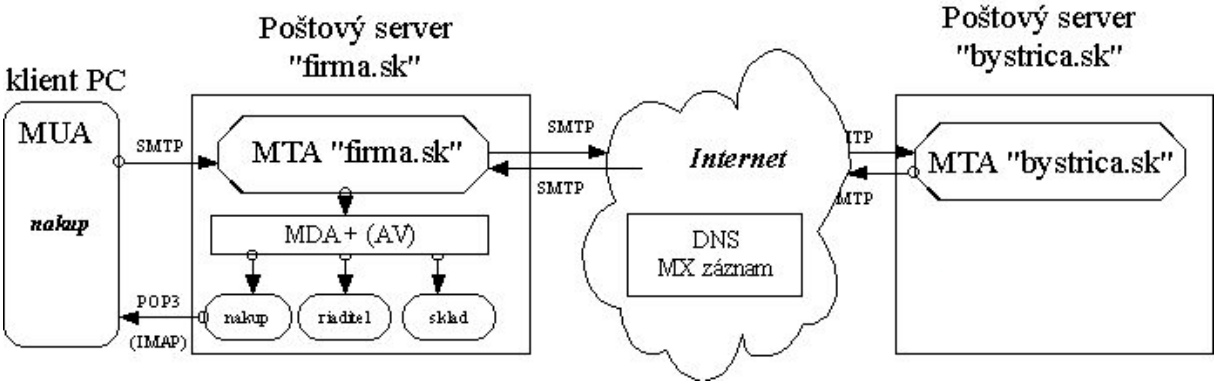
Linux prakticky ako server / 27.časť
(priame doručovanie pošty a procmail)

V minulej časti sme si vytvorili vlastný poštový server na báze postfixu, ktorého úlohou bolo nielen poštu vysielať, ale aj poštu prijímať, a to všetko protokolom SMTP. Náš server sa stal vo svete Internetu verejne známym, a to doslova a do písmena – má priradenú doménu, verejnú IP adresu a platný MX záznam v DNS súboroch. Po prevzatí poštu rozdelí sám postfix. Že sa to dá urobiť aj inak, to si dnes ukážeme.

Procmail
Už v predchádzajúcich častiach sme si hovorili, že samotný program postfix nemá veľmi silné možnosti na manipuláciu s prijatou poštou. Pre zložitejšie operácie sa používa určitý program MDA, ako je napríklad program procmail.
A ukázali sme si, ako spojiť program procmail s programom fetchmail.
Pri variante s priamym doručovaním pošty sa však program fetchmail nepoužíva a preto je program procmail nutné zviazať nejako s programom postfix.

Na obrázku č.1 je schéma nášho poštového servera v spojení s MDA programom procmail:



Princíp činnosti
Pošta z Internetu bude prijatá programom postfix za pomoci protokolu SMTP. Ten ju však neuloží do jednotlivých poštových schránok používateľov, ale ju odovzdá na ďalšie spracovanie programu procmail.
Potom procmail podľa nastavených konfiguračných súborov *procmailrc* alebo *.procmailrc* vykoná požadované operácie a poštu doručí (alebo ju zahodí – ak je potreba) do používateľských poštových schránok.
Odtiaľ si ju môžu jednotliví používatelia vyzdvihnúť protokolom POP3 alebo IMAP do svojich poštových klientov MUA.

Nastavenie postfixu pre prácu s programom procmail
Ako však posftix bude vedieť, že nemá poštu doručovať sám, ale ju má odovzdať procmailu?
To musíme nastaviť v konfiguračnom súbore *main.cf*!
Vyhľadáme direktívu ***mailbox_command***, ktorá je štandardne prázdna.
Napíšeme

```
mailbox_command = /usr/bin/procmail -a $DOMAIN -d $LOGNAME
```

a súbor uložíme.
Potom už len stačí vytvoriť príslušné konfiguračné súbory *procmailrc* alebo *.procmailrc* tak, ako sme si to ukázali v predchádzajúcich častiach.

A máme hotovo!
Odteraz bude pošta prechádzať nielen programom postfix, ale aj programom procmail. A na základe konfiguračného súboru programu procmail môže správa ešte pokračovať cez rôzne antivírové a antispamové programy (ukážeme si nabudúce).

