A zase spam

Bohuslav Moučka, Radim Peša, ÚVT MU

Podíl nevyžádané pošty na celkovém objemu zpráv přenášených elektronickou poštou se v současné době pohybuje přes 60 % procent všech přenesených zpráv. Nevyžádaná pošta nejenom znepříjemňuje uživatelů práci, ale způsobuje i značné finančně vyčíslitelné ztráty. Hrozí nebezpečí, že bez přijetí účinných opatření omezujících šíření nevyžádané pošty by elektronická pošta pravděpodobně přestala být použitelná jako efektivní komunikační nástroj.

O závažnosti této problematiky svědčí i fakt, že si v řadě zemí vyžádala vydání zákonů definujících pravidla hry v této oblasti. 1. ledna 2004 vstoupila ve Spojených státech amerických v platnost právní norma Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003), která definuje podmínky využívání nevyžádané pošty k marketingových účelům. Tato norma rozesílání nevyžádané pošty nezakazuje, ale definuje podmínky které musí odesílatel dodržovat. Odesílatel například musí dát příjemci možnost odmítnout příjem dalších zpráv, odesílatel je povinen uvádět ve zprávách svou skutečnou identitu atd. Mimoto zákon počítá s vybudováním seznamu adres uživatelů, kteří nechtějí dostávat žádnou nevyžádanou poštu.

V České republice je problematika spamu ošetřena v Návrhu zákona o některých službách informační společnosti. Návrh podalo Ministersvo informatiky, 21.1.2004 jej schválila vláda a nyní čeká na projednání v Poslanecké sněmovně. Česká norma na rozdíl od CAN-SPAM Act of 2003 vyžaduje, aby měl odesílatel nevyžádané pošty předem výslovný souhlas příjemce svých zpráv.

Obdobné normy regulující tuto oblast existuji i v řadě dalších zemí. Nicméně se zatím nezdá, že by po jejich přijetí došlo k poklesu počtu doručovaného spamu. Uvidíme, zda se to změní až dojde k prvním soudním řízením a odsouzením spammerů [6].

Jednotlivé statistiky a odhady zastoupení nevyžádané pošty v přenášené elektronické poště se liší. Výrazné rozdíly jsou například mezi jednotlivými regiony. Ze dvou často citovaných firem zabývajících se anti-spamovou ochranou elektronické pošty uvádí Brightmail [7] 64 % ní podíl spamu na veškeré poště, MessageLabs [8] pak dokonce 67.6 %.

Zajímavých údajem je i původ nevyžádané pošty. V dubnu 2004 pocházelo nejvíce spamů z následujících zemí:

USA	60.5 %
Čína	6.2 %
Jižní Korea	4.9 %
Kanada	4.3 %
Brazílie	2.9 %
Francie	2.0 %

Většina spamů obsahuje odkaz na WWW stránky; podíl jednotlivých států na celkovém počtu odkazovaných stránek byl v dubnu 2004 následující:

Čína	70.0 %
USA	22.0 %
Brazílie	2.3 %
Jižní Korea	1.8 %
Rusko	1.5 %

Tradiční způsoby šíření spamu byly popsány v článku [1]. V poslední době se však objevuje nový fenomén poskytující zázemí pro další akceleraci nárůstu množství rozesílaného spamu. Jedná se o propojení firem živících se rozesíláním spamu a autorů počítačových virů. Podle statistiky antivirové firmy Eset, bylo 70 % virů přijatých v období 1.7.2003 až 1.2.2004 využitelných ke spamovacím aktivitám. Tyto viry totiž instalují do napadených počítačů komponenty, které je možné vzdáleně kontaktovat a zneužít k masivnímu rozesílání elektronické pošty. Takto napadených počítačů je velké množství a nahrazují roli dříve zneužívaných open relay serverů. Tak jako se prodávají databáze elektronických adres, je prý nyní možné koupit i seznamy takto napadených strojů. Autorům počítačových virů se tak konečně naskýtá možnost využít komerčně svých znalostí.

