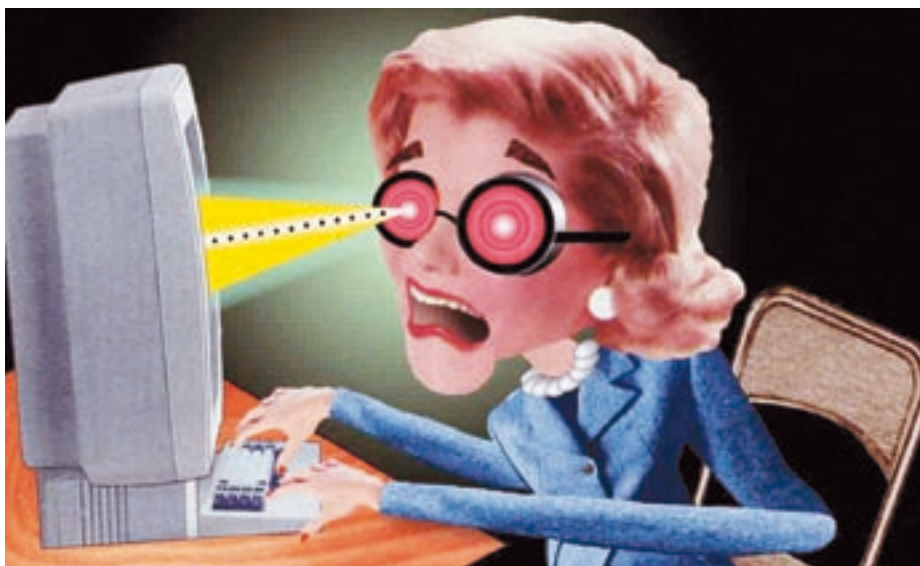


Spam chodí po lidech

Říká se „neštěstí nechodí po horách, ale po lidech“. Stejně je to i se spamem, buď už k vám pravidelně chodí, nebo se rozhlíží okolo a hledá, kde je nějaká vhodná e-mailová adresa, na kterou by se dalo něco poslat. Statistika antispamové brány instalované ve společnosti kde pracuji, ukázala, že během třiceti dní bylo zadrženo 80 % příchozích e-mailů. Převážně na základě reputace odesilatele.

Mirek Holý



Nabízí se otázka, zda aktivitu individuí majících potřebu hromadně rozesílat e-maily není možné nějak účinně omezit. Přestože je spam již delší dobu kriminalizován (www.spamlaws.com), jeho množství stále roste (Internet Security Trends for 2007, ironport.market2lead.com/go/ironportinc/securitytrends). Důvod, proč spammeři podstupují riziko vysokých pokut a trestů odnětí svobody, je prostý, jde o peníze. V lepším případě za spamem stojí snaha prodat skutečný plnohodnotný produkt. V horším případě jde například o snahu přimět ostatní na základě zavádějících informací k nákupu určitých akcií. Ti, kteří stojí za takovým spamem, nakoupí akcie nějaké málo obchodované, neznámé společnosti. Pak rozešlou spam, kde akcie co nejvěrohodněji prezentují jako podhodnocené. Najdou se tací, kteří sednou na lep a začnou nakupovat. Při malých obchodech i relativně málo kupujících dokáže pohnout cenou nahoru. Původní majitelé se ziskem prodají. Asi vůbec nejhorší je, když se pomocí spamu bez okolků podvádí. Často se tak

děje v případě on-line prodeje léků. Viagra nebo psychofarmaka k dostání bez předpisu jsou lákadlem. Bohužel je pravidlem, že se tímto způsobem distribuují napodobeniny populárních tabletek. Viagra je sice modrá, jak má být, účinek se ovšem nedostaví.

LZE NA SPAM VYZRÁT?

Jednoduchý recept na e-mailovou schránku beze spamu, který by zachovával účastníkům e-mailové komunikace dosavadní jednoduchost a nenáročnost používání elektronické pošty, neexistuje. Do popředí se tak dostávají řešení, která jsou založena na principu Popelčina vybírání hrachu z popela. V roli inteligentních holubů se objevují více či méně chytrá zařízení nebo programy schopné rozeznat spam na základě podobnosti předchozím e-mailům označeným jako spam nebo na základě signatur z takových e-mailů vytvořených, případně na základě jiných znaků. Stejně jako v případě virů i v případě spamu platí, že spammeři svádějí permanentní boj s výrobcí antispamových řešení. Neustále

mění rozesílané e-maily a testují jejich průchodnost přes antispamy. V případě spokojenosti se snaží v co nejkratším čase (než se antispamy stačí přizpůsobit) rozeslat co nejvíce e-mailů.

JAK TEDY NA SPAM?

Funkční a poměrně úspěšné antispamové řešení lze postavit na základě volně dostupného softwaru. Mám na mysli především program SpamAssassin (spamassassin.apache.org), s pomocí kterého lze realizovat síťovou antispamovou bránu. Základem každého antispamového řešení je znalostní báze, ze které program vychází při identifikaci spamu. Při přístupu „udělej si sám“ jsou za aktualizaci takové báze odpovědní zaměstnanci organizace. Přejde-li jim spam, označí ho, čímž se doplní znalostní báze a systém je zase o kousek „chytřejší“. Pomoci mohou přes internet volně dostupné znalostní báze, např. rulesety (www.rulesemporium.com) pro již zmíněný SpamAssassin.

Viděno idylicky, existuje spousta kouzelných krabiček (zařízení), které se prostě připojí do sítě a tam si v poklidu dělají svoji práci. Tak růžové to v praxi vždy není, i když právě v případě antispamových síťových zařízení není realita idylce příliš vzdálená. Antispamové kouzelné krabičky vás na rozdíl od kouzelných IDS krabiček nezbudí ve tři ráno dožadující se akutního zásahu. Není také třeba je opečovávat jako kouzelné firewallové krabičky, na kterých je nutné neustále měnit pravidla. Z pohledu velkých a větších organizací, kterých naplní je něco jiného než boj se spamem, je realizace antispamového řešení pomocí kouzelné krabičky logickou volbou. Tato zařízení si v krátkých časových intervalech (řádově minuty) přes internet obcerstvují znalostní bázi. O tu se nepřetržitě stará tým specialistů výrobce zařízení. Zařízení je tak schopno reagovat i na velmi čerstvou vlnu spamu.

Se spamem to není a nebude jednoduché, první se objevil už v sedmdesátých letech v dobách Arpanetu (www.templetons.com/brad/spam/spam25.html). Ani Bill Gates, který v roce 2004 prohlásil, že do dvou let bude problém spamu vyřešen, zatím nic převratného nevymyslel.

Autor působí ve společnosti Actinet Informační systémy.