Ešte predtým, ako sa pustíme do čistej antivírovej a antispamovej kontroly, dokážeme pomocou určitých direktív zlepšiť činnosť samotného programu postfix.

Ďalšie nastavenie programu postfix
Dnes si ešte ukážeme pár trikov na nastavenie programu postfix. Tieto triky využívajú direktívy konfiguračného súboru *main.cf*. Vhodným nastavením získame „veľa muziky za málo peňazí“.

Jednoduchá ochrana pred vírusmi
Aj bez antivírového programu – či už komerčného alebo free – sme schopní nastaviť akú – takú ochranu pred šírením vírusov. Hovorím „ochranu“, lebo nejde o antivírovú kontrolu v pravom slova zmysle.
Veľmi často sa stáva, že sa vírusy šíria v prílohe elektronickej pošty, hlavne v takých, ktoré majú príponu .exe, .pif, .lnk, .vbs a iné, ktoré dokážu niektoré poštové programy automaticky spustiť, a tým aj zavíriť celý počítač. Preto vytvoríme filter, ktorý nedovolí odoslať ani prijať poštu, v ktorej je ako príloha (attachment) súbor s uvedenými príponami.

Na vytvorenie spomínaného filtra využijeme direktívy konfiguračného súboru *main.cf*, a to položku ***header_checks*** a ***body_checks***.
Editujeme súbor *main.cf* a doplníme:

```
header_checks = pcre:/etc/postfix/header_checks
body_checks = pcre:/etc/postfix/body_checks
```

Direktíva *header_checks* určuje výraz, ktorý sa má hľadať v hlavičke správy. Podobne direktíva *body_checks* určuje výraz, ktorý sa má hľadať v tele správy.

Zápis */etc/postfix/header_checks* je súbor, ktorý obsahuje regulárne výrazy. Zápis *pcre* je forma tabuľky, konkrétne *Perl Compatible Regular Expression*, v ktorej bude daný súbor uložený.
Všeobecný zápis v tomto súbore má tvar

```
/regulárny výraz/ REJECT text
```

„Text“ sa vloží do skontrolovaného chybového mailu, ktorý sa vráti odosielateľovi ako nedoručiteľný. Prehľadávanie výrazov sa končí, ak sa nájde vyhovujúci výraz alebo na konci súboru s regulárnymi výrazmi.

Príklad regulárneho výrazu
Predstavme si, že by sme chceli odfiltrovať maily, ktoré majú vo svojej hlavičke text „Re: login“. Do súboru /etc/postfix/header_checks by sme zapísali takýto regulárny výraz:

```
/^Subject:\s+Re: login/ REJECT Prepacte, text v sprave je typicky pre internetove virusy
```

Po prijatí správy postfixom bude kontrolovaná hlavička správy, či neobsahuje zápis Re: login*. Ak sa takýto zápis nájde, správa bude vrátená odosielateľovi s textom* Prepacte, text v sprave je typicky pre internetove virusy.

Vráťme sa ale k nášmu nastaveniu:
V tomto našom prípade môžeme povedať, že obidva súbory */etc/postfix/header_checks* aj */etc/postfix/body_checks* budú rovnaké.
(Môžeme vytvoriť len jeden súbor a dať ho do obidvoch direktív, alebo vytvoríme symbolickú linku na ten druhý. Ak to nevieme, jednoducho okopírujeme súbor a jeden pomenujeme ako *header_checks* a druhý ako *body_checks*)

Obsah súboru bude takýto (je prevzatý z Internetu – od „vixa“) – výpis č.2:

```
/^begin \d\d\d .*\.(hta|cpl|vbe|vbs|exe|com|jb|bat|pif|scr|lnk|cmd)/ REJECT
Message content rejected; we do not accept executable attachments.
/^Content-
(Disposition|Type)\:.*name="?.*\.(hta|cpl|vbe|vbs|exe|com|jb|bat|pif|scr|lnk|cmd)
"?/ REJECT Message content rejected; we do not accept executable attachments.
/^\s*(file)?name="?.*\.(hta|cpl|vbe|vbs|exe|com|jb|bat|pif|scr|lnk|cmd)"?/ REJECT
Message content rejected; we do not accept executable attachments.
/^Subject:.*your account/ REJECT Message content rejected; message has subject
typical for viruses!
```

```
/The message cannot be represented in 7-bit ASCII encoding and has been sent as a
binary attachment./ REJECT Message content rejected; found text typical for
viruses.
/The message contains Unicode characters and has been sent as a binary
attachment./ REJECT Message content rejected; found text typical for viruses.
/Mail transaction failed. Partial message is available./ REJECT Message content
rejected; found text typical for viruses.
```

Poznámka:
Ak sa nám ho nechce odpisovať, môžeme si ho stiahnuť z www.cevaro.sk/download.

