgán bude činný v rozhodčím a dále trestním řízení.

Nejprve je třeba rozlišit, do které právní kategorie tento případ spadá a především, podle legislativy které země bude posuzován. Pro toto určení se rozlišuje tzv. mezinárodní právo soukromé a veřejné. Jestliže se jedná o trestný čin, čili porušení zákona, který chrání všeobecný veřejný zájem, žalobcem je stát a rozhodné právo se určí zpravidla pomocí mezinárodních smluv spadajících do mezinárodního práva veřejného. Příkladem takového jednání může být například rozesílání spamů, jelikož je ve veřejném zájmu, aby byl viník potrestán. Podle mezinárodního práva soukromého se naopak posuzuje rozhodné právo v tzv. právních deliktech, kdy jedna strana svým jednáním poškodí stranu jinou (např. tím, že poškozené straně ukradne cenná data).

Uvedený příklad by pravděpodobně postupoval podle následujícího scénáře:

- banka by na základě stížností svých klientů zjistila, že phisher rozeslal email jejím jménem, podala by tedy okamžitě trestní oznámení na neznámého pachatele. Jelikož se odeslané emaily snaží podvrhnout jejich původ, jsou dle legislativy USA považovány za spam.
- Případem by se začala zabývat FBI.
- Předpokládejme, že by se našlo několik klientů banky, kteří by důvěřivě „předali“ phisherovi své přihlašovací údaje. V tomto momentě se phisher dopustil dalšího trestného činu – krádeže identity.
- FBI by zjistila, že IP adresa serveru, na které běžely falešné stránky dané banky, patří rumunskému ISP. Musí tedy požádat o spolupráci rumunskou policii. Ta s americkou policií bude spolupracovat na základě úmluv spadajících do mezinárodního práva veřejného. Nyní záleží do značné míry na právem zaručených pravomocích rumunské policie, jestli bude

možné nashromáždit dostatečné množství digitálních stop (některé legislativy komplikují přístup k takovýmto informacím v zájmu ochrany osobních údajů).

- Předpokládejme, že se podaří zjistit, že server provozoval český občan. Do hry vstupuje Interpol[8], kterému se dejme tomu podaří tohoto phisera zadržet v České republice.
- Nyní je třeba určit, podle které legislativy bude případ posuzován. K tomuto se v mezinárodním právu soukromém používají často tzv. kolizní normy, jedná se o soupis pravidel, která provádí výběr rozhodného práva na základě okruhu právních otázek, na něž se kolizní norma vztahuje. Rozlišuje se zde určení podle právního řádu (lex cause), podle státní příslušnosti (domicil), podle sídla soudu / úřadu vedoucího řízení (lex fori). V tomto sporu by pravděpodobně záleželo na českých úřadech, jestli by vydaly svého občana (phishera) americké straně – v takovém případě by byl případ projednáván u soudu příslušejícímu obvodu, kde sídlí daná americká banka. Podle mezinárodních smluv zakotvených v českém mezinárodním právu veřejném by v případě nevydání musel být phisher souzen ze stejných obvinění naší jurisdikcí. To by pro něj bylo pravděpodobně výhodnější, nicméně záleží na konkrétních detailech celého případu.
- Banka by též phishera žalovala za poškození jejího dobrého jména, jelikož podle současného zákona musí všem svým klientům oznámit, že došlo k porušení bezpečnosti jejich účtů.
- Nejproblematičtější částí celého phishingového útoku je samotné přečerpání peněz ze získaných účtů. O toto by se již starala organizace, která si phishera najala. Využila by k tomu tzv. jezdce na mule, který by se snažil získat co nejvíce důvěřivých lidí (bílých koní). Přes tyto lidi (např. využitím jejich osobních kont) by postupně „proprala“ co nejvíce peněz z podvodně získaných účtů.
- Právní postih těchto lidí je zpravidla problematický, jelikož o trestném pozadí jejich činu většinou vůbec neví a jezdci si své muly vybírají zpravidla z méně vyspělých států, aby ztížili průběh samotného vyšetřování.
- Dalším problémem je uznání a výkon cizích rozhodnutí. Jedná se o to, že i když bude v některém státě phisher odsouzen, záleží jen na státě, jehož je phisher občanem, jestli toto rozhodnutí uzná a kde bude probíhat samotný výkon trestu. Tento proces může být poměrně komplikovaný, jestliže má phisher více občanství.

Z uvedeného případu je jasné, že je potřeba, aby proběhlo mnoho procedur nutných k dopadení a potrestání phishera. Tohoto jsou si organizované gangy velmi dobře vědomi. Spoléhají buď na to, že orgány činné v trestním řízení nebudou schopny dostatečně koordinovat svoji činnost a phisheři za

[8] Interpol, v anglickém překladu International Criminal Police Organization, je organizací sdružující 184 demokratických i nedemokratických států. Účelem této organizace je spolupráce policií při pronásledování a zatýkání pachatelů trestných činů. Opírá se především o systém ASF (Automated Search Facility), pomocí kterého může ústředna libovolného členského státu využít informace z mezinárodních databází.

sebou stihnou „zamést“ stopy nebo, že případ bude díky mezinárodním průtahům trvat dostatečně dlouhou dobu k tomu, aby došlo k jeho promlčení.