Současně se předpokládá, že naopak autoři virů využívají ke šíření virů spamovací techniky. To jim umožní v krátkém čase rozeslat kopie viru na velké množství adres a tím maximálně využít

první minuty a hodiny šíření počítačového viru, kdy se virus šíří nejúspěšněji. To by vysvětlovalo i případy extrémně rychlých virů z jara tohoto roku, kdy se konkrétní vir dokázal během méně než dvou hodin od svého zrodu masově rozšířit po celém světě. Po dvou hodinách již byly k dispozici aktualizace antivirových databází a masové šíření viru bylo ukončeno (minimálně na MU).

Jak se bránit

Mimo tradičních způsobů blokování nevyžádané pošty podle černých listin a prohledávání obsahu zprávy popsaných např. v [1], se stále hledají další technické prostředky pro omezení šíření nevyžádané pošty. Jsou to například následující dva způsoby upravení způsobu doručení elektronické pošty protokolem SMTP.

Greylisting [5]

Principem je využití obecné vlastnosti poštovních serverů, které při neúspěšném doručení dopis zařadí do fronty a pokusí se jej po určitém čase doručit znovu (spamerské rozesílače naproti tomu rozesílají spamy jednorázově).

Přijímající server si z každého dopisu přečte IP adresu odesílajícího stroje, adresu odesílatele a adresu příjemce. Pokud již má takovouto trojici ve své databázi, dopis doručí. V opačném případě dopis odmítne, vyrozumí o tom odesílající server a novou trojici si zapíše do databáze s příznakem, že po určenou dobu (například jednu hodinu) nebude dopisy se stejnými parametry přijímat. Jestliže dopis se stejnou trojicí přijde po uplynutí doby blokování, je doručen a v databázi je trojice označena jako povolená. Pokud dopis s blokovanou trojicí do určité doby nepřijde, je záznam vymazán.

Výhodou greylistingu je, že dopis je odmítnut již v začátku komunikace a analýza jeho obsahu nezatěžuje přijímací stroj. Nevýhoda je ve zpoždění doručení dopisů od neznámých odesílatelů a také to, že je možné ho obejít vhodným odesílajícím serverem. Proto se doporučuje používat greylisting v kombinaci s jinými metodami boje proti spamu.

Sender Policy Framework (SPF)

Spamy jsou rozesílány nejen na reálně existující adresy, ale i na vygenerované seznamy adres, z nichž jen malá část skutečně existuje. Nedoručitelné dopisy s neexistujícími adresami jsou automaticky vraceny zpět na adresu uvedenou v poštovní hlavičce. Často se stává, že poštovní server, je zcela zahlcen vracenými dopisy a jeho systém se zhroutí. Autoři spamů se snaží skrýt svou identitu a nechtějí dostávat chybové zprávy, proto jako odesílatele uvádějí cizí adresy, někdy je tam dokonce uvedena adresa příjemce spamu. Umožňuje jim to protokol SMTP, který vznikl před více než 20 lety a dovoluje odesílateli napsat do hlavičky libovolnou adresu. Tento problém se snaží řešit doplněk protokolu SMTP nazvaný Sender Policy Framework (SPF).

Pokud posíláme dopis na nějakou adresu, poštovní program zjistí, kam ho má poslat podle záznamů typu MX pro danou doménu. Tyto záznamy uvádějí jména počítačů přijímajících poštu pro doménu. Většinou jich není více než 3. Podobně malý je téměř u všech domén počet poštovních serverů, které poštu z dané domény odesílají. Jejich jména ovšem nemusejí být nikde uvedena. SPF zavádí do DNS záznam popisující, které počítače odesílají poštu z domény a nabízí moduly do nejrozšířenějších poštovních serverů, které kontrolují, zda dopis přichází skutečně z domény uvedené v hlavičce.

Přínos SPF v boji proti spamu a virům je v tom, že se odfiltrují dopisy s podvrženou adresou odesílatele. Pokud spameři budou používat svoje skutečné adresy, bude snadnější je odfiltrovat pomocí blacklistů. Problém s použitím SPF nastává při přesměrovávání dopisů do jiné domény, protože se nezmění adresa odesílatele a dopis bude serverem konečného příjemce odmítnut. Řešení přináší sender rewriting scheme (SRS) – další modul do poštovních serverů přepisující adresu odesílatele v obálce dopisu tak, aby byl přijat i serverem podporujícím SPF.

