Avatud vahendaja

24 aastat tagasi - 09.11.2001 Autor: Hasso Tepper

Käesolevas artiklis räägime natuke meiliserveri probleemist, millele pööratakse liiga vähe tähelepanu. See on olukord, kus meiliserver on avatud vahendajaks (Open Relay).

Avatud vahendaja on meiliserver, mis võtab vastu meile suvalistelt klientidelt Internetis ning saadab need edasi. Võtame näiteks MS Exchange serveri, mis haldab domeeni minu-maja.ee meile. Talle saadetakse meil, mille ümbrikul on saatjaks keegi earnmoneyfast@ yahoo.co.uk ja saajaks mrjones@aol.com. Mitte kuskilt pole võimalik välja lugeda, et tegu on minu-firma.ee kasutajaga. Häälestamata MS Exchange saadabki selle maili rahumeeli mrjones@aol.com aadressile ning teeb seda ka teiste kümnete ja sadade tuhandete meilidega, mis tavaliselt sellele järgnevad.

Tavaliselt arvatakse, et see on ainult serveri haldaja probleem, kas tema server on avatud vahendaja või mitte. Paraku pole see nii.

Probleemid

Serveri haldajale on suurimaks probleemiks see, et serverit läbiv meilide hulk hakkab üsna kiirelt ummistama Interneti ühendust. Kui tegemist on kiire ühendusega, ei pruugi seda esialgu tähelegi panna. Aeglaste ühenduste puhul aga annab see kõvasti tunda ning kehvemal juhul võib ühendus lokaalsetele kasutajatele kasutamiskõlbmatuks muutuda.

Avatud vahendajad on meiliserverid, mille kaudu saadetakse enamus maailmas ringlevast rämpspostist (spam). Taolise serveri leidmine on rämpsposti saatjatele tõeliseks kullaauguks. See võimaldab anonüümselt ning praktiliselt karistamatult saata piiramatus koguses meile. Rämpsposti saamine ei meeldi aga enamusele saajatest. Selle tõttu peetakse maailmas mitmeid "musti" nimekirju serverite kohta, mille kaudu saadetakse rämpsposti.

Mustad nimekirjad

Maailmas on olemas mitmed üsna tugevad organisatsioonid mis võitlevad rämpsposti ja avatud vahendajatega. Nendest tuntuim on SpamCop (http://www.spamcop.net/), mis on kiire ja efektiivne vahend rämpspostituse

tõrjeks.

Teiseks on olemas online nimekirjad masinatest, mis on avatud vahendajad või tegelevad rämpsposti saatmisega. Sellistes nimekirjades olevatest masinatest ei võta suur osa maailma meiliserveritest kirju vastu. Tuntuimad sellistest nimekirjadest on ORBZ (http://www.orbz.org/) ja MAPS (http://mail-abuse.org). Nimekirja sattumine on üsna lihtne, vaid vihje kelleltki ORBZ'i, mille peale ORBZ testib masinat ning saades kinnitava tulemuse lisab masina aadressi oma andmebaasi. Meiliserverid, mis kasutavad ORBZ'i baasi rämpsposti vältimiseks, kontrollivad iga saabuva meili puhul, kas saatja server on baasis kirjas või mitte. Kui on, siis ei edasta server meili isegi sel juhul, kui saajaks on minu-firma.ee kasutaja. Kui meiliserver satub näiteks MAPS musta nimekirja, sulgevad mitmed väga suured teenusepakkujad kogu liikluse mustas nimekirjas olevale serverile.

Kuidas vältida probleeme?

Tavaliselt on avatud vahendajateks seadistamata MS Exchange, Mdaemon või Sendmaili vanemad versioonid. Kuidas siis seadistada meiliserverit, et seda vältida? Kuna erinevaid meiliservereid on palju, ei hakka ma siin konkreetseid lahendusi tooma. Toon ära ainult põhimõtte:
Meiliserver tuleb seadistada nii, et vahendamisel (relay) aktsepteeritaks vaid teatud võrgublokist tulevaid meile (nagu seda on asutuse sisevõrk) ja ei vahendata väljastpoolt tulevaid meile, välja arvatud need, mis on domeenile @minu-firma.ee.

Kõik kaasaegsed meiliserverid oskavad teha sedasorti filtreerimist, vanemate meiliserverite puhul on olemas kas veaparandused või siis uuemad versioonid.

Avatud edastaja

Avatud vahendaja alaliik on avatud edastaja (open forwarder). Tüüpiliseks avatud edastajaks on valesti seadistatud Wingate (või mõni muu gateway). Sisevõrgus olijatele on Wingate's tehtud SMTP teenuse suunamine mõnele välisvõrgus olevale serverile, et lihtsustada kasutajatel meili saatmist, kuid on unustatud keelata ligipääs välisvõrgust. Sellisel juhul satub musta nimekirja meiliserver, millele suunamine on tehtud. Kui serveri omanik selle avastab, keelab ta tavaliselt momentaalselt ligipääsu oma serverile aadressilt, kust suunamine on tehtud. Seda loomulikult selleks, et mustast nimekirjast välja saada.

Meiliserveri ja gateway korrektne seadistamine ei ole raske ning aitab vältida probleeme, mis tabavad serveri omanikku musta nimekirja sattumisel.

Kas see on legaalne?

Paljud on küsinud, kas sellised nimekirjad on üldse legaalsed? Kas avatud vahendaja omanik saab näiteks ORBZ'i kohtusse kaevata selle eest, et põhjustatakse kahju meilide blokeerimisega? Lühike vastus on ei. Musta nimekirja haldaja ei blokeeri midagi. Nemad peavad ainult nimekirja IP'dest, mis on avatud vahendajad. Mida selle infoga peale hakata, otsustavad meiliserverite haldajad. Meilide liikumist blokeerivad just nemad ning neil on täielik õigus seda teha. Mitte miski ei keela seda neil teha. Seega pole mingit muud võimalust nimekirjast välja saamiseks, kui meiliserver õigesti seadistada.

Lõpetuseks mõned viidad tuntumatele mustadele nimekirjadele. Kõigil neil lehtedel on üleval ka põhjalik juhend, kuidas avatud vahendajate kohta infot saata, kuidas mustast nimekirjast välja saada jne.

- Lahendused

- Serverid
- Turvalisus
- Võrguseadmed