5.3 Model OPT-IN

Název OPT-IN by šel přeložit jako „zvolit si vejít dovnitř“. Toto je v podstatě i základní myšlenka tohoto právního systému.

Uživatel může dostat obchodní sdělení pouze tehdy, jestliže předtím jakoukoliv prokazatelnou formou udělil odesílateli své předchozí svolení. Pokud se takto nestalo, odesílatel se dopouští trestného činu. Toto svolení lze kdykoliv odepřít vyjádřením vůle nesouhlasu (například odpovědí na přijatý email). Správně by tedy mělo být vždy možné na přijatý email odpovědět, právní postižitelnost tohoto aspektu však není normovaná v rámci EU a kolísá stát od státu.

Většina států EU včetně České republiky tedy vychází z těchto směrnic:

- „*Directive on the protection of personal data*“ 1995/46/EC – tato direktiva upravuje způsob a nakládání s osobními daty. Zároveň zaručuje ochranu citlivých dat před zneužitím a stanovuje povinnost případných držitelů tato data chránit. Za osobní data se rovněž považuje veškerá osobní emailová komunikace.
- *„Directive on electronic commerce“* 2000/31/ES – v této směrnici jsou ošetřovány nejrůznější situace a celková koncepce elektronického obchodování.
- *„Directive on privacy and electronic communications“* 2002/58/ES – známá též jako E-Privacy. Zavádí model opt-in pro spamy, upravuje možnosti zneužití cookies či případné úniky osobních dat.

Tyto direktivy byly v roce 2004 přijaty jako základ pro obdobnou legislativu v ČR vydáním zákona o některých službách informační společnosti č. 480/2004 Sb. Dozorem nad dodržováním tohoto zákona je pověřen Úřad pro ochranu osobních údajů. Z velké části je klíčovou prací tohoto úřadu kontrola a případný postih veřejných obchodních sdělení (spamu).

V praxi to znamená, že firma, která se chce prezentovat pomocí emailové kampaně, musí mít souhlas všech klientů, kteří mají být adresáty těchto emailů. K tomuto stačí například, aby uživatel zaškrtnul (nebo nechal zaškrtnuté) políčko například s nápisem ve smyslu „chci na svůj email dostávat podrobnosti o nových produktech“. Samotná společnost pak musí kdykoliv být schopná tento fakt prokázat (například seznamem souhlasících zákazníků s jejich identifikací, IP adresou a přesným časem zápisu). Tento souhlas je zapotřebí, i kdyby byl uživatel stávajícím zákazníkem uvažované společnosti. V tomto ohledu je naše legislativa vzhledem k evropskému vzoru přísnější, neboť stálý klient určité společnosti může v jiných zemích EU obdržet jejich obchodní sdělení, nicméně pokud se jakýmkoliv způsobem vyjádří, že již o tato sdělení nemá zájem, nemůže být nadále

příjemcem takovýchto emailů. Naproti tomu se však naše protispamová legislativa vztahuje jen a pouze na obchodní sdělení. Zde je třeba zdůraznit, že přesně definovat pojem „obchodní sdělení“ je samo o sobě velmi obtížný úkol a bohužel je právě toto „kamenem úrazu“ našeho právního systému. V praxi se toto snaží marketingové firmy obejít informačním (nikoliv obchodním) účelem rozesílaného emailu. V tomto případě musí o povaze případného emailu rozhodnout správní řízení či soudní líčení.

Definice možností šíření obchodních sdělení jsou součástí zákona o některých službách informační společnosti (§7 zákon č. 480/2004 Sb.). Mimo nutnost předchozího souhlasu případného adresáta zákon též zakazuje šíření obchodního sdělení pokud:

a) toto není zřetelně a jasně označeno jako obchodní sdělení,

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

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

Nejvyšší pokutu může za spaming dostat jen právnická osoba, a to za předpokladu, že pro účely šíření obchodních sdělení zaslala elektronickou poštu, která uvádí neplatnou adresu, na niž by adresát mohl odeslat žádost o ukončení takové komunikace. V takovémto případě se uloží finanční pokuta do výše 10.000.000 Kč.

Problém spamingu je částečně řešen i dalším právním pohledem na problematiku nevyžádané pošty jako potenciální reklamy. V tomto případě lze na případný delikt nahlížet zákonem o regulaci reklamy č. 138/2002 Sb. Výhodou takovéhoto právního pohledu je snazší a účinnější kontrola spamů, tento zákon totiž přímo zakazuje mimo jiné tyto druhy reklamy:

- reklama skrytá. Takovou reklamou se pro účely tohoto zákona rozumí reklama, u níž je obtížné rozlišit, že se jedná o reklamu, zejména proto, že není jako reklama označena
- šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje.

