Antivirová ochrana v elektronické poště na MU

Miroslav Ruda, ÚVT MU

V souvislosti se stále rostoucím počtem virových útoků přicházejících na MU prostřednictvím elektronické pošty vypracoval Ústav výpočetní techniky MU systém celouniverzitní ochrany před viry šířenými touto cestou. Systém byl připraven k nasazení v polovině března t.r. a v době vyjití tohoto článku již by měl být ve spolupráci s fakultními LVT implementován na celé univerzitě.

Systém předpokládá antivirovou kontrolu veškeré elektronické pošty přicházející do Masarykovy univerzity a pošty odcházející z domény muni.cz. Kontrola se bude týkat jak veškeré pošty přicházející ze světa, tak také pošty mezi jednotlivými fakultami a ústavy.

Po zvážení a otestování více alternativ navrhl ÚVT *centrální model*, kdy veškerá antivirová kontrola elektronické pošty je prováděna pouze na vstupním uzlu MU (počítači relay.muni.cz). Přitom však jednotlivé fakulty a ústavy mají možnost definovat, jak se má zacházet se zavirovanými dopisy pro jejich uživatele. Vedle základních možností (zavirovaný dopis vrátit nebo propustit dál s varováním) je implementována i taková možnost, kdy dopis je pouze označen a rozhodnutí o způsobu zacházení se zavirovanou poštou je odloženo až na dobu doručení do uživatelova mailboxu. Tento přístup umožňuje, aby ve vybraných doménách mohli uživatelé sami rozhodovat o tom, kterou variantu zacházení se zavirovanou poštou budou preferovat. V takových případech však uživatel nese plnou odpovědnost za následky případné virové nákazy v situaci, kdy měl antivirovou ochranu „vypnutu“ (a přitom by bylo možné s jejím využitím virové nákaze předejít).

Základní principy navrhovaného řešení

Současný stroj relay.muni.cz bude postupně nahrazen několika PC na platformě Linux, mezi něž bude automaticky rozdělována zátěž při zpracování elektronické pošty tak, aby bylo dosaženo požadované propustnosti a antivirová kontrola nenarušovala ani ve špičkách provoz pošty na MU. Současně tím bude dosaženo i potřebné odolnosti proti případným výpadkům technického zařízení.

Provoz systému se řídí následujícími pravidly:

- příchozí dopis se kontroluje antivirem pouze tehdy, je-li jeho příjemce z domény muni.cz (relay.muni.cz slouží jako poštovní server i pro další domény)
- podle výsledků antivirových testů je do el.dopisu přidána hlavička

  X-Muni-Virus-Test: Clean – žádný virus nenalezen

  X-Muni-Virus-Test: Found – dopis (jeho příloha) obsahuje virus

  X-Muni-Virus-Test: Suspicious – heuristická analýza antiviru označila dopis jako podezřelý

- další zacházení s dopisem závisí na dohodě s příslušnou fakultou či organizační jednotkou univerzity a může nabývat některé z následujících podob:

  1. zavirovaný dopis je na úrovni celouniverzitního poštovního serveru *odmítnut*; příjemci i odesílateli je zasláno upozornění na pokus o doručení zavirovaného dopisu (nikoliv však dopis samotný)
  2. dopis po označení *prochází dál bez dalších změn*. Administrátoři subdomény nainstalují další nástroje pro ochranu uživatelů na základě hlavičky X-Muni-Virus-Test (viz. část Procmailová pravidla dále v tomto textu) na příslušný fakultní server
  3. zavirovaný dopis *prochází dál v upravené podobě*, a to tak, že v jeho první části je varování o tom, že dopis obsahuje virus, a pak následuje původní zavirovaný dopis (korektně zabalený do MIME hlaviček). Je na uživateli, zda dopis sám smaže nebo zda si jej odviruje a poté přečte. I v této variantě je možné použít další procmailová pravidla na fakultní úrovni.

– pro komunikaci mezi fakultami platí stejná pravidla
– u všech dopisů odcházejících z domény muni.cz se antivirová kontrola provádí, v případě nalezení viru se dopis vždy vrací odesílateli. Příjemci se v tomto případě upozornění neposílá.

Procmailová pravidla

V případě, že se fakulta rozhodne zavirovanou poštu apriori neodmítat, ale požaduje propustit ji v některé z výše uvedených podob dál na fakultní úroveň, připravilo ÚVT procmailová pravidla, která použijí hlavičku X-Muni-Virus-Test pro detekci zavirovaného dopisu a podle konfigurace zvolené fakultou dopis s virem dále zpracují. Fakultní LVT jsou v tomto případě zodpovědná za korektní instalaci a údržbu procmailových pravidel na fakultních serverech a podporu uživatelům při realizaci jejich osobních nastavení.

Je připraveno 5 variant zacházení se zavirovanou poštou, z nichž si uživatel může zvolit tu, která je pro něj optimální:

1. zavirovaný dopis se „zahodí“
2. zavirovaný dopis se „zahodí“ a odesílatel obdrží varování
3. zavirovaný dopis se uloží do speciálního mailboxu
4. zavirovaný dopis se uloží do speciálního mailboxu a příjemce obdrží krátké oznámení
5. zavirovaný dopis se uloží do uživatelova mailboxu beze změn, stejně jako kterýkoli jiný.

Možnosti fakult a uživatelů

Každá fakulta nebo ústav s poštovním serverem má možnost zvolit si metodu, jak se bude zacházet se zavirovaným dopisem pro jejich uživatele. V případě, že si zvolí metodu, kdy je dopis propuštěn beze změn dále, musí nainstalovat připravená procmailová pravidla. Je opět na správcích subdomény (resp. vedení fakult/ústavů), které procmailové pravidlo zvolí jako standardní a zda umožní uživatelům volbu jiné varianty.

Aktuální nastavení antivirových pravidel a ukázky dopisů při zamítnutí či přijetí zavirované pošty viz `http://www.ics.muni.cz/services/security/index.html`.

Spam

S novou konfigurací poštovního serveru relay.muni.cz je nabízen i další nástroj pro zamezení přijímání nevyžádané pošty (SPAMu) pomocí celosvětových „černých listin“ strojů, které rozesílání spamu dovolují. Centrální poštovní server MU nebude poštu od těchto strojů automaticky odmítat, ale ke každému přijatému dopisu přidá hlavičku X-Muni-Test-IP, která bude obsahovat IP stroje, ze kterého pošta přišla. Tím umožníme uživatelům (nebo fakultám, kde správci rozhodnou, že takové chování bude standardní) spam snadno odfiltrovat.

ÚVT dodá další procmailové pravidlo, které při ukládání dopisu do mailboxu kontaktuje příslušnou databázi spammerů a podle IP v hlavičce detekuje, zda jde o poštu ze stroje, který rozesílá spam. Pravidlo opět umožní dopis smazat nebo uložit do jiného mailboxu. □