Sender Policy Framework - zaštita od SPAM-a

Spam nas prati praktički od prvog poslanog maila, a danas čini većinu mail prometa na Internetu. Srećom, postoje načini kako količinu spama smanjiti, pa i gotovo eliminirati, što svakodnevno i pokušavamo raznim softverskim rješenjima.

Uspješnost je relativno dobra, ali spameri i dalje prate situaciju i pokušavaju na sve načine poboljšati količinu isporučenih neželjenih poruka. U nizu alata i načina borbe protiv spama, pogledat ćemo SPF - *Sender Policy Framework*. Za razliku od uobičajenih načina zaštite, ovog puta usredotočit ćemo se na drugu stranu - nas.

SPF je zamišljen kao autentikacijski sustav: "da, ovaj poslužitelj može slati mail za domenu nesto.hr", dakle ograničava sa kojih se adresa može slati mail koji u adresi pošiljetalja sadrži ime domene. Spameri vole postaviti adresu "MAIL FROM" s nekog poznatog poslužitelja (aol, google) kako bi njihov spam imao veće šanse proći do korisničkog sandučića. Uz pomoć SPF-a štitimo druge od mailova koji navodno stižu s naše domene, a i svoje korisnike koji znaju dobiti mail koji tobože potiče s lokalne domene.

Naše je samo to da postavimo određene zapise u DNS, a od udaljenog poslužitelja ovisi hoće li prihvatiti naše preporuke ili neće. Veliki email provideri sveć dulje vrijeme koriste SPF, jer ne žele da njihove domene postanu raj za spamere. SPF je osmislio Meng Weng Wong sa pobox.com-a, a sam SPF je u međuvremenu postao IETF standard.

Ukoliko je vaš raspon adresa 161.53.X.0/24 i imate dodatnu lokaciju na 193.198.X.128/26, bit će dovoljno da unesete sljedeći zapis u DNS:

```
TXT "v=spf1 mx ip4:161.53.X.0/24 ip4:193.198.X.128/26 ~all"
```

Ovime smo rekli da za našu domenu nesto.hr mail mogu slati samo poslužitelji iz ova dva raspona adresa. Konkretnije, ovaj redak treba upisati u (pretpostavimo da se držite standardnih naziva) datoteku /etc/bind/hosts.db.

Možete ga upisati, primjerice, odmah ispod zapisa MX ili NS:

```
$TTL 3600       ; 1 hour
@             SOA    server hostmaster (
                2013022701 ; serial
                1800       ; refresh (30 minutes)
                600        ; retry (10 minutes)
                604800     ; expire (1 week)
                3600       ; minimum (1 hour)
)
   NS      ns.nesto.hr.
   NS      slave.server.hr.
   A       161.53.X.Y
   MX      10 mojserver.negdje.hr.
   TXT     "v=spf1 mx ip4:161.53.X.128/26 ~all"
```

Ne zaboravite povećati broj "Serial" i restartati bind. Ovdje mogu stati oni nestrpljivi, svoje su

napravili, označili su odlazne mailove svojih korisnika koji sada imaju veću šansu da ne završe u mapi "spam" na nekom udaljemom poslužitelju.

Za sve ostale koje zanima nešto više, čitajte dalje.

SPF je uveden kao TXT zapis unutar DNS-a, koji nema određenu formu, nego je slobodnog oblika. Već je definiran i "pravi" SPF zapis, ali će proteći još neko vrijeme prije nego se počne primjenjivati u svim DNS serverima.

Dakle, zasada je najsigurnije ići na TXT zapis, iako RFC4408 (http://tools.ietf.org/html/rfc4408 [1]) preporučuje da se stave oba oblika (u Bindu 9.4.0 i višem postoji tip zapisa SPF).

Dakle, znamo kako SPF izgleda, no što znače pojedini unosi? Idemo redom:

```
v=spfv1       ina?ica SPF-a, ovdje je to 1
mx            odre?uje tip zapisa, ovo je "mail exchanger", može biti i A i PTR.
ip4           odre?uje IPv4 raspon adresa koje mogu slati mail za vašu domenu
~all          odre?uje "relaksirano" ponašanje, odnosno "soft fail" - omogu?ava dodat
no ispitivanje
```

Da smo stavili "-all", to bi značilo da samo rasponi navedeni ispred mogu slati mail za određenu domenu. Ukoliko to nije slučaj, mail se stopira bez dodatnog ispitivanja. Postoji i varijanta "+all", ali to dopušta slanje maila s bilo kojeg poslužitelja za našu domenu, pa je stoga njena korisnost upitna. I na kraju, postoji i oblik "?all", koji je zapravo neutralni, odnosno testni oblik i znači da se cijeli unos ne treba uvažiti.

Primjeri iz prakse:

```
# host -t txt google.com
google.com descriptive text "v=spf1 include:_spf.google.com ip4:216.73.93.70/31 ip4:2
16.73.93.72/31 ~all"
```

Ovdje se pojavljuje "include" mehanizam, koji zapravo uključuje dodatne domene, odnosno njihova pravila u ovisnosti o kontekstu zapisa. Ne vjerujemo da će vam trebati.

```
#  host -t txt carnet.hr
carnet.hr descriptive text "v=spf1 mx ip4:161.53.123.0/26 ip4:161.53.160.0/24 ip4:193
.198.184.128/26 ~all"
```

CARNet ima prilično jednostavan zapis, iako je to zapravo vrlo dobro, s obzirom da ga većina drugih hrvatskih ISP-ova uopće nema.

Više informacija o SPF-u možete naći na adresi http://en.wikipedia.org/wiki/Sender_Policy_Framework [2] .

Zdravko Rašić

sri, 2013-02-27 13:20 - Zdravko Rašić**Kuharice:** Linux [3]
Kategorije: Servisi [4]
Vote: 4.5

Vaša ocjena: Nema Average: 4.5 (4 votes)

Source URL: https://sysportal.carnet.hr/node/1215

Links
[1] http://tools.ietf.org/html/rfc4408
[2] http://en.wikipedia.org/wiki/Sender_Policy_Framework
[3] https://sysportal.carnet.hr/taxonomy/term/17
[4] https://sysportal.carnet.hr/taxonomy/term/28