Další výhodou je, že orgánem dozoru nad výkonem tohoto zákona je Okresní živnostenský úřad[9]. Je zde tedy díky regionálnosti a účinnější komunikaci větší šance, že bude případná stížnost na nevyžádanou poštu účinná. Tyto přestupky jsou řešeny v rámci správního řízení, přičemž mohou být pokutovány do výše 2.000.000,- Kč a to i opakovaně.

[9] Dalšími orgány dozoru jsou též Rada pro rozhlasové a televizní vysílání, Státní ústav pro kontrolu léčiv a Ministerstvo zdravotnictví. Bere se v potaz Okresní živnostenský úřad příslušející okresu trvalého bydliště nebo místa podnikání u právnické osoby.

5.4 Model OPT-OUT

OPT-OUT je systém, který by se dal z angličtiny přeložit jako „zvolit si odejít pryč“. Jak již název napovídá, jeho princip je zcela opačný oproti modelu OPT-IN. Znamená to tedy, že uživatel může bez předchozího souhlasu dostat email s obchodním sdělením, nicméně tento email musí splňovat zákonem stanovené parametry. Nejdůležitější je zde fakt, že takovýto email musí obsahovat jednoduchou a srozumitelnou možnost, kterou uživatel bude moci odmítnout případné další emaily od této společnosti. Ta poté pochopitelně již nemůže poslat takovému uživateli žádný další email.

Tento systém obrany proti spamu je hlavním pilířem antispamové legislativy USA, ze které vzešla celosvětově uznávaná právní norma (současně zákon v USA) obrany proti spamům – CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003). Podrobnosti o tomto zákonu jsou uvedeny v sekci 5.3.1. CAN-SPAM.

Orgánem dozoru nad výkonem tohoto zákona je Federal Trade Commision (FTC). Je třeba podotknout, že kritéria spamů jsou zde celkově sofistikovanější a případná finanční sankce se odvíjí právě od druhu rozeslaného spamu. Tato pokuta však může jít až do výše 11.000 USD, přičemž v případě, že spamer poruší zákon vícekrát, může být pokutován opakovaně a může být odsouzen i nepodmíněně.

Zajímavým aspektem této problematiky je fakt, že model OPT-OUT není tak účinný jako OPT-IN. I přesto, že právní norma CAN-SPAM je propracovanější než doporučená antispamová legislativa pro členské země EU, odhaduje se, že 60% všech spamů je původem právě z USA [14]. Některé země používají kombinaci těchto modelů (např. Austrálie) nebo upřesňují použití jednoho z těchto právních pohledů v závislosti na konkrétním typu spamu (například v Americe se považuje za spam i nevyžádaná SMS, přičemž se její spamová relevance posuzuje zároveň podle modelu OPT-IN i OPT-OUT).

5.5 Právní pohled na phishing

V České republice jsou případy phishingového útoku zatím poměrně ojedinělé, nicméně jsme se měli možnost setkat již s několika případy, které vyvolaly otázku právního pozadí tohoto činu. Jedná se především o 2 největší případy – phishingový útok na Českou spořitelnu a Citibank.

Z pohledu naší legislativy lze phishing kvalifikovat jako trestný čin podvodu dle § 250 trestního zákona. Podvodem se zde rozumí jakákoliv skutečnost, která uvede někoho v omyl, využije případného omylu či zamlčí důležité skutečnosti, a tímto způsobí někomu majetkovou škodu nebo obohacení na úkor druhého. Za takovéto jednání může být viník potrestán peněžitým trestem a

odnětím svobody až na 2 roky, pokud nebyla způsobená škoda větší než „nikoli malá“. V opačném případě či pokud se jedná dokonce o organizovanou činnost, dosahuje trestní hranice až 12 let odnětí svobody. Dalším důležitým faktem je, že minimální škoda na cizím majetku musí přesáhnout částku 5.000 Kč, kdyby se phisherovi nepodařilo samotnou finanční transakci realizovat, pak by případ setrval ve stádiu pokusu o podvod, který je samozřejmě také trestný, nicméně všeobecně mírnější.

