E-mail, spam a greylisting MU

Radim Peša, ÚVT MU

Objem elektronické pošty přepravované poštovními servery MU neustále narůstá. Výraznou část poštovního provozu přitom představuje spam – nevyžádané obtěžující e-maily. Rozsah spamu již dosáhl stupně, který pro řadu uživatelů znamená výraznou degradaci elektronické pošty jako nástroje efektivní komunikace. Na druhé straně představuje spam stále větší zátěž i pro poštovní infrastrukturu MU (centrální poštovní server MU a na něj navazující poštovní servery fakult a dalších součástí univerzity). V tomto článku uvedeme číselné údaje ilustrující objem elektronické pošty na MU a dopad nových opatření na omezení množství spamu – zavedení greylistingu na centrálním poštovním serveru MU.

1 Objem elektronické pošty na MU

Před zavedením celouniverzitního antispamového opatření ve formě greylistingu počátkem března 2007 [1] zpracovával centrální poštovní server MU téměř milión elektronických zpráv denně. Po zavedení greylistingu tento počet ještě stoupl, protože část dočasně odmítnutých zpráv přichází na MU opakovaně.

Celkový objem elektronické pošty na MU lze charakterizovat tabulkou 1. Ukazuje průměrné denní počty zpracovávaných (tj. doručených i nedoručených) zpráv na centrálním poštovním serveru MU, a to ve dvou různých týdnech. Týden 5.-11.2.2007 charakterizuje období před zavedením greylistingu MU a týden 5.- 11.3.2007 období těsně po zavedení greylistingu.

Řádek „doručené zprávy“ udává celkových počet e-mailů, které centrální poštovní server MU uspěšně odeslal kterýmkoli směrem – dovnitř MU nebo ven z MU. Nedoručené (AV ochrana) jsou zprávy přicházející do univerzity, které nejsou doručeny, protože obsahují počítačový vir nebo spustitelnou přílohu, které se do MU nedoručují [2]. Nedoručené (neexistují uživatel) jsou zprávy, které byly adresovány na neexistující uživatele – například spamy generované slovníkovou metodou. Nedoručené (ostatní chyby) jsou všechny ostatní zprávy, které nebylo možné z jiných důvodů doručit. Nedoručené (greylisting) se vyskytují až po zavedení greylistingu a zahrnují pokusy o předání zprávy, které byly odmítnuté metodou greylistingu (viz popis greylistingu ve [1]).

2 Situace kolem spamu na fakultách

V průběhu měsíce února byl proveden mezi laboratořemi výpočetní techniky (LVT) jednotlivých fakult dotazníkový průzkum zaměřený na problematiku spamu a její závažnost v rámci fakult MU.

Ze šetření vyplynulo, že všude je prováděna filtrace spamu na úrovni fakultních poštovních serverů – nejčastěji s využitím antispamového nástroje Spamassasin (na dvou fakultách i v kombinaci s dalšími filtry jako je dSpam). Individuálně v některých případech je navíc využívána antispamová kontrola v klientských poštovních programech uživatelů. Podpora koncovým uživatelům při nastavování a ladění jejich osobních filtrů je poskytována obvykle jen na vyžádání.

Nastavení antispamových nástrojů se na jednotlivých fakultách výrazně liší v závislosti na zvyklostech správců a uživatelů. Rovněž se liší hodnocení závažnosti problematiky spamu a obecné úspěšnosti jejího řešení na jednotlivých fakultách či pracovištích. LVT hodnotily situaci na svých fakultách v rozmezí od relativně dobrá až po velmi vážná; přičemž situaci jako vážnou až velmi vážnou hodnotili zástupci 5 fakult.

Přestože účinnost samotných fakultních antispamových filtrů je ze strany správců hodnocena vesměs jako velmi dobrá, vnímá většina LVT spam jako závažný problem a boj se spamem pro ně představuje značnou zátěž. Navíc ani vysoká účinnost fakultních filtrů nemusí nutně znamenat dostatečnou antispamovou ochranu na individuální úrovni u všech uživatelů. V závislosti na charakteru pošty, způsobu jejího využívání a dalších okolnostech může být situace u jednotlivých uživatelů značně rozdílná.

3 Greylisting MU a jeho přínosy

Od 1. března 2007 bylo na centrálním poštovním serveru MU nasazeno celouniverzitní antispamové opatření v podobě tzv. greylistingu

Denní počet zpráv	5.–11.2.	5.–11.3.
Doručené zprávy	387 833	74 105
Nedoručené (AV ochrana)	11 995	2 853
Nedoručené (neexistující uživatel)	216 966	188 440
Nedoručené (ostatní chyby)	272 971	102 642
Nedoručené (greylisting)	—	1 340 654

Tabulka 1: Objem pošty MU před a po greylistingu

[1]. Cílem tohoto opatření bylo snížit celkovou zátěž přinášenou spamy na univerzitní poštovní infrastrukturu (nároky na výpočetní a paměťové kapacity fakultních a dalších poštovních serverů) a současně i snížit počet spamů u koncových uživatelů.

Centrální poštovní server MU relay.muni.cz tak v současnosti provádí již dva typy filtrování elektronické pošty:

- *antivirová ochrana* – filtrují se zprávy obsahující počítačové viry a přílohy vybraných typů, jejichž přijímání na MU je z důvodů antivirové ochrany zakázáno [2];
- *antispamová ochrana* – filtrují se zprávy které nejsou doručovány podle standardních pravidel pro rozesílání elektronické pošty.