Regulárne výrazy sú pomerne ťažké pre linuxového začiatočníka. Ale aj bez dostatočnej znalosti prípadne dokážeme uvedený súbor s regulárnymi výrazmi upraviť pre naše potreby. Jedná sa hlavne o texty, ktoré budú odosielateľovi zaslané v nedoručiteľnej pošte.

Po úprave súboru nesmieme zabudnúť reloadnuť postfix, napríklad príkazom **service postfix reload**.
Vykonáme skúšku tak, že si sami sebe pošleme mail, v ktorom bude ako príloha súbor s nebezpečnou príponou a následne mail s neškodnou príponou.
Ak všetko funguje ako má, pokročili sme zase o jeden stupienok vyššie.

Treba spomenúť, že tento filter odstráni každý súbor s nebezpečnou príponou! On nevie, či je súbor naozaj škodlivý alebo nie! Nedokáže urobiť analýzu súboru na vírusy a iné červy, on len kontroluje meno prípony. Preto musíme svojich používateľov a klientov vycvičiť, aby ani neškodné súbory nezasielali s nežiadúcimi príponami.
Ak sa už naozaj nemôžeme vyhnúť odoslaniu súboru s nebezpečnou príponou, je tu ešte možnosť, že súbor premenujeme a do tela správy napíšeme adresátovi poznámku, prečo sme tak urobili. V takom prípade súbor filtrom prejde a príjemca si súbor premenuje ručne naspäť. Tým zabránime, že sa automaticky spustí na základe prípony sám, čo by mohol napáchať nejakú škodu.

Obmedzenie spamu
Ani tentokrát nepôjde o čisto antispamovú kontrolu pošty (tú ozajstnú si ukážeme nabudúce). My sa len budeme snažiť pomocou nastavenia konkrétnych direktív zabrániť šíreniu potencionálneho spamu.

Na to využijeme tieto direktívy súboru *main.cf*:

- *local_recipient_maps*
- *disable_vrfy_command*
- *disable_vrfy_command*

Prejdime si jednotlivé direktívy:

local_recipient_maps
Veľmi často sa stáva, že spammer cvične zašle určitý mail na určitú doménu. Keď mail príde neexistujúcemu príjemcovi, bude vrátený odosielateľovi ako nedoručiteľný, lebo adresát neexistuje.
To môže spammerovi napomôcť a preto tomuto zabránime.
Nastavíme direktívu

```
local_recipient_maps = $alias_maps unix:passwd.byname
```

čím odmietneme prijímanie pošty pre neexistujúcich používateľov ešte počas príjmu (vôbec sa neprijme a tak sa nevygeneruje ani mail o neexistujúcom používateľovi.
Táto direktíva určuje tabuľku používateľov, pre ktorých sa pošta prijíma, v tomto prípade je to súbor */etc/passwd*.

Pozor!
Ak služba SMTP používa chroot, musíme súbor /etc/passwd skopírovať do adresára, kam má postfix prístup, a to pri každej jeho zmene!

disable_vrfy_command
Ďalším vhodným opatrením je nastavenie direktívy ***disable_vrfy_command***. Príkaz VRFT protokolu SMTP slúži na zisťovanie existencie poštovej schránky.