Policie se však musí sehnat dostatečné množství důkazního materiálu, aby mohlo být prokázáno, že konkrétní osoba (phisher) odeslala danou emailovou zprávu, dále že tato osoba zneužila získané přístupové údaje tím, že použila finanční prostředky na účtech poškozených, a to vše v úmyslu obohatit sebe či někoho jiného (zpravidla organizací, která si jej najme) částkou vyšší než 5.000,-Kč. Je tedy jasné, že v tomto ohledu musí naše policie dobře spolupracovat s policií jiných států. V této oblasti se u nás standardní postupy teprve rozvíjejí, nicméně již nyní se připravují klíčové změny trestního zákona. Zde se mají objevit nové skutkové podstaty počítačové trestné činnosti. Právě nedostatečné definování těchto skutkových podstat v našem trestním právu nám zatím brání ratifikovat Mezinárodní úmluvu o kyberkriminalitě. Státy, které podepsaly tuto smlouvu sdílejí mezinárodní systém spolupráce a výměny informací mezi orgány činnými v trestním řízení.

5.6 Precedenční případy phishingu

První soudní případ phishingu byl zaznamenán v roce 2004 v USA, tehdy FTC (Federal Trade Commision) žalovala mladého teenagera z Kalifornie, který vytvořil webovou stránku s identickým designem banky America Online a použil ji k získání přístupových údajů, jež následně zneužil.

Úspěšnost tohoto případu byla vzorem pro mnoho dalších států a prakticky spustila vlnu aktivit směřujících k vystopování a odsouzení dalších phisherů. Jeden z největších úspěchů tohoto snažení bylo zatčení vedoucího člena vysoce organizované phishingové společnosti - Valdir Paulo de Almeina. Ten během 2 let svého působení odcizil až $37.000.000. Tento případ také rozpoutal otázku efektivního sběru digitálních stop v mezinárodním prostředí, jelikož členové této phisherské skupiny sídlili v různých státech a samotný Valdir byl nakonec zatčen v Brazílii. Většina phishingových útoků byla provedena na americké banky, nicméně v roce 2006 se s touto problematikou setkala i japonská justice, která odsoudila 8 lidí, kteří se podvodným způsobem využívajícím phishingové metody obohatili o 100 miliónů yenů ($900.000). V současné době byl pro phishing vyčleněn i stálý speciální vyšetřovací tým FBI.

Jelikož počet phishingových útoků stále narůstá, situace si v rámci zjednodušení trestního stíhání případných zločinců vyžádala účinnější právní ošetření tohoto druhu zločinu. V roce 2005 tedy senátor Patrick Leahy představil novou právní normu – tzv. Anti-Phishing Act. Tento zákon definuje jako trestný čin již samotné vytvoření podvodné stránky či rozesílání emailu který využívá nepravdivých údajů k oklamání příjemce za účelem krádeže identity. Nejvyšší trestní sazba, kterou tento zákon ukládá, je finanční pokuta ve výši 250.000 dolarů a odnětí svobody na dobu pěti let. Jelikož se však v USA trestní sazby jednotlivých deliktů sčítají, byl zaznamenán případ, kdy phisher čelil možnému trestu 101 let ve vězení. Tento soud se odehrával v roce 2007, Jeffrey Brett Goodin z Kalifornie čelil obvinění i z porušení zákona CAN-SPAM Act of 2003, elektronického bankovního podvodu a z poškození dobrého jména společnosti AOL. Nakonec však soud rozhodl o trestu „pouze" 70 měsíců. V současné době přijímají antiphishingové zákony postupně i další země. Příkladem může být Velká Británie a její zákon Fraud Act 2006, který považuje za trestné i vytváření či distribuci nástrojů, které by prokazatelně mohly sloužit k realizaci phishingového útoku.

Zajímavým případem české modifikace poměrně elegantního phishingu byl email, který rozeslala trojce podvodníků z Přerova. Ta místním firmám poslala oznámení, kde jménem Všeobecné zdravotní pojišťovny informovali o změně bankovního účtu této organizace. I takto jednoduchý trik měl svůj úspěch, jelikož 3 poměrně velké společnosti na tento účet opravdu začaly posílat peníze. Policie však tuto trojici dopadla již za 3 měsíce. Co se týče opravdového phishingu, zatím jediným známým případem v ČR, kdy oběti přišly i o finanční hotovost je útok na Komerční banku. Tehdy bylo podvedeno 10 klientů, nicméně v rámci zachování dobrého jména jim Komerční banka vzniklou škodu nahradila.

5.7 Mezinárodní iniciativy

Při řešení právního deliktu na úrovni mezinárodního práva je velmi výhodné, když jednotlivé právní normy zainteresovaných států jsou kompatibilní. Vzniká tedy spousta iniciativ, které se snaží unifikovat postup proti internetové kriminalitě. Tyto iniciativy probíhají většinou na úrovni pravidelných konferencí, jejichž výstupem je legislativní norma, kterou mohou využít jiné státy.

V Evropské unii je takováto norma vytvořena formou směrnic či nařízení. Nařízením je závazný akt normativní povahy. Je to pravidlo obecně závazné na úrovni Společenství i na úrovni jednotlivých členských států. Může tedy přímo zavazovat i vnitrostátní subjekty práva (osoby). Naproti tomu směrnice nemá obecnou závaznost, předepisuje jen výsledek jehož má být dosaženo, zatímco formy a metody dosažení tohoto cíle zůstávají na vůli států. V praxi to znamená, že Evropská

unie vydá směrnici upravující např. postihování spamu, nicméně záleží na každém státě, jak si ji upraví a zakomponuje do své legislativy.

