Spamassassin: blokiranje spama pomoću vlastitih pravila

U službi pomoći za sistemce zaprimili smo nekoliko praktički jednakih upita, a tiču se spama. Naime, u zadnje vrijeme primjećena je pojačana aktivnost spamera, a zajedničko svim tim spamovima je isti sadržaj, dok se adresa pošiljatelja mijenja. Adrese pošiljatelja su redovito one s institucije, mada ima i adresa od starih korisnika kojih više nema na sustavu. Ovo upućuje na to da se spamer, odnosno njegov softver, prilagođava poslužitelju te pokušava prikazati kao da spam potiče s tog poslužitelja. Na taj način pokušavaju zavarati korisnike tako što se čini da mail potiče od njihovih kolega, te su veće šanse da će spam pročitati.

Blokiranje po IP adresama nema smisla, jer se mijenjaju (vrlo vjerojatno se radi o zaraženom relay računalu negdje u svijetu). Kako se Subject poruke ne mijenja (što ne znači da neće!), probajmo eliminirati problem pomoću SpamAssassinove direktoive "header". U datoteku /etc/spamassassin/local.cf upišite:

```
header ESTATE_SPAM              Subject =~ /\bInternational Real Estate Consulting C
ompany needs/
score ESTATE_SPAM               4.0
describe ESTATE_SPAM            Spam sa subjectom: International Real Estate Consult
ing Company...
```

Ne zaboravite restartati amavis nakon ovoga (/etc/init.d/amavis restart). Također, ukoliko imate amavis, ne trebate imati pokrenut proces spamd (osim ako ga rabite u neke svoje svrhe). Amavis ima sve što je potrebno da SpamAssassin radi, kombinacija klijenta (spamc) i SA daemona (spamd) vam ne treba u standardnoj konfiguraciji.

Nego, što smo postigli upisom gornjih redaka? Svakom mailu koji sadrži tekst unutar kosih crta u svom Subjectu će biti povećan spam score za 4.0 bodova. Zašto odmah ne staviti 10, 20 ili više? Ako napravimo tako, Amavis će mail odmah staviti u karantenu, no što ako nam vlastiti korisnici proslijede taj spam mail s upitom što da učine? Mi taj korisnikov mail onda nećemo ni vidjeti, jer će prijeći granicu $sa_kill_level_dflt (koja je po defaultu 5.0 bodova, ali često je podešeno na 6.3 ili 6.9, i to ne treba smanjivati).

Neki kolege prijavljuju da Subject spamova nije uvijek isti, ali da svi imaju istu adresu u tijelu poruke. SpamAssassin može i tome doskočiti pomoću direktive "body":

```
body SPAM_ADDRESS_1         /\@westeur-consult\.com/
describe SPAM_ADDRESS_1     Spam adresa unutar tijela poruke 1
score SPAM_ADDRESS_1        4.0
```

Dakle, SpamAssassin omogućuje pregled tijela poruka, a sve gore spomenuto vrijedi i dalje, a vrijednost koju ste dodijelili spam scoreu držite nisko kako bi izbjegli lažne pozitive.

- Logirajte [1] se za dodavanje komentara

čet, 2011-03-24 12:43 - Željko Borš**Kuharice:** Linux [2]
Kategorije: Servisi [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (4 votes)

Source URL: https://sysportal.carnet.hr/node/842

Links
[1] https://sysportal.carnet.hr/sysportallogin
[2] https://sysportal.carnet.hr/taxonomy/term/17
[3] https://sysportal.carnet.hr/taxonomy/term/28