Amavis: kako zabraniti određene vrste priloga

Amavis podržava zabranu primanja maila s prilogom (*attachmentom*), i to po određenim kriterijima. Kriteriji mogu biti ekstenzija datoteke, tip datoteke koju vraća naredba *file(1)* ili MIME tip, kojeg svaki mail klijent danas šalje zajedno s prilogom. Na ovaj način možemo osujetiti pokušaje virusa i crva da se sakrivaju preko dvostrukih ili lažnih ekstenzija.

Iako email virusi danas nisu ni približno raširenи kao nekad, potreba zabrane slanja određenih tipova priloga i dalje ostaje.

Podešavanje se radi u Amavisovoj konfiguracijskoj datoteci /etc/amavis/conf.d/20-debian_defaults, odnosno /etc/amavis/conf.d/50-user (gdje možemo navesti vrijednosti koje će vrijediti umjesto *defaultnih*), u varijabli $banned_filename_re. Najčešće, i najlakše ćemo zabraniti prilog prema ekstenziji datoteke:

```
$banned_filename_re = new_RE(qr'.\.(mp3|mp4|wma|wmv|avi)$'i,);
```

Ovime postupkom smo zabranili neke (najčešće) nepoželjne datoteke. Naravno da ovdje možete upisati bilo koju ekstenziju koju želite zabraniti, u dogovoru sa odgovornim osobama i u skladu sa sigurnosnom politikom ustanove.

Ovo nije sve, jer amavis može zabraniti pojedine priloge po tipu, bez obzira na navedenu ekstenziju datoteke. Amavis ovo utvrđuje preko standardne Unix naredbe file(1) [1], koja se ne da zavarati ekstenzijom, nego tip datoteke traži u njenom zaglavlju.

Otkomentirajte sljedeće u amavisd.conf:

```
qr'^\.exe$'i
```

To će zabraniti bilo kakav prilog koji ima izvršnu datoteku, primjerice .com, .exe ili slično.

Nadalje, Amavis može zabraniti prilog prema njegovom MIME tipu, koji se nalazi u zaglavlju svakog maila s prilogom:

```
qr'^application/x-msdownload$'i, # banned MIME type
```

Ovime smo spriječili prolaz svim attachmentima tipa 'application/x-msdownload'. Ovaj tip attachmenta često rabe virusi, kao što
je nekada činio virus Bagle-U.

Pogledajte i članak http://sistemac.carnet.hr/node/188 [2], koji rješava problem sa slanjem "message/partial" priloga.

Nakon prve instalacije Amavisa, jedina podrazumijevana postavka je to da je zabranjeno slanje priloga s dvostrukom ekstenzijom (.txt.pif, doc.exe, ...), što je bio pokušaj nekih virusa da zavaraju korisnika koji bi onda pokrenuo datoteku misleći da se radi o nečem drugom:

```
qr'\.[^.]*\.(exe|vbs|pif|scr|bat|cmd|com|dll)$'i
```

U amavisovoj konfiguraciji su navedeni dodatni primjeri, pa možete konfigurirati svoj sustav po želji. Sve ovisi o vašoj sigurnosnoj politici i potrebama na vašoj ustanovi.

- Logirajte [3] se za dodavanje komentara

pet, 2008-10-31 12:53 - Željko Borš**Vote:** 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/452

Links
[1] https://sysportal.carnet.hr/node/559
[2] https://sysportal.carnet.hr/node/188
[3] https://sysportal.carnet.hr/sysportallogin