Inspirací pro obsah takovýchto směrnic bývá zpravidla doporučení vycházející z činnosti mezinárodních organizací sdružující odborníky, státní i soukromý sektor. Příkladem takovýchto iniciativ mohou být tyto skupiny:

CNSA (Contact Network of Spam Enforcement Authorities) – organizace působící v rámci EU, jejímž cílem je nejen potírání spamu, ale i vytvoření databáze a vhodného komunikačního nástroje mezi evropskými zeměmi, který by byl schopen efektivně sbírat tzv. digitální stopy použitelné jako důkazní materiál pro orgány činné v trestním řízení. Tento projekt se vyvíjí od roku 2005 pod Názvem SpotSpam a je dotován finančními prostředky z fondů EU.

London Action Plan – jedná se o sdružení, jehož členy je 26 států světa a řada obchodních společností. Hlavním cílem tohoto sdružení je společně vyvíjet strategii boje proti emailové kriminalitě, a to především spamu, phishingu a virům, které je podporují. Výhodou tohoto sdružení je, že zde probíhá komunikace mezi zástupci zákonodárců jednotlivých zemí a průmyslovými firmami, které mají s touto problematikou zkušenosti, či se podílejí na vývoji samotného řešení.

Anti-Phishing Working Group(APWG) – celosvětová organizace sdružující IT společnosti, státní agentury a největší světové banky za účelem boje proti phishingu. Tato organizace vyvíjí nové metody obrany, udržuje repozitář phishingových stránek, monitoruje rozsah phishingových útoků a zabývá se i právními úpravami této problematiky, z nichž mohou čerpat jiné státy.

Je třeba říci, že nejen tyto, ale i spousta dalších nezmíněných iniciativ jsou velmi užitečné, jelikož případný zločin spáchaný v rámci států, které mají takto sjednocenou legislativu či systém forenzních postupů, je mnohem rychleji a účinněji dopátrán a případně potrestán. Nicméně tohoto faktu jsou si pochopitelně vědomi i samotní phisheři či spameři, a proto důsledně využívají států, jejichž legislativní kultura ještě není tak vysoká a nejsou členy těchto společenství. Musí se pak tedy řešit kolize právních norem jednotlivých států výše popsanými postupy a celý proces se tímto velmi zkomplikuje a prodlouží.

5.8 Internetová policie

Tímto otevírám myšlenku samostatného aktivního orgánu, který by byl součástí veřejného sektoru a jehož práva a pravomoc by byla zaručena legislativou příslušného státu. Můžeme si tuto myšlenku představit jako internetový ekvivalent dopravní policie, která aktivně hlídá dodržování pravidel silničního provozu, řeší případné kolize a za určitých okolností je schopna zcela řídit dopravu. Obdobně by se internetová policie starala o to, aby internet nebyl zatěžován spamy, nežádoucími stránkami s protiprávním obsahem, ale byla by schopna i efektivně řešit další internetovou kriminalitu (porušení autorských práv, phishing, atd.).

Již ze zmíněného příkladu lze vidět zásadní věc, o kterou se tato myšlenka opírá. Pro funkčnost institutu internetové policie je totiž zapotřebí především pevné zakotvení v legislativě, kdy stejně jako dopravní policie může kdykoliv zkontrolovat jakoukoliv veřejnou komunikaci, musí i internetová policie mít dostatečný přístup k serverům poskytovatelů internetových služeb. DNS serverům, atd. Bylo by též potřeba vytvořit právní normy pro sběr digitálních stop v internetovém prostředí a samotné forenzní postupy.

Pochopitelně, že již v dnešní době naše policie tyto problémy řeší (jedná se o útvar pro odhalování kriminality na Internetu Policie České republiky), nicméně vzhledem k nedostatečným pravomocem, špatnému sběru digitálních stop a nekoncepčnosti spolupráce s internetovými společnostmi je případné dohledání takovéto kriminality neefektivní a často i neúčinné. Myslím si, že informaticko-právní rozbor této myšlenky by byl velmi zajímavý a přínosný, nicméně tato myšlenka je již nad rámec této bakalářské práce. Hodlám ji však později rozpracovat společně se studenty právnické fakulty Masarykovy univerzity.

6 Implementace nástroje na rozpoznávání phishingových emailů

Součástí této práce je implementace nástroje na analýzu dat o phihsingu. Jelikož phisheři využívají pro svou činnost především podvodných emailů, rozhodl jsem se naprogramovat aplikaci, která by byla schopna rozpoznat tyto emaily.

