Vírusellenőrzés a levelezőkiszolgálón

Az Amavis program segítségével elektronikus levelekhez csatolt vírusoktól szabadulhatunk meg.

A levelezőkiszolgálón futó Amavis program, ellenőrzi az átmenő leveleket, lecsatolja a mellékleteket, és egy külső vírusirtó programot futtat rajtuk. Amennyiben vírust észlel, értesíti a kiszolgáló postamesterét, a levél feladóját és a címzettet is. Ilyen esetben az eredeti levél kézbesítését a kiszolgáló megtagadja.
A program használatával sem kerülhető el azonban az ügyfeleken futó vírusirtó alkalmazása, hiszen vírusokat nem csak levelek útján kaphatunk. Ennek ellenére nagyobb biztonságban érezhetik magukat a rendszergazdák és a felhasználók, ha a felismert vírusos levelek az ügyfélgépekig el sem jutnak.
A program telepítése nem egyszerű, de ha összeszedtük a működéséhez szükséges összetevőket és egyéb alkalmazásokat, gyorsan működésre bírható, és karbantartást sem igényel. A telepítés menetét Debian 2.2-es rendszerre írom le. Mivel az Amavis programot Perlben írták, működése csaknem rendszerfüggetlen.

Az Amavis program lelőhelye ➲ http://www.amavis.org/

Előkészületek

Első lépésként szedjük össze az összes szükséges programot. Töltsük le az Amavis-Perl programot
`wget http://www.amavis.org/dist/perl/amavis-perl-11.tar.gz` paranccsal és csomagoljuk ki a */usr/src* könyvtárba:

```
cd /usr/src; tar -xzvvf
  ➥/home/peter/packages/amavis-perl-11.tar.gz
```

Az Amavis-Perl néhány olyan Perl-modulra támaszkodik, amely valószínűleg nincs a rendszerünkön. Kényelmes telepítésükhöz használjuk a Perl CPAN-modulját. Rendszergazdaként írjuk be:

```
perl -MCPAN -e shell
```

Ha hibaüzenetet látunk, töltsük le a CPAN-modult, csomagoljuk ki a */usr/src* könyvtárba és telepítsük:

```
make
make install UNINST=1
```

Az alábbi utasítás kiadása után

```
cd /usr/src; tar -xzvvf
  ➥/home/peter/packages/CPAN-1.59.tar.gz
cd CPAN-1.59
```

itt adjuk ki a

```
perl -MCPAN -e shell
```

parancsot. A megjelenő kérdésekre általában elegendő az ENTER megnyomásával válaszolnunk, kivéve azokra, amelyek a hozzánk közeli tükörkiszolgálót választják ki. Értelemszerűen válasszuk először Európát, majd Magyarországot. Ha sikerült a beállítás, megjelenik a `cpan>` parancssor. Ekkor kezdhetjük el az Amavis README! fájljában leírt Perl-modulok telepítését az `install` *`modulnév`* parancs beírásával. A következőket kell beírnunk:

```
install Unix::Syslog
install Convert::Uulib
install Convert::TNEF
install Compress::Zlib
install Archive::Tar
install Archive::Zip
install G/GB/GBARR/MailTools-1.15.tar.gz
install MIME::Tools
install Bundle::libnet
```

A vírusirtó telepítése

Az Amavis-csomag súgójában olvashatunk a használható vírusirtókról. Én a Sophos vírusirtóját választottam. A Sophos cég által készített csomag sajnos (mint a legtöbb víruskereső program) fizetős, ezért a cég webhelyéről egy csökkentett változatot tudunk letölteni. Ez a változat ugyanúgy megtalálja a vírusokat, de nem távolítja el azokat. Egy nagyobb cégnél ma már elengedhetetlen, hogy komoly vírusvédelem legyen. Töltsük le a programot a ➲ http://www.sophos.com/downloads/products/unix_506.html címről. Linuxhoz libc5-ös és libc6-os változattal működőt is találhatunk. Próbáljuk ki a libc5-öshöz tartozót, ami a ➲ http://downloads.us.shopos.com/products/full/linux.intel.libc5.tar.Z címen érhető el. Letöltés után az `uncompress` paranccsal csomagoljuk ki, majd a `tar` paranccsal irányítsuk az *src* könyvtárba:

```
cd /usr/src; tar -xvvf
  ➥/home/peter/packages/linux.intel.libc5.tar
```

Váltsunk át a létrejött ***sav-install*** könyvtárba, olvassuk el az ***install.txt*** és ***readunix.txt*** fájlokat.
A `./install.sh -v -ni` paranccsal lehet telepíteni. Ha a