Protispamová opatření na MU

Centrální poštovní brána Masarykovy univerzity provádí u každé příchozí emailové zprávy následující úkony [2]:

1. Zápis IP adresy poštovního serveru, od kterého je zpráva přijata, do hlavičky zprávy X-Muni-Spam-TestIP
2. Ověření IP adresy poštovního serveru, od kterého je zpráva přijata, v databázích černých listin (black list) spammerů. Při pozitivním výsledek je do hlavičky zprávy X-Muni-Spam-List zapsán název černé listiny, v níž je poštovní server registrován.

Tyto údaje jsou zaznamenány pro usnadnění další detekce a zpracovaní spamu na poštovních serverech subdomén MU (fakult). Všechny dopisy přijaté na poštovní bráně jsou doručovány dále na poštovní servery subdomén MU (výjimkou jsou zprávy nepřijímané z důvodu antivirové ochrany). Na úrovni těchto serverů, případně samotných poštovních schránek uživatelů, je pak většinou implementována filtraci nevyžádané elektronické pošty. Konkrétně, na šesti fakultách (ESF, FF, FI, FSS, PedF, PřF), rektorátu a ÚVT byl v okamžiku psaní tohoto článku instalován filtr *spamassassin*. Na LF je zatím používána antispamová konfigurace programu sendmail (ručně udržovaný seznam nežádoucích adres), PrávF a FSpS prozatím žádnou antispamovou kontrolu neuplatňovaly.

Zpracování nevyžádané pošty v různých součástech univerzity se liší podle politiky uplatňované v jednotlivých subdoménách. Všichni uživatelé by měli mít možnost aktivovat si filtr nevyžádané pošty. Jednotlivé subdomény se liší ve způsobu výchozího nastavení. Některé subdomény mají jako výchozí nastavení uživatelů zapnuto filtrování nevyžádané pošty (Fakulta informatiky), jiné aplikují spamové filtry až na explicitní žádost uživatele. Dá se říct, že běžně používané antispamové nástroje [3, 4] dostupné na poštovních serverech MU umožňují uživatelům kvalitní odfiltrování nevyžádané pošty. Například již pouhou aktivací nástroje [3] dochází k odfiltrování cca 80% nevyžádané pošty. Dalším odladěním samoučících filtrů je možné dosáhnout i 95% a vyšší úspěšnosti. Bohužel toto ladění již vyžaduje netriviální součinnost uživatele se správcem antispamového nástroje. Je proto potřeba hledat způsoby filtrace nevyžádané pošty, které mají vysokou účinnost a jsou pro uživatele maximálně jednoduché na použití.

Filtry nevyžádané pošty bývají implementovány nejenom na poštovních serverech. Pro hojně rozšířené poštovní klienty existují doplňky, které přidávající funkcionalitu filtrování nevyžádané pošty na úrovni poštovního klienta. Microsoft Outlook 2003 a poštovní klient obsažený v balíku Mozilla mají tuto funkci přímo zabudovanou. Jejich použití je uživatelsky přívětivé, nevýhodou je vazba na poskytované ochrany na konkrétního poštovního klienta.

Literatura

[1] M. Kolaja, M. Bartošek. Jemný úvod do (anti)spamové problematiky, Zpravodaj ÚVT MU, ISSN 1212-0901, 2002, roč. 12, č. 5, s. 1–6.

[2] M. Ruda. Opatření proti spamům na MU. Zpravodaj ÚVT MU, ISSN 1212-0901, 2002, roč. 12, č. 5, s. 6–7.

[3] http://www.spamassassin.org

[4] http://bogofilter.sourceforge.net

[5] http://www.greylisting.org

[6] FTC Announces First Can-Spam Act Cases, http://www.ftc.gov/opa/2004/04/040429canspam.htm

[7] http://www.brightmail.com

[8] http://www.messagelabs.com □