Implementovaný nástroj je jednoduchá aplikace napsaná v jazyce C++ určená pro obdobu operačního systému Linux. Tato aplikace má z důvodu snadnější prezentace funkčnosti 2 modifikace. 1. verze se jmenuje phishtank_test a pracuje jako zcela nezávislý klient, který se připojí na poštovní server pomocí protokolu POP3, prohlédne předem zadaný počet nejnovějších zpráv a vyhodnotí jejich obsah. Druhá modifikace tohoto programu je pojmenována jako phishtank a předpokládá nasazení na poštovním serveru, nebo na klientu pracujícím s emaily pomocí lokálních složek (například pomocí programu fetchmail). Tato implementace již samostatně nestahuje emaily z poštovních účtů, nýbrž zpracovává emaily po jiných programech (například program procmail). První modifikace tohoto nástroje je určena především pro testovací a prezentační účely, proto v ní lze zapnout několik pomocných výpisů znázorňujících běh programu. Druhá implementace vyžaduje vhodné nastavení samotného poštovního serveru nebo aplikace (ta musí znát umístění emailů a spustit se v době, kdy počítač tyto emaily zpracovává).

6.1 Princip analýzy obsahu emailů

Tento program využívá základního principu, díky kterému phisheři oklamou svou oběť, a sice podvodných hypertextových odkazů.

Při své analýze tedy postupně pročítá obsah emailu a hledá v něm hypertextové odkazy. Jakmile nalezne v těle emailu takovýto odkaz, zakóduje jej pomocí vestavěného algoritmu do base64 (pro tyto účely není použito žádné knihovny). Dále se program připojí na server phistank.com, který obsahuje volně přístupnou databázi url adres použitých v phishingových emailech. Tento server vyhodnotí, jestli se zakódovaná url adresa nalézá v jeho databázi a vrátí odpověď v podobě xml výstupu. Program následně vyhodnotí informace obsažené v této odpovědi a na základě toho provede s emailem příslušnou akci (v případě serverové implementace vloží do předmětu emailu nápis ***

PHISH ***, u demonstrační implementace program zobrazuje veškeré statistiky na standardní výstup).

6.2 Instalace a spuštění programu phishtank

Program phishtank je určen pro systémy pracující na platformě linux. Jelikož se jedná o poměrně jednoduchý program, stačí jej jen zkompilovat pomocí příkazu *make* a případně nahrát do požadované složky. Jedinou podmínkou správného běhu programu je to, aby měl právo zápisu do uvažované složky a aby v této složce existoval soubor *tmp* který používá jako pracovní dočasný soubor.

Nyní lze phishtank otestovat pomocí přiloženého souboru *ukazka*, nebo lze použít programu phishtank_test, který poměrně názorně demonstruje funkci phishtanku.

6.2.1 Program phishtank_test

Tento program je určen pro demonstraci funkce phishingového filtru. Samotný program phishtank byl vyvinut původně z tohoto programu. Výhodou aplikace phishtank_test je především snadné a názorné použití.

Phishtank_test je jednoduchý klient, který se připojí na předem zadaný POP3 server. Zde prohlédne předem daný počet nejnovějších emailů a vypíše na standardní výstup výsledky provedené analýzy. Syntaxe spuštění tohoto programu je následující:

```
phishtank_test jméno_pop3_serveru:port jméno heslo [-v]
```

Jako jméno serveru je třeba uvést celou adresu serveru s číslem portu, na který se chceme připojit (většinou 110). Program se na serveru přihlašuje pomocí jména a hesla uvedeného v položce *jméno* a *heslo*. Přepínač *–v* je nepovinný a při jeho zapnutí program vypisuje url adresy, které nalezl během analýzy emailů.

6.2.2 Program phishtank

Phishtank je program, který lze provozovat na poštovním serveru i na klientské stanici. Záleží na aktuálním nastavení a politice počítače, na kterém tento program běží. Nejpraktičtější nastavení je podle mého názoru přidání programu phishtank do fronty programů zpracujících příchozí poštu. V tomto případě se phishtank spustí vždy v momentě, kdy na lokální poštovní účet dojde nový email. Jelikož emaily jsou ukládány ve formě jednoho textového souboru pro každý účet, je cesta k tomuto souboru potřebným argumentem při spuštění programu phishtank. Syntaxe spuštění je tedy:

```
phishtank path [-v]
```

Jméno požadovaného souboru s jeho kompletní cestou se doplňuje jako parametr *path*. Přepínač *–v* zapíná pomocné výpisy, které zobrazují výsledky analýzy emailů.

Pokud program phishtank zjistí, že zkoumaný email je phishingový, připíše v poli jeho předmětu nápis *** PHISH ***. Phishtank nepotřebuje ke své funkci moc operační paměti bez ohledu na množství a velikost emailů, jelikož pracuje pomocí dočasného souboru tmp.