Az OpenAntivirus projekt honlapja: ➲ http://openantivirus.prg

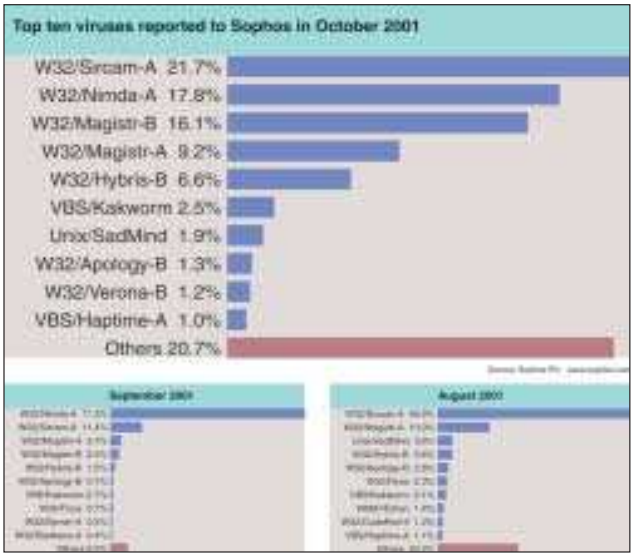
Az Amavis által küldött értesítés vírusos levélről

A Sophos Anti-Virus weboldala ➲ http://www.sophos.com/

`-ni` kapcsoló nélkül telepítjük, egy `sweep`-felhasználót kell létrehoznunk, de ne tegyük, mert fölösleges.
A telepítés a `sweep` programot a */usr/local/bin*-be teszi. A vírusmeghatározó fájlok a */usr/local/sav* könyvtárban vannak, havi frissítéssel jelennek meg, a mostani változat a *vdl-3.51.dat* nevet viseli. A program mindig a *vdl.dat* fájlt keresi, úgyhogy a pillanatnyi vírusadatbázisra egy *vdl.dat* nevű közvetett hivatkozás mutat. Az újabb *dat*-fájlok megjelenése előtt is kapunk frissítéseket *ide*-végződésű fájlok képében, ezeket szintén ebbe a könyvtárba kell helyeznünk. A ➲ http://www.sophos.com/downloads/ide/ könyvtárból az összeset egyenként vagy zipfájlba tömörítve tölthetjük le. Válasszuk a zippelt változatot és bontsuk ki a */usr/local/sav* könyvtárba:

```
cd /usr/local/sav; unzip /home/peter/351_ides.zip
```

Rögtön próbáljuk ki a vírusirtót a `sweep` paranccsal. Ha nem adunk meg fájlnevet, a program rögtön segítséget kínál a használatához. Mostanra letöltöttük az Amavis programot, a hozzávaló Perl-modulokat és egy vírusirtót. Még a levelekhez csatolt tömörített állományok kicsomagolásához szükséges programokat kell beszereznünk: ezek a `file`, `arc`, `bunzip2`, `lha`, `unarj`, `uncompress`, `unrar`, `zoo`.
Telepítsük ezeket is. A `file` parancs valószínűleg már elérhető.



A Sophos folyamatosan figyeli, hogy mely vírusok a legaktívabbak

A többi tömörítőprogramra akkor van szükség, ha a levélmelléklet éppen ilyen formátumú. Az `arc` programot nem sikerült Debian-csomag formájában fellelnem az Interneten, forrásból azonban telepíthető. Ha valaki ehhez nem érez kedvet, az Amavis *configure* parancsfájljában tegye megjegyzésbe az 1573-1575-ös sorokat:

```
#if test "x$arc" = "x" ; then
#{ echo "configure: error: Sorry, you need
#arc" 1>&2; exit 1; }
#fi
```

Ezután rátérhetünk az Amavis telepítésére. Lépjünk be a */usr/src/amavis-perl-11* könyvtárba és gépeljük be: `./configure`. Ha sikeresen lefutott, adjuk ki a `make` parancsot. Az eredményt a `make check` paranccsal lehet ellenőrizni. A folyamat sajnos hibával áll le, ha az `arc` programot nem telepítettük, mivel az ellenőrzéshez használt csatolt állomány *arc* formátumú. Ez azonban nem fog gondot okozni, hiszen manapság senki se használ arc-tömörítést. Hozzunk létre egy Amavis nevű felhasználót, ne adjunk neki parancssoros héjat, sőt – biztonsági okokból – a felhasználót tiltsuk le:

```
adduser amavis
chsh -s /bin/false amavis
passwd -l amavis
```

```
make install
```
Ezzel az Amavis telepítése sikeresen befejeződött.