Toto zakážeme nastavením

```
disable_vrfy_command = yes
```

čím zabránime spammerovi otestovať existenciu či neexistenciu poštovej schránky.

maps_rbl_domains
Internetová komunita sa snaží proti spammerom brániť. Preto vznikol zoznam spammerov a serverov, cez ktoré je možné spam úspešne šíriť. Tak sa spammeri ocitli takpovediac na „čiernej listine“. A naozaj, týmto zoznamom sa hovorí ***blacklist***.
Postfix je schopný v reálnom čase skontrolovať, či sa odosielateľ nachádza na niektorej čiernej listine. To dosiahneme nastavením direktívy ***maps_rbl_domains***, za ktorú uvedieme zoznam internetových adries s blacklistami, ktoré chceme skontrolovať.
Takže zadáme napríklad

```
maps_rbl_domains = sbl.spamhaus.org, block.blars.org, opm.blitzed.org
```

Jednotlivé adresy zapisujeme do jedného riadku a položky oddeľujeme čiarkou.
Treba povedať, že blacklistov je veľmi veľa a ich ucelenejší zoznam nájdeme na adrese http://www.declude.com/Articles.asp?ID=97.
Nedávajme do tejto direktívy veľa blacklistov, pretože by kontrola bola veľmi časovo náročná a trvala by dlho, čím by sa zaťažovala linka a tak by sa spomaľovala celá pošta a aj sieť.

Pozor!
Kľudne sa nám môže stať, že ak my dobre nezabezpečíme náš poštový server a stane sa open relay, teda že cez neho môže ktokoľvek poslať poštu, objavíme sa (teda naša IP adresa) na niektorom zozname z blacklistov! Preto ak nám odosielanie nefunguje správne a predsa sme presvedčení, že je všetko riadne nastavené, problém môže byť v tom, že sme niekde na „čiernej listine“.

Kanonické adresy
Podstata tvorby prihlasovacích mien do Linuxu nedovoľuje, aby sme vytvorili používateľa s menom napríklad *Miroslav.Oravec*. A cez to všetko by bolo naozaj dobré, keby som mohol používať adresu elektronickej pošty v tvare napríklad *Miroslav.Oravec@firma.sk*. Tomuto zápisu hovorievame aj kanonické mená.
Uznajte, že často používaná konvencia „prvé písmeno+priezvisko“ môže spôsobiť zámenu osôb, tak ako v mojom prípade tvar *moravec* či inú veselú alebo menej veselú kombináciu.
A tak pomocou direktívy ***canonical_maps*** a príslušných databáz môžeme spôsobiť, že sa môj login *moravec* v hlavičke odchádzajúceho mailu prevedie na *Miroslav.Oravec* a naopak. Za príklad si môžeme vziať aj imaginárneho Stanislav Omara, ktorý tiež by chcel radšej používal zápis *Stanislav.Omar* namiesto ako trochu smiešneho zápisu *somar@firma.sk* (a nedajbože by to bol ešte k tomu aj náš šéf...).

Najprv v direktíve *canonical_maps* určíme databázu s kanonickými menami, napríklad takto:

```
canonical_maps = hash:/etc/postfix/canonical
```

Potom do súboru */etc/postfix/canonical* napíšeme:

moravec	miroslav.oravec
somar	stanislav.omar

Aby sme z tohto čisto textového súboru vytvorili postfixovú databázu typu *hash*, musíme spustiť z príkazového riadku príkaz

```
[root@rubin spool]# postmap /etc/postfix/canonical
```

Aby dochádzalo aj k spätnému prekladu, teda že pošta v tvare *Miroslav.Oravec@firma.sk* bude doručená používateľovi *moravec*, vytvoríme nám už známu tabuľku ***aliases***, napríklad tak, že do súboru */etc/postfix/aliases* napíšeme toto:

miroslav.oravec:	moravec

stanislav.omar:	somar

a spustíme príkaz

```
[root@rubin spool]# newaliases
```

Nakoniec postfix *reloadneme*.

Aby to celé fungovalo, musia používatelia *moravec* a *somar* v systéme naozaj existovať.
Treba si zapamätať, že po tejto úprave už nebudeme schopní odoslať poštu v tvare ***moravec@firma.sk***, lebo sa VŽDY hlavička zamení za ***miroslav.oravec@firma.sk***.
(teda dá sa to pomocou prepisovacích máp, ale o tom inokedy...)

To by na dnes stačilo a aj nabudúce sa budeme venovať antivírom a antispamom a pošte, ale tentokrát v spojení s čítaním pošty cez Internet. Tiež vás napadá, ako to efektívne vo firme či škole využiť?

Miroslav Oravec