6.3 Výhody a nevýhody této implementace

Největší výhodou této implementace je především univerzálnost použití a nenáročnost z hlediska prostředků nutných pro běh samotného programu. Tato aplikace pracuje s emaily uloženými na disku přímo, bez nutnosti načítat jejich obsah do operační paměti (pro modifikaci souboru využívá záložní tmp soubor). Díky této charakteristice lze tuto aplikaci použít i na velmi velký počet emailů bez výrazných ztrát výkonu. Jelikož je tento program nezávislý na žádném konkrétním protokolu (pomineme-li prezentační verzi), lze použít jak na poštovním serveru, tak na klientu. Použitá databáze serveru phistank.com je největší veřejně dostupnou databází phishingových url adres na síti internet.

Na druhou stranu tento program bohužel nemůže dostatečně rychle reagovat na nové phishingové emaily. Vzhledem k tomu, že phistank funguje na základě reportů o phishingových emailech ze strany svých zaregistrovaných uživatelů a dalších obdobných serverů, musí nejprve daný falešný link potvrdit dostatečné množství uživatelů, aby bylo možné posoudit, zdali se jedná o phishing či nikoliv. Díky tomuto vzniká prodlení, které může znamenat, že email je zpracován pomocí poštovního agenta dříve, než se phistank dozví, že se jedná o podvodný email. Tato situace

není až tak špatná v rámci USA a dalších zemí, které jsou častými oběťmi phishingu, zde je reakční doba phishtanku jedna až několik hodin. Nicméně toto bohužel neplatí pro Českou republiku, kdy díky nízkým zpětným vazbám podvodných emailů na phishtank ověření validity ohlášení phishové adresy trvá až několik dní. Tato reakční doba je poměrně nedostatečná, jelikož phisheři většinou odešlou všechny své podvodné emaily během jednoho dne. Nelze tedy soupeřit s profesionálními řešeními antiphishingové ochrany, které používají propojenou síť honeypotů, díky kterým se reakční doba na výskyt podvodného emailu rapidně zkracuje.

6.4 Možná vylepšení antiphishingového nástroje

Na tomto nástroji by se dalo ještě v budoucnu dále pracovat. Za velmi přínosné bych považoval tato vylepšení:

- rozšíření analýzy emailu o textový parser hledající klíčová slova či neshody v zápisu url adres (zobrazené url se liší od odkazovaného url)
- spolupráce s databázemi spamů (možnost podílet se na celkové emailové ochraně)
- implementace spolupráce aplikace s programem sendmail pomocí API knihovny MITL (ta umožňuje, aby naše aplikace naslouchala na portu, na který ji sendmail postupně přeposílá obdržená data. V případě pochybnosti o legitimitě emailu může naše aplikace zaslat pokyn k ukončení samotného SMTP přenosu. Email lze tedy takto filtrovat ještě dříve, než je uložen na disk)

Závěr

Tato práce si klade za cíl především osvětlit současné problémy emailové komunikace. Proto jsem se snažil poukázat na související právní pohled a zároveň nahlédnout do samotného technického pozadí emailových problematik.

Myslím si, že právě prozkoumání právních rámců emailové problematiky může být velmi přínosné. Spousta firem si například neuvědomuje, kde leží pomyslná hranice spamu a jaké jsou případné postihy. Dalším zajímavým cílem v mé práci bylo zasadit emailovou kriminalitu do prostředí mezinárodního práva. Tato problematika je poměrně složitá, nicméně vzhledem k současnému rozšíření phishingu, který doslova využívá nevyspělé právní kultury některých zemí, je velmi aktuální.

Dále bylo mým cílem nahlédnout do tvorby nástrojů sloužících k zabezpečení schránek proti nevyžádaným emailům. Zde jsem si zkusil implementovat jednoduchý phishingový filtr. Považuji za velmi zajímavou zkušenost poznání, že naprogramovat samotný filtr bylo poměrně jednoduché, ale uvést jej do provozu tak, aby spolupracoval s jinými programy a byl co nejuniverzálnějším, byl úkol, který v sobě skrýval spoustu úskalí. Postupem vývoje jsem přišel i na několik vylepšení, která by tento program mohl mít, nicméně musím konstatovat, že vzhledem k omezeným možnostem nekomerčních databází a nutnosti velmi rychle reagovat na nové phishingové emaily, tento program nikdy nebude a ani nemůže dosahovat kvalit velmi dobře zaplacených antiphishingových řešení modifikovaných na míru konkrétní bance.

Myslím si, že v této práci lze nalézt spoustu témat, která jsou velmi aktuální, bohužel jsou však informace o nich poměrně neucelené, nebo roztříštěné na mnoha místech sítě internet. Doufám tedy, že tato práce bude cenným zdrojem či inspirací pro případného čtenáře.

Zdroje

[1] *Spam-o-meter* [online]. 2006 [cit. 2008-03-11]. Publikováno diskusní skupinou news.admin.net-abuse.email (NANAS). Dostupný z WWW: <http://www.spam-o-meter.com/>.