Podívejme se, jak se aplikace greylistingu na centrálním poštovním serveru MU projevila na množství e-mailových zpráv doručovaných na jednotlivé fakultní servery. V tabulce 2 jsou uvedeny denní průměry počtu doručovaných zpráv na jednotlivé fakulty v týdnu 5.2.-11.2.2007 (před zavedením greylistingu) a v týdnu 5.3.-11.3.2007 (po zavedení greylistingu).

Uvedená tabulka vypovídá o poklesu celkového množství doručované pošty o 80 % až 90 %. Můžeme předpokládat, že tento rozdíl je – až na výjimky – tvořen nedoručováním elektronických zpráv obsahujících spam.

Další zajímavý údaj – kolik spamu je i po zavedení greylistingu na fakultní stroje doručováno – není už tak snadné zjistit. Jisté vodítko může ale poskytnout záznam z antispamového nástroje Spamassasin na serveru dior.ics.muni.cz pro poštu ÚVT MU. Na základě především analýzy obsahu označuje Spamassassin přijímanou poštu jako spam nebo normální poštu. V následující tabulce jsou vidět denní statistiky ze Spamassissinu ÚVT MU ze stejných týdnů jako v předchozí tabulce (před zavedením greylistingu a po něm).

a) ÚVT MU – stav před zavedením greylistingu:

Den	Spam	Normální	Podíl spamu
PO 5.2	8834	3474	72 %
ÚT 6.2	8188	3588	70 %
ST 7.2	8584	4024	68 %
ČT 8.2	8966	3650	71 %
PÁ 9.2	8376	3174	73 %
SO 10.2	7895	2124	79 %
NE 11.2	7769	2014	79 %

b) ÚVT MU – stav po zavedení greylistingu:

Den	Spam	Normální	Podíl spamu
PO 5.3	539	2102	20 %
ÚT 6.3	606	1807	25 %
ST 7.3	630	1921	25 %
ČT 8.3	579	2055	22 %
PÁ 9.3	671	1635	29 %
SO 10.3	519	713	42 %
NE 11.3	521	741	41 %

Před nasazením greylistingu byly přibližně tři čtvrtiny kontrolované pošty rozpoznány Spamassassinem jako spam. Po zavedení greylistingu se tento podíl snížil na jednu čtvrtinu v pracovní dny (o víkendu se poměr vzhledem k nižšímu počtu normální pošty mění). Zavedením greylistingu rovněž poklesl počet zpráv označených jako normální pošta. Pravděpodobně se jedná o spam, který nástroj Spamassasin nerozpoznával, což je potřeba při interpretaci uvedených čísel brát v úvahu.

Uvedené údaje vypovídají o dvou vybraných týdnech a mapují skokový rozdíl způsobený zavedením greylistingu. Na jejich základě se greylisting jeví jako velmi účinná součást protispamových opatření. Pro přesnější vyhodnocení účin-

Denní počet zpráv	Před greylistingem	Po greylistingu	Pokles počtu zpráv
PřírF	53 999	8 303	85 %
FI	48 321	8 187	83 %
PedF	31 225	3 030	90 %
FF	29 120	3 637	88 %
LF	23 663	3 352	86 %
ÚVT	20 557	3 968	81 %
FSS	17 092	3 060	82 %
ESF	10 261	1 407	86 %
PrávF	8 798	1 233	86 %
Rektorát	7 041	1 246	82 %
FSPS	5 931	953	84 %
SKM	1 571	237	84 %

Tabulka 2: Denní průměrné počty e-mailů dle fakult

nosti bude třeba sledovat vývoj v rámci delšího časového období.

Dva týdny po nasazení greylistingu na centrálním poštovním serveru MU byl u fakultních LVT dotazníkovou formou ověřen výsledek opatření. Podle přijatých odpovědí byl na jednotlivých fakultách zaznamenán úbytek přijímaného spamu o 80 % až 90 %. Současně na nebyly na většině fakult zaznamenány zásadní stížnosti ze strany uživatelů na změny v chování poštovního systému (zpoždění v doručování zpráv z neznámých adres nebo nedoručení očekávané zprávy). V jednom odůvodněném případě byly vybrané e-mailové adresy vyňaty z režimu greylistování; šlo o adresy používané pro potřeby trvalých rychlých odpovědí v rámci speciálního výzkumu.

4 Závěr

Dá se předpokládat, že s tím, jak bude větší část spammerů nacházet účinné protizbraně, bude význam greylistingu v budoucnu slábnout. A bude třeba hledat nová opatření. Nicméně v současné době umožňuje greylisting – spolu s pokračujícím filtrováním a protispamovými opatřeními na úrovni fakult i jednotlivých uživatelů – udržet systém elektronické pošty v chodu a ve stavu únosném pro uživatele MU.

Literatura

[1] M.Ruda. *E-mail a centrální poštovní server Masarykovy univerzity*. Zpravodaj ÚVT MU. ISSN 1212-0901, 2007, roč. XVII, č. 4l

[2] ÚVT MU. *Pravidla pro přijímání pošty v doméně muni.cz*. Dostupné na `http://www.ics.muni.cz/techinfo/abuse.html`