Az Exim program beállítása

Ezt követően a levelezőkiszolgáló programját kell beállítanunk. Debianhoz az Exim települ fel, ezért ennek a beállítását részletezem, de az Amavis leírásában a többi ismert programhoz is találunk ismertetést. Módosítsuk az Exim beállítófájlját (*/etc/exim.conf*):

1. A `trusted_users = mail` részhez írjuk be az Amavis-felhasználót:
```
trusted_users = amavis:mail
```

2. A `TRANSPORT CONFIGURATION` rész elejéhez illesszük:
```
amavis:
driver = pipe
command = "/usr/sbin/amavis -f
  ➥${sender_address} -d ${pipe_addresses}"
prefix =
suffix =
check_string =
escape_string =
# for debugging change return_output to true
return_output = false
return_path_add = false
user = amavis
group = amavis
path = "/bin:/sbin:/usr/bin:/usr/sbin"
current_directory = "/var/amavis"*
```

3. A `DIRECTORS CONFIGURATION` rész elejére pedig az alábbi sorokat írjuk:
```
amavis_director:
condition = "${if eq
  ➥{$received_protocol}{scanned-ok} {0}{1}}"
driver = smartuser
transport = amavis
```

4. A ROUTERS CONFIGURATION rész elejére:
```
amavis_router:
condition = "${if eq
  ➥{$received_protocol}{scanned-ok} {0}{1}}"
driver = domainlist
route_list = "*"
transport = amavis
```

Mivel valószínűleg a nyomda ördöge sem alszik, jól tesszük, ha a fenti példákat az Amavis leírásában található ***README.exim*** fájlból másoljuk ki. Az ellenőrzéshez írjuk be:

```
tail -f /var/log/syslog
```

Indítsuk újra az Eximet (*/etc/init.d/exim restart*) és próbáljunk vírusos levelet küldeni magunknak. Rendes működésnél a naplófájlokban például ilyen üzenettel találkozhatunk:

```
amavis[3900]: Virus found - quarantined as
virus-20011020-084755-3900
```

Ha nincs kéznél vírusos levél, bármilyen vírusos fájl jó, amit csatolt állományként küldhetünk. Ha ilyen sincs, a ➲ http://www.eicar.org/download/eicar.com címről letölthetünk egy fájlt, amely ugyan nem tartalmaz igazi vírust, csupán egy olyan bájtsorozatot, amit a legtöbb vírusirtó vírusként ismer fel.

A vírusadatbázis frissítése

A Sophos frissen tartásához időnként (havi 1-2 alkalommal) egy teljes változatot le kell töltenünk, a legutolsó teljes változat kiadása óta megjelent új vírusokhoz tartozó ***ide*** állományokat tartalmazó zipfájlt pedig napi rendszerességgel .
Nézzünk erre egy bash-héjprogramot, amely a ***README.scanners*** fájlban található példa módosított változata (a sorszámok csak a magyarázat kedvéért kerültek a sorok elejére):

```
1. #!/bin/bash
2. VIRFILE="'sweep -v|/bin/grep 'Product
      ➥version'| /usr/bin/tr -d -c
      ➥[:digit:]'_ides.zip"
3. SOPHOS_URL='http://www.sophos.com/
      ➥downloads/ide/'
4. IDE_PATH='/usr/local/sav'
5. cd $IDE_PATH
6. /usr/bin/wget $SOPHOS_URL$VIRFILE
7. /usr/bin/unzip -q -n $VIRFILE
8. rm -f $VIRFILE
9. chmod 644
```

A 2. sorban a `VIRFILE` változóba az ***ide***-fájlokat tömörítve tartalmazó állomány neve kerül. Ez általában az ***_ides.zip***-re végződik, az eleje pedig a vírusirtó változatszáma. Ezt a változatszámot kapjuk meg, ha a `sweep` programot elindítjuk a `-v` értékkel:

```
peter@mercury:~$ sweep -v
SWEEP virus detection utility
Copyright (c) 1989,2001 Sophos Plc,
www.sophos.com
System time 10:31:40, System date 20 October
2001

Product version: 3.50
Engine version: 2.6
User interface version: 2.03.079
Platform: Linux/Intel
Released: 01 October 2001
```

A kimenet `Product version` szöveget tartalmazó sorából a `tr` paranccsal az összes nem számjegyet tartalmazó karaktert kiszűrjük, így kapjuk meg a ***350_ides.zip*** szöveget. A parancsfájl többi részében `wget`-tel letöltjük a fájlt, `unzip`-pel kicsomagoljuk, töröljük a letöltött fájlt és beállítjuk a fájljogosultságot. A fenti parancsfájlt naponta a crontabból futtathatjuk. Ha a Sophos új változatot ad ki, inkább azt kézzel töltsük le és telepítsük.

Az Amavis egyéb lehetőségei

Vírus észlelésekor levél érkezik a postamesterhez és a feladóhoz. Ha a címzetteket is értesíteni akarjuk, akkor a `configure` parancsfájlt a `--with-warnrecip=yes` értékkel hívjuk meg. Az értesítésekhez tartozó levélmintákat az Amavis könyvtárának ***amavis/notify*** könyvtárában találjuk. Az itt levő ***admin***, ***recip*** és ***sender*** fájlokat a megfelelő óvatossággal módosítva tetszőleges üzenetet készíthetünk.

Borkuti Péter
(borkuti@freemail.hu) matematika-informatika szakos tanár, rendszergazda, informatikus, rendszerépítő és programozó.