[2] MSNBC. *Survey: 2 million bank accounts robbed* [online]. 2004 [cit. 2008-03-28]. Dostupný z WWW: <http://www.msnbc.msn.com/id/5184077/>.

[3] All Media Inc.. *Email List Rental* [online]. 2008 [cit. 2008-03-28]. Dostupný z WWW: <http://www.allmediainc.com/email-list-rental.html>.

[4] *Spam-o-meter statistics by percentage* [online]. 2006 [cit. 2008-03-29]. Dostupný z WWW: <http://www.spam-o-meter.com/stats/index.php>.

[5] Sender Score Certified [online]. 2008 [cit. 2008-02-02]. Systém ověřování autentičnosti emailu na základě DNS whitelistu. Dostupný z WWW: <http://www.bondedsender.org/senderscorecertified/index.php>.

[6] Habeas Inc.. *Habeas Improves Email Delivery Rates, Avoid Email Blacklists with Monitoring and Authentication Email Compliance Solutions* [online]. 2008 [cit. 2008-03-29]. Dostupný z WWW: <http://www.habeas.com/en-US/Home/>.

[7] Federal Trade Commission. Email Address Harvesting and : A Report by the Federal Trade Commission's Division of Marketing Practices. [s.l.] : [s.n.], 2005. 10 s. Dostupný z WWW: <http://www.ftc.gov/opa/2005/11/spamharvest.pdf>.

[8] *Seznam - ideální pro spammery* [online]. 2003 [cit. 2008-04-02]. Dostupný z WWW: <http://www.lupa.cz/clanky/seznam-idealni-pro-spammery/>.

[9] *WORKING TO PROTECT INTERNET NETWORKS WORLDWIDE* [online]. 2007 [cit. 2007-12-02]. Dostupný z WWW: <http://www.spamhaus.org/images/dnsbl_mirrors.gif>.

[10] *Statistics about phishing activity and PhishTank usage* [online]. 2007 [cit. 2007-12-19]. Dostupný z WWW: <http://www.phishtank.com/stats.php>.

[11] *Phishing scam reports archive* [online]. 2003 [cit. 2008-01-10]. Stránky spolupracující s APWG, které obsahují aktuální komerční databázi phishingových scamů. Dostupný z WWW: <http://www.millersmiles.co.uk/archives.php>.

[12] APWG - Anti Phishing Working Group. *Phishing and Crimeware Map* [online]. 2008 [cit. 2008-01-10]. Nezávislé sdružení zabývající se bojem proti phishingu a jeho monitorováním. Dostupný z WWW: <http://www.antiphishing.org/crimeware.html>.

[13] The Honeynet Project & Research Alliance. *Detailed analysis of first incident at German Honeynet Project* [online]. 2004 [cit. 2008-01-19]. Dostupný z WWW: <http://www.honeynet.org/papers/phishing/details/de-detailed.html>.

[14] Internacional Telecommunication Union. *ITU Activities on Countering Spam* [online]. 2005 [cit. 2007-11-11]. Dostupný z WWW:
<http://www.itu.int/osg/spu/spam/>.

Literatura

[1] LANCE, James. *Phishing bez záhad*. Lubomír Dlouhý. 2007. vyd. [s.l.] : Grada, 2007. 356 s. ISBN 978-80-247-1766-1.

[2] COSTALES, Bryan, et al. *Sendmail* . [s.l.] : O\'Reilly Media, Inc., 2007. 1308 s. 4. edice. ISBN 978-0596510299.

[3] *SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ : Boj proti spamu a špionážnímu („spyware") a škodlivému softwaru („malicious software").* KOMISE EVROPSKÝCH SPOLEČENSTVÍ. 2006. Brusel : KOM, 15.11.2006. Dostupný z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:CS:PDF>.

[4] TISCHLER, Jan. *Spam a bezpečnost emailové komunikace*. [s.l.], 2007. 79 s. České vysoké učení technické v Praze, Fakulta elektrotechnická, Katedra počítačů. Vedoucí diplomové práce Ing. Jan Kubr.

[5] *Aplikace evropského práva národním soudcem*. Příručky Ministerstva Spravedlnosti ČR. 1997. vyd. Praha : SEVT, a. s., 1997. 63 s. 56. svazek.

[6] OUTLÁ, Veronika, HAMENÍK, Pavel. *Praktikum práva Evropské Unie*. Plzeň : Aleš Čeněk, s.r.o., 2005. 283 s. ISBN 80-86898-10-5.

[7] MALENOVSKÝ, Jiří. Mezinárodní právo veřejné. Masarykova univerzite Brno. Brrno : Doplněk, 1993. 179 s. ISBN 80-85765-09-8.

Seznam obrázků

Seznam příloh

Příloha 1. CD s programem Phishtank