Opatření proti spamům na MU

Miroslav Ruda, ÚVT MU

V návaznosti na zavedení centrální antivirové kontroly elektronické pošty na MU (viz minulé číslo Zpravodaje) hledá ÚVT MU také vhodné možnosti centrální podpory pro ochranu uživatelů MU proti spamům. Na rozdíl od virů nepředstavují spamy pro uživatele přímé ohrožení (nemají destruktivní účinky v podobě ztráty dat či funkčnosti výpočetního systému) a také míra jejich dopadu a vnímání škodlivosti je u jednotlivých uživatelů podstatně variabilnější. Přesto však strmý nárůst počtu spamů v elektronické poště představuje pro řadu uživatelů problém, který chtějí řešit.

Současné možnosti obrany proti spamům jsou mnohem méně účinné, než je tomu v případě počítačových virů. Je také mnohem obtížnější rozhodovat na centrální úrovni o tom, co je či není spammem a případně ze kterých serverů blokovat příjem (nežádoucí) pošty (aniž by tím neúměrně stoupalo riziko zablokování také pošty žádoucí). V daleko větší míře než v případě virů je zde potřeba individuálních nastavení a přístupů na úrovni jednotlivých uživatelů, má-li být obrana proti spamům rozumně účinná a přitom i bezpečná.

Navrhovaný systém centrální podpory pro antispamovou ochranu na MU využívá prvků zavedených již dříve v systému antivirové ochrany elektronické pošty (nový poštovní server s možností centrálního značkování přicházející pošty a mechanismus pro zpracování označkované pošty na úrovni fakult resp. individuálních poštovních schránek). Základní principy jsou následující:

- centrální poštovní server MU relay.muni.cz žádné spamy přímo nelikviduje, ale značkuje poštu přicházející do domény `muni.cz` pro potřeby fakultní či individuální antispamové ochrany, a to způsobem popsaným níže
- každý dopis přicházející z open-relay serveru, který je uveden v některé ze sledovaných černých listin spammerů, je označen hlavičkou **X-Muni-Spam-List**; tato hlavička obsahuje název černé listiny registrující ve svých seznamech daný open-relay server [1]
- každý přicházející dopis bez rozdílu je označen hlavičkou **X-Muni-Spam-TestIP**, ve které je uvedena IP adresa serveru, ze kterého dopis přišel do domény muni.cz. Uživatelé preferující jinou než centrálně používanou černou listinu mohou využít tuto informaci pro nastavení vlastních filtrovacích kritérií (viz dále)
- dopis prochází po označení dál na úroveň subdomény xxx.muni.cz. Administrátor subdomény (resp. koncový uživatel) může instalovat procmailová pravidla připravená na ÚVT MU, která na základě hlavičky X-Muni-Spam-List, nebo X-Muni-Spam-TestIP (a následného dotazu do uživatelem zadané černé listiny) příslušný dopis-spam dále zpracují, tj. smažou nebo uloží do speciální poštovní schránky (v závislosti na konkrétním nastavení).

V květnu t.r. probíhal na MU testovací provoz výše popsaného systému, při němž vybraní uživatelé z ÚVT MU a FI MU sledovali účinnost značkování (kolik opravdových spamů bylo na základě dotazování uvedených černých listin jako spam také skutečně označeno). Zjištěná průměrná účinnost se pohybovala kolem 50%.

Aktuální informace k centrální podpoře antispamové ochrany na MU, včetně příslušných procmailových pravidel, lze nalézt na bezpečnostní stránce ÚVT MU, `http://www.ics.muni.cz/services/security/`. □

[1] V současné době využívá centrální poštovní server MU pro značkování tří černých listin: `relays.ordb.org`, `blackholes.mail-abuse.org` a `bl.spamcop.net`. Aktuální seznam používaných černých listin je vystaven na www stránkách ÚVT MU, viz závěr článku.